medialaws

Rivista di diritto dei media
3/2022 dicembre



DIRETTORE RESPONSABILE
EDITOR-IN-CHIEF
Oreste Pollicino (Università Bocconi)

DIRETTORI
EDITORS
Giulio Enea Vigevani (Università di Milano - Bicocca)
Carlo Melzi d'Eril (Avvocato in Milano)
Marina Castellaneta (Università di Bari)
Marco Bassini (Tilburg University)

VICEDIRETTORI
VICE-EDITORS
Marco Cuniberti (Università di Milano)
Giovanni Maria Riccio (Università di Salerno)
Marco Orofino (Università di Milano)
Ernesto Apa (Avvocato in Roma)

REDAZIONE
EDITORIAL BOARD
Marco Bassini (*coordinatore*) (Tilburg University)
Flavia Bavetta (*vice coordinatore*) (Università Bocconi)
Redazione di Bari
Teresa Catalano, Giuseppe Gallo, Stefania Rutigliano
Redazione di Milano-Bicocca
Maria Galbusera, Giacomo Mingardo, Giulia Napoli
Redazione di Milano-Bocconi
Pietro Dunn, Giuseppe Muto, Federica Paolucci

SEDE
CONTACTS
ACCMS Studio Legale
Via Podgora 13 – 20122 Milano

Università Bocconi - Dipartimento di Studi Giuridici
Via Roentgen 1 - 20136 Milano
e-mail: submissions@medialaws.eu

COMITATO SCIENTIFICO- STEERING COMMITTEE

Shulamit Almog *(University of Haifa),* Fabio Basile *(Università di Milano),* Mirzia Bianca *(La Sapienza – Università di Roma),* Elda Brogi *(European University Institute),* Giuseppe Busia *(Autorità Nazionale Anticorruzione),* Licia Califano *(Università di Urbino, già Garante per la protezione dei dati personali),* Angelo Marcello Cardani *(Università Bocconi, già Autorità per le garazie nelle comunicazioni),* Marta Cartabia *(Università Bocconi, Presidente emerito della Corte costituzionale),* Massimo Ceresa-Gastaldo *(Università Bocconi),* Pasquale Costanzo *(Università di Genova),* Marilisa D'Amico *(Università di Milano),* Filippo Donati *(Consiglio Superiore della Magistratura),* Mario Esposito *(Università del Salento),* Giusella Finocchiaro *(Università di Bologna)*, Tommaso Edoardo Frosini *(Università Suor Orsola Benincasa),* Maurizio Fumo *(Suprema Corte di Cassazione),* Alberto Maria Gambino *(Università Europea – Roma),* Michale Geist *(University of Ottawa),* Glauco Giostra *(La Sapienza – Università di Roma),* Enrico Grosso *(Università di Torino),* Uta Kohl *(University of Southampton),* Krystyna Kowalik-Bańczyk *(Tribunale dell'Unione europea),* Simone Lonati *(Università Bocconi),* Fiona Macmillan *(University of London),* Vittorio Manes *(Università di Bologna),* Michela Manetti *(Università di Siena),* Christopher Mardsen *(University of Sussex),* Manuel D. Masseno *(Instituto Politécnico de Beja),* Roberto Mastroianni *(Tribunale UE),* Luigi Montuori *(Garante per la protezione dei dati personali),* Antonio Nicita *(LUMSA, già Autorità per le garanzie nelle comunicazioni),* Monica Palmirani *(Università di Bologna)*, Miquel Pequera *(Universitat Oberta de Catalunya),* Vincenzo Pezzella *(Suprema Corte di Cassazione),* Laura Pineschi *(Università di Parma),* Giovanni Pitruzzella *(Corte di giustizia UE),* Francesco Pizzetti *(Università di Torino),* Andrea Pugiotto *(Università di Ferrara),* Margherita Ramajoli *(Università di Milano),* Gianpaolo Maria Ruotolo *(Università di Foggia),* Sergio Seminara *(Università di Pavia),* Salvatore Sica *(Consiglio di Presidenza della Giustizia Amministrativa),* Pietro Sirena *(Università Bocconi),* Francesco Viganò *(Corte costituzionale),* Luciano Violante *(Fondazione Leonardo - Civiltà delle Macchine)*, Lorenza Violini *(Università di Milano),* Roberto Zaccaria *(Università di Firenze),* Nicolò Zanon *(Corte costituzionale),* Vincenzo Zeno-Zencovich *(Università di Roma Tre)*

COMITATO DEGLI ESPERTI PER LA VALUTAZIONE - ADVISORY BOARD

Maria Romana Allegri, Giulio Allevato, Benedetta Barbisan, Marco Bellezza, Daniela Bifulco, Elena Bindi, Carlo Blengino, Monica Bonini, Manfredi Bontempelli, Fernando Bruno, Daniele Butturini, Irene Calboli, Simone Calzolaio, Quirino Camerlengo, Gianluca Campus, Nicola Canzian, Marina Caporale, Andrea Cardone, Corrado Caruso, Stefano Catalano, Adolfo Ceretti, Francesco Clementi, Roberto Cornelli, Giovanna Corrias Lucente, Filippo Danovi, Monica Delsignore, Giovanni De Gregorio, Giovanna De Minico, Gabriele Della Morte, Marius Dragomir, Fernanda Faini, Fabio Ferrari, Roberto Flor, Federico Furlan, Giovanni Battista Gallus, Marco Gambaro, Gianluca Gardini, Ottavio Grandinetti, Antonino Gullo, Erik Longo, Valerio Lubello, Federico Lubian, Nicola Lupo, Paola Marsocci, Claudio Martinelli, Alberto Mattiacci, Alessandro Melchionda, Massimiliano Mezzanotte, Francesco Paolo Micozzi, Donatella Morana, Piergiuseppe Otranto, Omar Makimov Pallotta, Anna Papa, Paolo Passaglia, Irene Pellizzone, Sabrina Peron, Bilyana Petkova, Davide Petrini, Marina Pietrangelo, Federico Gustavo Pizzetti, Augusto Preta, Giorgio Resta, Francesca Rosa, Andrej Savin, Salvatore Scuto, Monica Alessia Senor, Stefania Stefanelli, Giulia Tiberi, Bruno Tonoletti, Emilio Tosi, Lara Trucco, Luca Vanoni, Gianluca Varraso, Silvia Vimercati, Thomas Wischmeyer, Paolo Zicchittu

ANNO 2022 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

MediaLaws - Rivista di diritto dei media è una rivista quadrimestrale telematica, ad accesso libero, che si propone di pubblicare saggi, note e commenti attinenti al diritto dell'informazione italiano, comparato ed europeo.

La rivista nasce per iniziativa di Oreste Pollicino, Giulio Enea Vigevani, Carlo Melzi d'Eril e Marco Bassini e raccoglie le riflessioni di studiosi, italiani e stranieri, di diritto dei media.

I contributi sono scritti e ceduti a titolo gratuito e senza oneri per gli autori. Essi sono attribuiti dagli autori con licenza Creative Commons "Attribuzione – Non commerciale 3.0" Italia (CC BY-NC 3.0 IT). Sono fatte salve, per gli aspetti non espressamente regolati da tale licenza, le garanzie previste dalla disciplina in tema di protezione del diritto d'autore e di altri diritti connessi al suo esercizio (l. 633/1941).

Il lettore può utilizzare i contenuti della rivista con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons "Attribuzione – Non commerciale 3.0 Italia" (CC BY-NC 3.0 IT), in particolare menzionando la fonte e, laddove necessario a seconda dell'uso, conservando il logo e il formato grafico originale.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Comittee on Publication Ethics).

La qualità e il rigore scientifici dei saggi della Rivista sono garantiti da una procedura di *double-blind peer review* affidata a un comitato di esperti per la valutazione individuato secondo criteri di competenza e rotazione e aggiornato ogni anno.

MediaLaws - Rivista di diritto dei media
Regolamento per la pubblicazione dei contributi

1. "MediaLaws – Rivista di diritto dei media" è una rivista telematica e ad accesso aperto che pubblica con cadenza quadrimestrale contributi attinenti al diritto dell'informazione.

2. Gli organi della rivista sono il Comitato di direzione, il Comitato scientifico e il Comitato degli esperti per la valutazione. L'elenco dei componenti del Comitato di direzione e del Comitato scientifico della rivista è pubblicato sul sito della stessa (rivista.medialaws.eu). Il Comitato degli esperti per la valutazione è sottoposto ad aggiornamento una volta l'anno.

3. La rivista si compone delle seguenti sezioni: "Saggi", "Note a sentenza" (suddivisa in "Sezione Europa", "Sezione Italia" e "Sezione comparata"), "Cronache e commenti" e "Recensioni e riletture". I singoli numeri potranno altresì ospitare, in via d'eccezione, contributi afferenti a sezioni diverse.

4. La sezione "Saggi" ospita contributi che trattano in maniera estesa e approfondita un tema di ricerca, con taglio critico e supporto bibliografico.

5. La sezione "Note a sentenza" ospita commenti alle novità giurisprudenziali provenienti dalle corti italiane, europee e straniere.

6. La sezione "Cronache e commenti" ospita commenti a questioni e novità giuridiche di attualità nella dimensione nazionale, europea e comparata.

7. La sezione "Recensioni e riletture" ospita commenti di opere rispettivamente di recente o più risalente pubblicazione.

8. La richiesta di pubblicazione di un contributo è inviata all'indirizzo di posta elettronica submissions@medialaws.eu, corredata dei dati, della qualifica e dei recapiti dell'autore, nonché della dichiarazione che il contributo sia esclusiva opera dell'autore e, nel caso in cui lo scritto sia già destinato a pubblicazione, l'indicazione della sede editoriale.

9. La direzione effettua un esame preliminare del contributo, verificando l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

10. In caso di esito positivo, la direzione procede ad assegnare il contributo alla sezione opportuna.

11. I saggi sono inviati alla valutazione, secondo il metodo del doppio cieco, di revisori scelti dall'elenco degli esperti per la valutazione della rivista secondo il criterio della competenza, della conoscenza linguistica e della rotazione. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore. La direzione garantisce l'anonimato della valutazione.

12. La direzione comunica all'autore l'esito della valutazione.
Se entrambe sono positive, il contributo è pubblicato.
Se sono positive ma suggeriscono modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. La direzione si riserva la facoltà di sottoporre il contributo così come modificato a nuova valutazione, anche interna agli organi della rivista. Se solo una valutazione è positiva, con o senza modifiche, la direzione si riserva la facoltà di trasmettere il contributo a un terzo valutatore. Se entrambe le valutazioni sono negative, il contributo non viene pubblicato.

13. Per pubblicare il contributo, l'Autore deve inviare una versione definitiva corretta secondo le regole editoriali della rivista pubblicate sul sito della stessa, un abstract in lingua italiana e inglese e un elenco di cinque parole chiave. Il mancato rispetto dei criteri editoriali costituisce motivo di rigetto della proposta.

14. Le valutazioni vengono archiviate dalla direzione della rivista per almeno tre anni.

15. A discrezione della direzione, i saggi di autori di particolare autorevolezza o richiesti dalla direzione possono essere pubblicati senza essere sottoposti alla procedura di referaggio a doppio cieco ovvero essere sottoposti a mero referaggio anonimo, previa segnalazione in nota.

Indice
Index

Editoriale

11 Ordine, 60 anni. La trappola della censura educativa
Ferruccio de Bortoli

Saggi

15 L'incostituzionalità del sistema di "doppio binario" in materia di diritto d'autore riapre il dibattito sulla legittimità strutturale dei cumuli punitivi: verso una nuova stagione del *ne bis in idem*?
Simone Lonati

54 Avvertenze per il consumatore e obblighi delle piattaforme del commercio elettronico. Alcune osservazioni sulla sentenza *Lee v. Amazon*
Rosario Petruso

76 La normativa a tutela dei minori nel Testo Unico per la fornitura di servizi di media audiovisivi con uno sguardo rivolto al regolamento (UE) 2022/2065
Marco Orofino

94 Messaggistica WhatsApp ed e-mail nel contesto delle prerogative dei membri del Parlamento *ex* art. 68, terzo comma, Cost. Prospettive costituzionali di diritto della comunicazione
Enrico Albanesi

109 La disciplina delle piattaforme *online* fra giurisdizioni e legislatori nazionali e sovranazionali. Dai casi *Airbnb* al *Digital Services Package*
Maria Esmeralda Bucalo

137 Intelligenza urbana e tutela dei diritti fondamentali. Antinomia o complementarità nella nuova stagione algoritmica?
Federica Paolucci - Oreste Pollicino

158 La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino.
Sarah Lattanzi

179 Dati sanitari e *e-Health* europea: tra trattamento dei dati personali e decisione amministrativa algoritmica
Giuseppina Lofaro

209 *European Media Freedom Act:* la tutela europea della libertà dei media
Giuseppe Muto

237 A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)
Chiara Gallese

Note a sentenza

272 Negazionismo: la Cassazione precisa i contorni dell'aggravante in linea con la giurisprudenza di Strasburgo
Marina Castellaneta

289 The (posthumous) exercise of the right to be forgotten
Federica Casarosa

296 Il concetto di algoritmo in una recente sentenza del Consiglio di Stato
Silvia Cereda

301 Il nuovo perimetro di liceità per la pubblicazione di immagini di un atleta senza il suo consenso
Sabrina Peron

308 Internet e "standard della community" nella regolamentazione delle piattaforme online: sulla non vessatorietà delle clausole in materia di disinformazione
Matteo Gozzi

316 NFT e proprietà intellettuale: problemi e prospettive
Sveva Ruggiero

Cronache

326 La digitalizzazione nell'UE: una sfida costituzionale
Giuseppe Muto

337 Diritto all'oblio. Prime riflessioni sull'introduzione dell'art. 64-*ter* disp. att. c.p.p.
Margherita Pisapia - Carlotta Cherchi

352 Il contrasto legislativo ai socialbot e le soluzioni avanzate nella Repubblica di Singapore e nella Repubblica d'Irlanda
Alessandro Tedeschi Toschi - Giampaolo Berni Ferretti

386 Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale
Agostino Sola

405 Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo - NIS
Flavia Bavetta

415 Dati personali e decisioni automatizzate: quale trasparenza?
Gianluca Fasano

Indice
Index

Editorial

11 The trap of "educational censorship"
Ferruccio de Bortoli

Essays

15 The declaration of constitutional illegitimacy of the "dual track" system in the copyright legislation reopens the debate on the structural legitimacy of the double penalty tracks: towards a new season of the *ne bis in idem* principle?
Simone Lonati

54 Consumer warnings and e-commerce platforms obligations after Lee v. Amazon judgment
Rosario Petruso

76 Minors protection in the Italian Audiovisual Media Services Code. An overview in light of regulation (EU) 2022/2065
Marco Orofino

94 Freedom of communication via WhatsApp and e-mail messages and parliamentary immunities
Enrico Albanesi

109 The regulation of online platforms between national and supranational jurisdictions and legislators. From Airbnb cases to the Digital Services Package
Maria Esmeralda Bucalo

137 Urban intelligence and protection of fundamental rights. Antinomy or complementarity in the new algorithmic season?
Federica Paolucci - Oreste Pollicino

158 The fight against disinformation in the relationship between European Union and third countries in light of the Russian-Ukraine war
Sarah Lattanzi

179 Health data and European e-Health: between personal data processing and algorithmic administrative decision
Giuseppina Lofaro

209 European Media Freedom Act: the european protection of media freedom
Giuseppe Muto

237 A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)
Chiara Gallese

Case notes

272 Genocide denial: Italian Supreme Court fine-tunes the scope of the aggravated crime in accordance with the European Court of Human Rights case law
Marina Castellaneta

289 The (posthumous) exercise of the right to be forgotten
Federica Casarosa

296 The concept of algorithm in a recent judgment of the Italian Council of State
Silvia Cereda

301 The new scope of lawfulness for publishing images of an athlete without his consent
Sabrina Peron

308 Internet and community standards in the regulation of social platforms: the non-vexatiousness of disinformation clauses
Matteo Gozzi

316 NFT and intellectual property rights: problems and perspectives
Sveva Ruggiero

Comments

326 Digitization in the EU: a constitutional challenge
Giuseppe Muto

337 Right to be forgotten: the introduction of art. 64-*ter* of the implementing provisions of the Italian Criminal Procedure Code
Margherita Pisapia - Carlotta Cherchi

352 Regulation of socialbots: recent attempts in Singapore and Ireland
Alessandro Tedeschi Toschi - Giampaolo Berni Ferretti

386 Data economy, new powers and administative authorities: a focus on the Italian Cybersecurity Agency
Agostino Sola

405 The NIS 2 Directive: Road to higher levels of cybersecurity at the European level
Flavia Bavetta

415 Personal data and automated decision-making: which transparency?
Gianluca Fasano

Sono stati sottoposti a referaggio anonimo a doppio cieco i saggi di Enrico Albanesi, Maria Esmeralda Bucalo, Chiara Gallese, Sarah Lattanzi, Giuseppina Lofaro, Simone Lonati, Giuseppe Muto, Marco Orofino, Federica Paolucci-Oreste Pollicino e Rosario Petruso.
Su determinazione della Direzione, ai sensi dell'art. 15 del Regolamento, sono stati altresì sottoposti a referaggio anonimo i contributi di Silvia Cereda, Gianluca Fasano, Sveva Ruggiero, Agostino Sola, Alessandro Toschi Tedeschi-Giampaolo Berni Ferretti

Editoriale

Ordine, 60 anni. La trappola della censura educativa

Ferruccio de Bortoli

Il mio contributo a questa importante giornata, nella quale festeggiamo i 60 anni dell'Ordine, può avere come titolo - anche se non si dovrebbe fare il titolo prima di scrivere l'articolo - la trappola della censura educativa. Mai come nel periodo che stiamo vivendo, complice la rivoluzione digitale che è, ricordiamocelo bene, nostra amica e non nemica perché allarga e valorizza potenzialmente lo spazio della professione giornalistica, mai come in questo momento dicevo vi è stata una tale convergenza di pensieri, azioni, semplici riflessi mentali che privilegiano la supposta e ipotetica correttezza dell'informazione alla libertà d'espressione, per non parlare dei fenomeni *woke* e dell'ossessione della cosiddetta *cancel culture*.

In linea di principio dovremmo essere tutti d'accordo. Ognuno di noi sa quanto dannose siano per una democrazia rappresentativa, nella quale la pubblica opinione è l'architrave della democrazia - come scriveva Giovanni Sartori, siamo nel centenario dalla nascita - le notizie false, le *fake news*. Ma nel combatterle non dobbiamo commettere l'errore di pagare un prezzo troppo alto al pluralismo e alla libertà di tutte le voci, giuste o sbagliate che siano, di esprimersi. E, nello stesso tempo, dobbiamo scongiurare il rischio, letale, di concedere agli Stati - al ppotere esecutivo più che a quello legislativo e giudiziario - una missione sostanzialmente censoria, pur nella condivisione degli obiettivi e nella salvaguardia di beni pubblici come per esempio la salute.

Una *fake news* si può prevenire - ma chi ha il potere e l'autorità di giudicarla tale? - si può rimuovere, con gli strumenti che offre la legge, ma certamente la si può combattere ancora di più e meglio smascherandola nella trasparenza, nella responsabilità di un'informazione professionale e qualificata, e soprattutto salvaguardando il pluralismo delle voci che è il vero antidoto. Se si uccide - pur perseguendo un obiettivo condivisibile, quello di limitare le *fake news* - la libertà d'espressione dei soggetti, si rischiano danni irreparabili alla qualità dell'opinione pubblica, si indeboliscono gli anticorpi di una democrazia, si priva il cittadino di strumenti essenziali per accrescere il proprio spirito critico, lo si tratta come un eterno minorenne e, dunque, lo si espone ancora di più a comunicazioni subdole, verosimili, strumentali che lo sviluppo degli algoritmi e dell'intelligenza artificiale, renderà ancora più difficilmente rintracciabili.

Va guardata con una certa preoccupazione - e non con il compiacimento per un intervento che limita solo apparentemente il loro strapotere - quella che due giuristi come Carlo Melzi d'Eril e Giulio Enea Vigevani (*Potere, informazione, diritti,* Edizioni Il Sole 24 Ore) chiamano una "alleanza censoria" tra Stati e grandi *social network*. Giusto intervenire - come prescrivono diversi accordi in particolare per iniziativa dell'Unione europea - per contrastare istigazioni a compiere dei reati, discorsi violenti e d'odio, diffusione di immagini lesive di diritti personali - ma rimane il problema di chi abbia la legittimità di operare questo tipo di censura, se vi sia o no un controllo giudiziale, e

se non sia meglio, in molti casi, affidarsi al senso di responsabilità dei soggetti professionali dell'informazione, alla loro autorevolezza o sensibilità. E ovviamente a diverse e più evolute regole del gioco.
Non è giusto a mio avviso, togliere la libertà di parola - da parte di un privato poi - a un presidente degli Stati Uniti, è dovere invece dell'informazione denunciarne i falsi. Gli accordi dei *social network* sono spesso fatti con regimi autoritari che si impossessano dei dati relativi alle vite dei propri cittadini per reprimere ancora di più la libertà. La pandemia prima, e la guerra dopo, hanno indotto gli Stati, non avendo altri strumenti a disposizione, a premere sui *social network* perché agevolassero una sorta di "verità di Stato", di "informazione educativa di emergenza", in alcuni casi assolutamente condivisibile per lo scopo di affrontare delle emergenze, ma non priva di elementi di rischio e di potenzialità negative.
Ma quanto è esteso l'interesse generale che si vuole tutelare e qual è il limite oltre il quale si comprime in maniera intollerabile un diritto d'opinione? È più facile contrastare reati, peraltro gravi, come la pedopornografia, o difendere il diritto d'autore. Sono fattispecie comunque circoscritte. L'individuazione di un confine dell'interesse generale è, invece, del tutto arbitraria. Il limite tende a sfuggire a un controllo giurisdizionale, rientra nella discrezionalità della politica. Se ritengo, per esempio, che sia nell'interesse generale, l'esigenza di una dieta alimentare diversa a tutela dell'ambiente, la proibizione del fumo o dell'alcol, questo autorizza a limitare la libertà di espressione su questi temi? L'obiettivo è meritorio, non il mezzo attraverso il quale si cerca di raggiungerlo. Abbiamo bisogno per realizzare la transizione ecologica o per migliorare la salute dei cittadini, cambiando le loro abitudini, non solo alimentare, di persone informate, consapevoli, adulte, dotate di spirito critico. E non di minorenni cresciuti, incapaci di distinguere il bene dal male e bisognosi di un tutore civico.
La trappola della censura educativa non risparmia i media tradizionali. Le regole che tutelano soggetti deboli sono chiare. Il rispetto della dignità delle persone, che non sono mai merce dell'informazione, discende da discipline di legge e da codici di autoregolamentazione. C'è un limite al diritto di cronaca che si bilancia costituzionalmente con altri diritti soggettivi. Ne dobbiamo avere sempre di più la consapevolezza per informare meglio. Ma censurare immagini di fatti pubblici - mi riferisco per esempio all'assalto con vernici al Senato - per il timore di scatenare effetti cumulativi, è sinonimo di una postura educativa che rischia di spostare sempre più in avanti quel concetto di interesse generale di cui vi parlavo. Allora non c'è più limite. Il diritto all'oblio è sacrosanto ma non cancella i fatti, quelli rimangono. Sono solo le autocrazie che hanno sfruttato un diritto delle democrazie per cancellare, rimuovere e strumentalizzare la storia.
Allora vi chiederete quali possono essere i rimedi? Innanzitutto, la già richiamata salvaguardia del pluralismo delle voci, l'autorevolezza, la serietà e la responsabilità della professione giornalistica. Nell'era dell'intelligenza artificiale - l'esperienza con la chat GPT è impressionante e sembra sostituire di fatto ogni giornalista - c'è anche un nuovo tema di regole e della loro esigibilità per il quale dovremmo sentirci tutti più impegnati. Per esempio la trasparenza degli algoritmi pur nel rispetto del segreto industriale. L'assoggettazione dei *social network* a un loro giudice naturale al quale il cittadino

possa appellarsi. Le piattaforme dovrebbero poi sentirsi in obbligo di non ospitare più contenuti provenienti da robot o da account non accertati. O almeno di denunciarne la provenienza, in modo da mettere in guardia i lori iscritti. Questo non significa far venir meno la libertà di anonimato o di celarsi dietro un *nickname*, ma di consentirne l'eventuale individuazione nel caso di reati o di comunicazioni false e strumentali. Ma per perseguire questi obiettivi, dobbiamo essere coscienti di quanto pericolosa sia la trappola della censura educativa e di quanto elevato sia il rischio di esserne di fatto complici. Sprovveduti ma non innocenti.

Saggi

L'incostituzionalità del sistema di "doppio binario" in materia di diritto d'autore riapre il dibattito sulla legittimità strutturale dei cumuli punitivi: verso una nuova stagione del *ne bis in idem*?*

Simone Lonati

Abstract

La Corte costituzionale, per la prima volta, ha sancito l'illegittimità di uno dei diversi cumuli punitivi attualmente vigenti nell'ordinamento interno: quello previsto dalla normativa a tutela del diritto d'autore. Lo ha fatto con una sentenza (n. 149/2022), per certi versi inattesa, i cui itinerari logico argomentativi appaiono interamente incentrati sulla fisionomia europea del divieto di *bis in idem*. In questa prospettiva, la pronuncia della Corte costituisce lo spunto per tornare a riflettere sul significato di un principio, quello del *ne bis in idem*, che da sempre – e ancora oggi – stenta a trovare un proprio definitivo approdo. Ripercorrere gli itinerari evolutivi e involutivi della garanzia nella giurisprudenza delle due Corti europee, consentirà di comprendere la portata realmente innovativa della sentenza della Consulta sul doppio binario in materia di diritto d'autore, la quale, ben oltre i limiti formali del giudicato costituzionale, appare destinata a lasciare un segno profondo, rimettendo in discussione la legittimità delle scelte legislative fondate sul familiare schema del doppio binario sanzionatorio.

For the first time the Constitutional Court has established the constitutional illegitimacy of one of the double penalty tracks currently in force in the Italian domestic system, namely that provided for in the copyright legislation. It did so in a judgment (No. 149/2022), that came in some ways unexpected, through legal arguments entirely focused on the European interpretation of the *ne bis in idem* principle. From this perspective, the Court's judgment represents an opportunity to dwell on the

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

meaning of the principle, that still struggles to find its own definitive haven. In the light of the analysis of the two European Courts' case law, the truly innovative reach of the Constitutional Court's judgment will be unveiled. Indeed, far beyond the formal limits of the Constitutional rulings, the judgment appears intended to leave an important mark, by calling into question the legitimacy of legislative choices based on the common scheme of the double penalty track.

Sommario

1. Alla base della sentenza n. 149/2022: sistemi di doppio binario e divieto di *bis in idem* - 2. La fisionomia "euro convenzionale" del *ne bis in idem*. I presupposti operativi della garanzia: il *bis* e l'*idem factum* nella giurisprudenza delle due Corti europee - 2.1. La discussa funzionalità del principio: tra divieto di doppia sanzione e divieto di doppio giudizio - 2.1.1. (segue) Itinerari evolutivi e involutivi nella giurisprudenza della Corti europee: dalla sentenza *Grande Stevens* alla pronuncia *Åkerberg Fransson* – 2.1.2 (segue) Dalla sentenza *A e B c. Norvegia* alle pronunce *Garllson, Menci e Di Puma Zecca* - 3. La sentenza costituzionale n. 149/2022: l'ordinanza di rimessione - 3.1. (segue) La decisione della Corte - 4. Le "due direttrici fondamentali" della pronuncia: l'adesione alla logica processuale del *ne bis in idem* - 4.1. (segue) Il limitato effetto additivo della sentenza di accoglimento.

Keywords

corte costituzionale - diritto d'autore - diritto penale - doppio binario sanzionatorio - *ne bis in idem*

1. Alla base della sentenza n. 149/2022: sistemi di doppio binario e divieto di *bis in idem*

Con la sentenza n. 149 del 16 giugno 2022[1], la Corte costituzionale è tornata nuovamente a pronunciarsi su un tema, quello relativo alla legittimità strutturale dei sistemi punitivi c.d. a "doppio binario" (penale e amministrativo), che costituisce uno snodo tra i più controversi dell'intero panorama penale e processuale e che, da

[1] Corte cost., 16 giugno 2022, (ud. 10 maggio 2022), n.149, in *Cass. pen.*, 2022, 3370. Per un primo commento alla sentenza, cfr. S. Seminara, *Il divieto di bis in idem: un istituto inquieto*, in *Dir. pen. proc.*, 11, 2022, 1381 ss.; N. Recchia, *L'ennesima stagione del ne bis in idem nel costituzionalismo multilivello: la riaffermazione del suo ubi consistam processuale contro ogni riduzionismo sostanziale*, in *Riv. it. dir. proc. pen.*, 2022, (in corso di pubblicazione); M. Scoletta, *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario punitivo in materia di diritto d'autore*, in *Sist. Pen.*, *on line*, 23 giugno 2022; A. Nocera, *Ne bis in idem, doppio binario sanzionatorio e diritto d'autore: prima pronuncia d'illegittimità costituzionale*, in *Il penalista*, 13 luglio 2022; R. Rudoni, *Ancora a proposito di giurisdizione costituzionale, cumuli punitivi eterogenei e ne bis in idem, (riflessioni a partire da Corte cost., sent. n. 149/2022 relativa al 'doppio binario' in materia di diritto d'autore),* in *Nomos*, 2, 2020.

sempre, è al centro di un vivace dibattito costituzionale e politico criminale[2].
Alla base vi è, infatti, il difficile tentativo di realizzare un equo contemperamento tra esigenze primarie e sostanzialmente eterogenee: se da un lato, infatti, viene in considerazione l'interesse statuale alla diversificazione delle strategie punitive, nell'ottica di garantire l'effettività della risposta sanzionatoria in particolari settori nei quali, più che altrove, si avverte l'insufficienza della sola sanzione penale, d'altra parte, la duplicazione delle sanzioni e delle procedure rispetto ad uno stesso fatto, deve fare i conti con il riconoscimento del superiore principio del *ne bis in idem* europeo[3].
Principio di «civiltà giuridica»[4], che, nella sua duplice e concorrente declinazione convenzionale ed euro unitaria[5], funge da parametro interposto nel giudizio di legittimità costituzionale dei sistemi di "doppio binario"[6]: il divieto (*ne*) di doppio giudizio (*bis*) per il medesimo fatto (*in idem*), infatti, mira non solo ad evitare una

[2] Tema di grande interesse, che si inserisce nel solco della c.d. «amministrativizzazione» del diritto penale, per tale intendendosi la tendenza all'incremento di fattispecie incriminatrici incentrate sulla violazione di regole cautelari, ovvero sull'inosservanza di prescrizioni amministrative. Per un approfondimento si rinvia a M. Donini, *Un nuovo medioevo penale? Vecchio e nuovo nell'espansione del diritto penale economico*, in *Cass. pen.*, 2003.

[3] Per un inquadramento di ordine generale del principio del *ne bis in idem* europeo, tema sul quale la letteratura è assai ampia, si rinvia per tutti a: G. Caneschi, *Il divieto di bis in idem*, in M. Ceresa-Gastaldo - S. Lonati (a cura di), *Profili di procedura penale europea*, Milano, 2021, 134 ss.; G. De Amicis, *Diritto dell'UE e della Cedu e problema del ne bis in idem*, in *Libro dell'anno del diritto 2015*, Roma, 2015, 664 ss; G. De Francesco, *Ne bis in Idem: evoluzione e contenuti di una garanzia, nello scenario dell'integrazione europea*, in *Leg. pen.*, 2015, 1 ss.; F. Gaito, *Ne bis in idem (profili europei)*, in *Dig. Disc. pen.*, Agg. IX, Torino, 2021, 461 ss.; N. Madia, *Ne bis in idem europeo e giustizia penale*, Milano, 2020; A. Mangiaracina, *Verso l'affermazione del ne bis in idem nello spazio giudiziario europeo*, in *Leg. pen.*, 2006, 633 ss.; B. Nascimbene, *Ne bis in idem, diritto internazionale e diritto europeo*, in *Dir. pen. cont.*, *on line*, 2018; P. P. Paulesu, *Riflessioni in tema di ne bis in idem europeo*, in *Riv. dir. proc.*, 2015, 645 ss.; A. Procaccino, *Metamorfosi del ne bis in idem: da "certezza del diritto" a "divieto di doppio processo" a "possibilità di procedimenti integrati*", in D. Chinnici - A. Gaito, *Regole europee e processo penale*, IIª ed., Milano, 2018, 325 ss; J.A.E. Varvele, *Ne bis in idem: verso un principio costituzionale transnazionale in UE?,* in *Riv. it. dir. proc. pen.*, 2014, 49 ss.

[4] Corte cost., 21 luglio 2016, n. 200, in *Giur. cost.*, 2016, 1420.

[5] Come noto, il principio del *ne bis in idem* risulta "codificato", da un lato, nell'art. 4 del Protocollo n. 7 della Convenzione Europea dei Dritti dell'Uomo (CEDU), firmato a Strasburgo il 22 novembre 1984 e, dall'altro, nell'art. 50 della Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE) proclamata una prima volta il 7 dicembre 2000 a Nizza, e una seconda volta, in una versione adattata, il 12 dicembre 2007 a Strasburgo. Per un commento a tali disposizioni, si rinvia rispettivamente a: S. Allegrezza, *sub Art. 4, prot. n. 7 CEDU*, in S. Bartole - P. De Sena - V. Zagrebelsky (a cura di), *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2012, 894 ss.; C. Amalfitano, R. D'Ambrosio, *Art. 50 - Diritto di non essere giudicato o punito due volte per lo stesso reato*, in R. Mastroianni - O. Pollicino - S. Allegrezza - F. Pappalardo - O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 1026 ss. Il divieto di *bis in idem*, peraltro, sul piano internazionale trovava già esplicito riconoscimento nell'art. 14, par. 7, del Patto internazionale sui diritti civili e politici, entrato in vigore il 23 marzo 1976, nonché nell'art. 20 dello Statuto della Corte Penale Internazionale, siglato a Roma il 17 luglio 1998 ed entrato in vigore il 1°luglio 2002. Nell'ordinamento interno, benché sia formalmente enunciato solo nel testo dell'art. 649 c.p.p., vi è unanimità di vedute nel ritenerlo principio implicitamente già desumibile dalle garanzie di cui agli artt. 24 e 111 Cost. (in tal senso, *ex multiis*, Corte cost., 21 luglio 2016, n. 200, cit.).

[6] Corte cost., 2 marzo 2018, n. 43, in *Giur. cost.*, 2018, 510. Cfr., § 5 del 'considerato in diritto', ove – con specifico riferimento al principio del *ne bis in idem* – la Corte ribadisce che «Le disposizioni della CEDU e dei suoi protocolli addizionali vivono nel significato loro attribuito dalla giurisprudenza della Corte EDU (sentenze n. 349 e n. 348 del 2007), che introduce un vincolo conformativo a carico dei poteri interpretativi del giudice nazionale quando può considerarsi consolidata».

indiscriminata duplicazione del potere punitivo da parte dello Stato (o di più Stati) che vantassero giurisdizione sullo stesso fatto illecito, ma anche ad assicurare la certezza oggettiva del diritto e la stabilità dei rapporti giuridici, evitando conflitti di giurisdizione tra autorità astrattamente competenti a valutare gli stessi fatti[7].

Un bilanciamento tra interessi eterogenei dietro al quale si intravede, nitida, la contrapposizione tra il legislatore, sovrano nella scelta sul come, quando e perché punire, e le Corti di legittimità – nazionali ed europee – chiamate a rendere effettiva la garanzia del *ne bis in idem* e, per tale via, a porre un argine al libero dispiegarsi della potestà punitiva dello Stato[8].

L'argomento è complesso, le implicazioni che ne derivano sono molteplici e altrettanto variegati gli aspetti problematici: dalla questione relativa alla esatta definizione dei margini applicativi del divieto di *bis in idem* sino a quella che, più direttamente, riguarda la funzionalità del principio. Tutti temi che, a più riprese, e con risultati assai spesso altalenanti, hanno richiesto l'opera chiarificatrice della giurisprudenza e l'intervento del legislatore.

Nel nostro ordinamento, tra le alterne pronunce delle due Corti europee, le scelte legislative tendenti alla configurazione di veri e propri sistemi punitivi alternativi e paralleli a quello penale, avevano potuto trovare – quantomeno sino ad oggi – il sostanziale avallo da parte del Giudice costituzionale, che mai si era spinto sino al punto di decretarne l'illegittimità, per contrasto con il vincolo europeo del *ne bis in idem*.[9]

---

[7] Per il riconoscimento di questa duplice *ratio* del principio, S. Allegrezza, *sub Art. 4, prot. n. 7 CEDU*, in S. Bartole - P. De Sena - V. Zagrebelsky (a cura di), *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, cit., 895, nonché M.C. Carta, *Il principio del ne bis in idem nell'art. 50 della Carta dei diritti fondamentali UE e nella recente giurisprudenza della Corte di giustizia*, *Diritto@ Storia*, 17, 2019.

[8] Cfr., in tal senso, A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, in *Riv. it. dir. proc. pen.*, 2017, 1058, nonché F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A Mangiaracina, *Il ne bis in idem*, Torino, 2021, 205.

[9] In più di un'occasione, come noto, la Corte costituzionale è stata chiamata a valutare – attraverso il consueto parametro interposto di cui all'art. 117 Cost. – la legittimità strutturale dei sistemi punitivi di doppio binario rispetto al vincolo europeo del *ne bis in idem*. Sul punto, tra pronunce di inammissibilità e restituzione degli atti al giudice remittente, si vedano: Corte cost. 12 maggio 2016, n. 102, in *Giur. cost.* 2016, 1479 ss (con nota di A.F. Tripodi, *Il doppio binario sanzionatorio all'esame del giudice delle leggi*, *ivi*, 1498 ss.), in cui la questione di legittimità costituzionale dell'art. 649 c.p.p. è stata dichiarata inammissibile in ragione del carattere "perplesso" della motivazione; Corte cost., 20 maggio 2016, n. 112, in *Giur. cost.*, 2016, 958 ss., in cui la Corte ha ordinato la restituzione degli atti per *ius supervenines*; Corte cost., 2 marzo 2018, n. 43, cit., (con note di F. Pepe, *La corte costituzionale prende atto della metamorfosi del ne bis in idem europeo: fine della storia?,* ivi, 520 ss., e A.F. Tripodi, *Il nuovo volto del ne bis in idem convenzionale agli occhi del giudice delle leggi. Riflessi sul doppio binario sanzionatorio in materia fiscale*, ivi, 530 ss.) in cui la Corte ha nuovamente ordinato la restituzione degli atti per *ius supervenines*; Corte cost., 24 ottobre 2019, n. 222, in *Giur. cost.*, 2019, 2642 (con nota di M. Scoletta, *Legittimità in astratto e illegittimità in concrreto del doppio binario punitivo in materia tributaria al cospetto del ne bis in idem europeo*, ivi 2649 ss) in cui la questione di legittimità dell'art. 649 c.p.p. è stata dichiarata inammissibile per insufficiente descrizione della fattispecie oggetto di giudizio e per difetto di motivazione in punto di rilevanza e non manifesta infondatezza; Corte cost., ord. 12 giugno 2020, n. 114, in *Giur. cost.*, 2020, 1275, in cui la questione di legittimità è stata dichiarata inammissibile per insufficiente motivazione della non manifesta infondatezza e rilevanza della questione prospettata, (per un commento, cfr. F. Brandi, *Rapporto tra sanzioni penali e tributarie: no all'incostituzionalità della norma sul ne bis in idem*, in *Il Societario*, 3 settembre 2020); Corte cost., ord. 1° luglio 2021, n. 136, in *Cass. pen.,* 2021, 3150 (con nota di E. Aprile, *Osservazioni: C. cost., data udienza (10 giugno 2021), data deposito 1° luglio 2021, n. 136, ivi, 3154*), in cui, ancora, la questione di legittimità costituzionale dell'art. 649 c.p.p. è stata dichiarata inammissibile per insufficiente descrizione della fattispecie oggetto

Sino ad oggi, appunto.
Ora, con la sentenza n. 149/2022, la Corte costituzionale ha compiuto un primo, deciso passo verso la necessità di ripensare in generale i modelli punitivi di doppio binario dichiarando l'incostituzionalità dell'art. 649 c.p.p. nella parte in cui tale norma non estende il divieto di doppio giudizio al sistema di doppio binario vigente in una materia, quella relativa alla tutela del diritto d'autore, forse meno nota di altre ma, non per questo, meno problematica[10].
La sentenza della Corte costituzionale sollecita nell'interprete diversi spunti di riflessione: nel merito, essa – e prima ancora l'ordinanza di rimessione che l'ha generata – appare interamente fondata sul significato del *ne bis in idem* desumibile dalla più recente giurisprudenza della Corte europea, la cui autonoma lettura della garanzia – come sempre accade nell'ambito di ogni giudizio relativo alla legittimità dei sistemi puntivi di doppio binario – ha costituito il riferimento normativo essenziale per riempire di contenuto concreto il parametro interposto di legittimità costituzionale. Per questa stessa ragione, del resto, la pronuncia della Corte costituzionale contiene importanti affermazioni di principio che, ben oltre i limiti formali del giudicato costituzionale, appaiono (quantomeno) in grado di (ri)mettere in discussione – in termini generali – la legittimità strutturale dei sistemi di doppio binario vigenti in numerosi settori nell'ordinamento interno.
Ecco che, in questa prospettiva, prima di soffermarsi sulla specifica questione trattata dal Giudice delle leggi, si reputa opportuno passare in rassegna i principali orientamenti interpretativi della giurisprudenza europea maturati rispetto ad alcuni aspetti chiave della materia. Aspetti che, per le dirette implicazioni che assumono in ordine alla sentenza in commento, consentiranno non solo di comprendere appieno gli itinerari logico argomentativi seguiti dalla Corte costituzionale per giungere al risultato di smantellare uno dei tanti sistemi di doppio binario vigenti nell'ordinamento interno, ma anche di ipotizzare i possibili scenari futuri rispetto ai molti altri sistemi di doppio binario – almeno formalmente – non intaccati dalla declaratoria d'incostituzionalità.

2. La fisionomia "euro convenzionale" del *ne bis in idem*. I presupposti operativi della garanzia: il *bis* e l'*idem factum* nella giurisprudenza delle due Corti europee

Delineare la fisionomia europea del divieto di *bis in idem* significa, in primo luogo, definire i presupposti operativi della garanzia e, quindi, il suo esatto perimetro applicativo. Si tratta, è bene intendersi, di un profilo talmente consolidato nell'interpretazione delle Corti sovrannazionali da potersi ritenere ormai un punto fermo della materia.[11] Nondimeno, esso, proprio ai fini del giudizio circa la legittimità dei sistemi

del giudizio.

[10] V. infra., §§ 3 ss.

[11] Sul tema, per un'ampia rassegna della giurisprudenza europea, si rinvia per tutti a: E. M. Mancuso

punitivi di doppio binario c.d. penale – amministrativo, riveste importanza decisiva o, per così dire, "pregiudiziale": come noto, infatti, è solo l'ampia interpretazione dei presupposti operativi della garanzia ciò che, di fatto, ha consentito di estenderne la portata applicativa rispetto a quei sistemi di "doppio binario" che sarebbero stati altrimenti intangibili, in quanto caratterizzati dalla coesistenza, rispetto a un medesimo fatto, di sanzioni e procedure formalmente penali, accanto ad altre (solo) formalmente amministrative ma sostanzialmente penali.

I presupposti operativi del *ne bis in idem* – che l'art. 4 del Protocollo n. 7 della CEDU esplicita sul piano esclusivamente interno, mentre l'art. 50 della Carta di Nizza estende a tutto lo spazio giuridico europeo e, quindi, anche ai rapporti tra pronunce e procedimenti di diversi Stati membri[12] – sono comuni e ben noti: sul presupposto di una previa decisione (di condanna o assoluzione) che sia divenuta irrevocabile e che concerna il merito della responsabilità, il divieto (*ne*) esige che uno stesso soggetto (*idem c.d. soggettivo*), per il medesimo fatto (*idem c.d. oggettivo*), sia nuovamente sottoposto ad altro procedimento penale (*bis*).

Ancorché la formulazione delle disposizioni che lo prevedono faccia espressamente riferimento al divieto di «perseguire» o «condannare» nuovamente taluno nell'ambito di un «procedimento penale» per un «reato», è noto che, nell'interpretazione dei presupposti operativi della garanzia, entrambe le Corti europee abbiano mostrato di prediligere un approccio di carattere sostanziale.[13] Ciò, segnatamente, sia quanto alla qualificazione del "*bis*" sia quanto alla definizione dell'"*idem factum*".

Iniziando da quest'ultimo aspetto, è noto come a partire dal *leading case Zolotukhimn c. Russia*[14], si sia definitivamente compiuta la metamorfosi dal concetto di *idem legale* a quello di *idem factum*: da allora[15] il giudizio circa la medesimezza del fatto deve svol-

– F. Viganò, *Art. 4 prot. n. 7 – Diritto a non essere giudicato o punito due volte*, in G. Ubertis – F. Viganò (a cura di) *Corte di Strasburgo e giustizia penale*, 2016, 379 ss.; C. Amalfitano, R. D'Ambrosio, *Art. 50 - Diritto di non essere giudicato o punito due volte per lo stesso reato*, in R. Mastroianni - O. Pollicino - S. Allegrezza - F. Pappalardo - O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, cit., 1016 ss.; L. Bin, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole*, in *Dir. pen. cont.*, *Riv. Trim.*, 3, 2020, 98 ss.

[12] Per un maggiore approfondimento sul diverso ambito di applicazione che il divieto di *bis in idem* assume a livello convenzionale ed euro unitario, si veda B. Nascimbene, *Ne bis in idem, diritto internazionale e diritto europeo*, cit. Più in generale, per un confronto sulla diversa applicabilità degli strumenti internazionali (con particolare riferimento alla CEDU e alla CDFUE), I. Andrò, *Carta dei diritti fondamentali dell'Unione europea e CEDU: dieci anni di convivenza*, in *Federalismi.it*, 2020.

[13] Così, tra gli altri, A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1058 ss.

[14] Corte EDU, Grande Camera, *Zolotukhin c. Russia*, 10 febbraio 2009, ric. 14939/03.

[15] La giurisprudenza di Strasburgo, prima di pervenire alla nozione di *idem factum*, era per lungo tempo rimasta fedele al criterio dell'*idem legale*, fondato sul mero raffronto tra fattispecie astratte (paradigmatiche di questo orientamento, sia pure con alcune differenze rispetto al modo di intendere il concetto di *idem* legale, Corte EDU, *Ponsetti e Chesnel c. Francia*, 14 settembre 1999, ric. 36855/97 e n. 41731/98; Corte EDU, 14 settembre 2004, *Rosenqvist c. Svezia*, ric. 60619/00, Corte EDU, 30 luglio 1998, *Oliveira c. Svizzera*, ric. 25711/94; Corte EDU, 29 maggio 2001, *Franz Fisher c. Austria*, ric. 37950/97). Per contro, deve sottolinearsi come, in sede "unionale" la Corte di Lussemburgo, avesse già da tempo aderito ad una nozione materiale di *idem* (se ne trova traccia già nelle sentenze CGUE, 9 marzo 2006, *Van Esbroeck*, C-436/04; CGUE, 18 luglio 2007, *Norma Kraaijenbrink*, C-288/05). Per più ampi riferimenti in ordine agli orientamenti delle due Corti, cfr. L. Bin, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole*, cit. 101 ss.; F. Gaito, *Ne bis in idem (profili europei)*, cit., 466 ss.; S. Seminara, *Il divieto di* bis in idem: *un istituto inquieto*, cit., 1383 ss.

gersi avuto riguardo all'accadimento naturalisticamente inteso, ossia al fatto storico (*idem factum*), senza che a nulla rilevi la sua qualificazione giuridica nell'ordinamento interno (*idem legale*)[16].

Quanto al *bis*, altrettanto noto è che la valutazione circa la duplicazione delle procedure e delle sanzioni, prescindendo dall'etichetta "penale" formalmente assegnata alle stesse nell'ambito dell'ordinamento interno, venga ora a dipendere esclusivamente dalla loro natura "sostanzialmente punitiva", da apprezzarsi secondo gli ormai noti *Engel criteria* elaborati dalla Corte europea[17], e successivamente recepiti dalla Corte di giustizia[18].

Per questa strada, svincolato da rigorosi e stringenti vincoli formali, il divieto di *bis in idem* ha visto notevolmente ampliati i propri margini applicativi sino al punto di venire in considerazione non più solo rispetto alla reiterazione di un giudizio penale già definito, ma anche – anzi, soprattutto – rispetto alla duplicazione di procedimenti paralleli, ma appartenenti a diverse branche del diritto (penale e amministrativo). Situazioni che, secondo la tradizionale concezione "endopenalistica" del divieto sarebbero state inidonee ad integrare il requisito del *bis* e che, invece, lo sono divenute – con relativa estensione della portata operativa del principio – per effetto dell'autonoma nozione di *matière penale*[19] elaborata dalle due Corti europee e della conseguente adozione di una prospettiva «panpenalistica»[20] delle sanzioni tale da

[16] In questa prospettiva, dunque, non interessa confrontare gli elementi costitutivi del fatto tipizzato nelle due norme incriminatrici, bensì verificare se i fatti posti a base delle medesime, e giudicati nei rispettivi procedimenti, siano o meno materialmente gli stessi, assumendo quali parametri di verifica l'insieme delle circostanze fattuali concrete relative allo stesso autore e indissociabilmente legate fra loro nel tempo e nello spazio. L'orientamento interpretativo, comune alle due Corte europee, è stato poi recepito nell'ordinamento interno dalla Corte costituzionale (Corte cost., 21 luglio 2016, n. 200, cit., sulla quale, in termini critici, si vedano: D. Pulitanò *Ne bis in idem. Novità dalla Corte Costituzionale e problemi aperti*, in *Dir. pen. e proc.*, 2016, 1588 ss., nonché, D. Vicoli, "*Il ne bis in idem tra approccio naturalistico e dimensione tripartita del fatto: la Corte costituzionale delinea i nuovi equilibri*", in *Giur. cost.*, 2016, 2466 ss.

[17] Cfr. Corte EDU, Grande Camera, 8 giugno 1976, *Engel c. Paesi Bassi*, ric. nn. 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, Serie A n. 22. Si tratta di criteri che, a partire dalla celebre pronuncia, sono stati suddivisi in un triplice ordine: a) la qualificazione giuridica dell'illecito compiuta nell'ordinamento interno (qualificazione che, se formalmente penale, di per sé importa l'attivazione della garanzia); b) la natura effettiva della violazione (da valutarsi alla luce della struttura della norma, verificando ad esempio la tipologia degli interessi oggetto di tutela); c) la natura e il grado di severità della sanzione (aspetti rispettivamente desumibili, la gravità, dal contenuto dell'intervento sanzionatorio, e la natura, dallo scopo della sanzione e dalla procedura prevista per la sua adozione). Per un approfondimento sui criteri elaborati dalla sentenza Engel, si veda M. Chiavario, *La lunga marcia dei diritti dell'uomo nel processo penale*, in A. Balsamo - E. Kostoris (a cura di), *Giurisprudenza europea e processo penale italiano*, Torino, 2008, 16 ss. Si segnala che nella successiva elaborazione giurisprudenziale il requisito dello scopo della sanzione ha assunto valore autonomo, rispetto agli altri parametri, in tal senso cfr. Corte EDU, *Welch c. Regno Unito*, 9 febbraio 1995, ric. 17440/90; Corte EDU, *Phillips c. Regno Unito*, 5 luglio 2001, ric. 52024/99; Corte EDU *Lauko c. Slovacchia*, 2 settembre 1998, ric. 26138/95; Corte EDU, *Sud. Fondi e a. c. Italia*, 5 luglio 2007, ric. 75909/01.

[18] CGUE, Grande Sezione, 5 giugno 2012, *Bonda*, C-489/10.

[19] Sull'elaborazione e la progressiva espansione del concetto di *matière penale,* nella giurisprudenza sovrannazionale, si rinvia per tutti a L. Masera, *La nozione costituzionale di materia penale*, Torino, 2018, 25 ss, nonché F. Mazzacuva, *Le pene nascoste. Topografia delle sanzioni punitiva e modulazione dello statuto garantistico*, Torino, 2017, 95 ss.

[20] Così, F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A Mangiaracina, *Il ne bis in idem*, cit., 208.

porre in primo piano il tema della «unitarietà della funzione afflittiva»[21]. Anzi, sono proprio queste ultime – quelle contrassegnate dalla coesistenza di sanzioni e procedure penali e amministrative – le situazioni di doppio binario che hanno finito per assumere un ruolo preponderante nella casistica giudiziaria relativa al divieto di *bis in idem* divenendo, se così può dirsi, bersaglio privilegiato delle censure delle Corti europee[22].

2.1. (segue) La discussa funzionalità del principio: tra divieto di doppia sanzione e divieto di doppio giudizio

Definito il perimetro operativo della garanzia, un ulteriore e decisivo aspetto sul quale si rende opportuno soffermare l'attenzione – in tal caso, per le più evidenti implicazioni che esso assume rispetto alla pronuncia della Corte costituzionale – è quello relativo alla funzionalità del divieto di *bis in idem* europeo.
Un aspetto, quest'ultimo, inscindibilmente connesso con la dibattuta questione relativa alla natura – sostanziale o processuale – della garanzia, dalla quale prioritariamente dipende il giudizio sulla tenuta dei sistemi di doppio binario vigenti nell'ordinamento interno, e sulla quale, tuttavia, allo stato non può ancora dirsi raggiunta un'unanimità di vedute nella giurisprudenza delle due Corti europee[23].
Per comprendere i termini della questione – sulla quale, lo si anticipa, la Corte costituzionale parrebbe aver assunto una chiara presa di posizione – è bene introdurre, per sommi capi, la distinzione concettuale tra i due significati tradizionalmente associati al *ne bis in idem* che, come emerge dalla laconicità dell'espressione che lo denota, è principio declinabile su piani alternativi[24], significativi di diversi fenomeni e di altrettante funzioni [25].

[21] In questi termini, M. A. Sandulli, *Sanzioni amministrative e principio di specialità: riflessioni sull'unitarietà della funzione afflittiva*, in *giustamm.it*, 2012.

[22] Assunto condiviso dalla dottrina pressoché unanime. Tra gli altri, cfr. F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 205, nonché A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1058 ss.

[23] Sul tema, per un'ampia rassegna della giurisprudenza europea, si rinvia a M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, in *Dir. pen. cont.*, *Riv. trim.*, 4, 2021, 182 ss.; L. Bin, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole*, cit., 101 ss.

[24] In realtà, mentre in dottrina e giurisprudenza non vi è alcun dubbio circa la rappresentabilità in termini di "principio" del *ne bis in idem* processuale, come confermato dalla sua espressa formalizzazione in testi normativi, (cfr. in tal senso D. Caprioli - D. Vicoli, *Procedura penale dell'esecuzione*, IIª ed., Torino, 2011, 65, nonché Corte Cost., 31 maggio 2016, n. 200, cit.) , lo stesso non può dirsi per il *ne bis in idem* sostanziale, la cui fisionomia di "principio" è alquanto discussa in dottrina. A favore del riconoscimento di un vero e proprio principio, similmente a quanto avviene in ambito processuale, F. Mantovani, *Conflitto di norme nel diritto penale*, Bologna, 1966, 470 ss., a giudizio del quale, in assenza di una norma positiva espressamente dedicata, il principio sostanziale sarebbe desumibile da una serie di disposizioni normative, tra cui, oltre all'art. 15 c.p., gli artt. 84, 61, 62, prima parte, 301 e 581 c.p) Di diverso avviso, per tutti, G. Conso, *I fatti giuridici processuali penali. Perfezione ed efficacia*, Milano, 1955, 101 ss.

[25] In tal senso, A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1048. La tesi della fisionomia "ibrida" – sostanziale e processuale – del *ne bis in idem* è condivisa dalla dottrina, che ne ha sottolineato un vero e proprio processo di «metamorfosi», così N. Recchia, *Note minime sulle tre recenti sentenze della Corte di giustizia dell'Unione europea in tema di ne bis in idem"*, in *www.eurojus.it*, 22 marzo 2018;

Sul piano sostanziale, il principio evoca il divieto di duplicare la qualificazione e, perciò stesso, di reiterare la sanzione rispetto ad un medesimo fatto[26]. Nella sua vocazione sostanziale, come divieto di doppia sanzione, il principio risponde a logiche niente affatto diverse da quelle che, nell'ordinamento interno, informano l'istituto del concorso apparente di norme[27]: evitare che l'interferenza tra fattispecie possa indurre ad una multipla considerazione delle medesime note di disvalore del fatto, per ragioni di garanzia individuale che, tradizionalmente, sono state individuate nell'esigenza di giustizia sostanziale[28], equità e soprattutto proporzionalità del trattamento sanzionatorio[29].

Declinato sul piano processuale, invece, il principio evoca il divieto di iniziare o proseguire un secondo procedimento nei confronti di chi, per i medesimi fatti, sia già stato giudicato in maniera definitiva. In questa diversa accezione calibrata sulla logica bi-procedimentale – quella cui espressamente si riferiscono gli art. 4 del Protocollo n. 7 della CEDU, e 50 della Carta di Nizza, nonché, nell'ordinamento interno, l'art. 649 c.p.p.[30] – il divieto di doppio giudizio risponde all'esigenza individuale di

in senso analogo, V. Felisatti, *Il ne bis in idem domestico. Tra coordinazione procedimentale e proporzionalità della sanzione*, in *Dir. pen. cont.*, *Riv. trim.*, 3, 2018, 119 ss.; A. Gaito, *La progressiva trasfigurazione del ne bis in idem*, in *Arch. pen.*, *on line*, 1, 2021; N. Madia, *Il ne bis in idem europeo nella sua "nuova" veste sostanziale: la sua possibile efficacia anche nell'ambito di un unico procedimento in materia di cumuli punitivi"*, in *Arch. pen. on line*, 3, 2019; C. Silva, *La deriva del ne bis in idem verso il canone di proporzionalità*, in *Arch. pen.*, *on line*, 1, 2019; N. Galantini, *Il principio del ne bis in idem tra doppio processo e doppia sanzione*, in *Giur. it.*, 2019, 215 ss. Per una più approfondita disamina del tema dei rapporti tra il piano sostanziale e processuale del principio, cfr. F. Gaito - G. Rainaldi, *Introduzione allo studio dei rapporti tra ne bis in idem sostanziale e processuale*, in *Arch. pen.*, *on line*, 1, 2017, nonché F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 209 ss.

[26] A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1048. Più precisamente, è in discussione se il divieto riguardi la doppia qualificazione o valutazione del fatto, ovvero, la doppia punizione, sul punto si rinvia a M. Papa, *Le qualificazioni giuridiche multiple*, Torino, 1997, 7 ss.

[27] F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 209. In generale sull'approccio metodologico circa la risoluzione del concorso di reati, nel senso della relativa apparenza, secondo i differenti approcci monistico e pluralistico, si rinvia a: G. De Francesco, voce *Concorso apparente di norme*, in *Dig. Disc. Pen.*, II, Torino, 1988, 417 ss., nonché A. Pagliaro, voce *Concorso di norme (dir. Pen)*, in *Enc. Dir.*, VIII, Milano, 1961, 551 ss.

[28] In tal senso, con diversità di accenti, F. Mantovani, *Concorso e conflitto di norme nel diritto penale*, Bologna, 1966, 592 ss.; G. Neppi Modona, *Inscindibilità del reato complesso, e ne bis in idem sostanziale*, in *Riv. it. dir. proc. pen.*, 1966, 204 ss.; G. Vassalli, voce *Reato complesso*, in *Enc. Dir.*, vol. XXXVIII, Milano, 187, 835 ss., M. Romano, *Commentario sistematico del codice penale*, I, III[a] ed., Milano, 2004, 179 ss.

[29] Cfr., B. Romano, *Il rapporto tra norme penali,* Milano, 1996, 280 ss.; A. Pagliaro, voce *Concorso di norme (dir. Pen)*, in *Enc. Dir.*, cit., 551, nonché, più recentemente, F. Consulich, *La norma penale doppia, ne bis in idem sostanziale e politiche di prevenzione generale: il banco di prova dell'autoriciclaggio*, in *Riv. trim. dir. pen. ec.*, 2015, 73.

[30] Si precisa che, diversamente dalle due Corti europee che riferiscono l'operatività del divieto di *bis in idem* alla sola ipotesi in cui si sia formato il giudicato, la Corte di cassazione ha esteso l'operatività de divieto di cui all'art. 649 c.p.p. anche ai casi di litispendenza, ossia alle ipotesi in cui il primo procedimento non sia ancora giunto a definizione, empre che i due processi abbiano ad oggetto il medesimo fatto attribuito alla stessa persona, siano stati instaurati ad iniziativa dello stesso ufficio del p.m. e siano devoluti, anche se in fasi o in gradi diversi, alla cognizione di giudici della stessa sede giudiziaria.. In tal senso, Cass. pen., sez. un., 28 settembre 2005, n. 34655, in *Cass. pen.* 2006, 28 ss. Sul tema si rinvia D. Caprioli - D. Vicoli, *Procedura penale dell'esecuzione*, cit., 69 ss., nonché, anche per le implicazioni di tale orientamento rispetto alla giurisprudenza europea, N. Madia, *Il ne bis in idem convenzionale e comunitario alle prese con la litispendenza*, in *Dir. pen. cont.*, *on line*, 9 giugno 2015.

sottrarre il singolo dalla «spirale di reiterate iniziative penali per il medesimo fatto»[31] (certezza in senso soggettivo)[32], nonché ad esigenze pubblicistiche di certezza del diritto (in senso oggettivo) ed economia dei giudizi[33].

Ancorché si tratti di una tematica indubbiamente complessa, che meriterebbe ben altro approfondimento[34], le considerazioni sin qui svolte sono sufficienti per cogliere le differenze[35] e le intersezioni tra i due piani dello stesso principio. Quanto alle prime basti osservare che, seppure in entrambi i casi l'operatività del divieto di *bis in idem* esiga il riferimento allo stesso soggetto (*eadem persona*), sul piano sostanziale «solo due condanne, anche se in unico procedimento, possono dar vita ad una violazione del divieto», mentre, sul piano processuale, «la violazione potrebbe originare anche da due assoluzioni, ma solo se i procedimenti sono più di uno»[36]. Detto altrimenti: la trasgressione del divieto di doppia sanzione non determina di per sé anche la trasgressione del divieto di doppio giudizio (almeno quando le sanzioni siano irrogate all'interno di un unico procedimento) e, per converso, la trasgressione del divieto di doppio giudizio, non necessariamente implica anche la trasgressione del divieto doppia sanzione (almeno quando uno o entrambi i processi siano culminati con un proscioglimento)[37]. Ciò posto, con altrettanta evidenza emerge l'intersezione

[31] Corte cost., 31 luglio 2016, n. 200, cit.

[32] Valorizzano il fondamento garantistico del divieto di doppio giudizio, N. Galantini, *Il divieto di doppio processo come diritto della persona*, in *Riv. it. dir. proc. pen.*, 1981, 97 ss.; P. P. Rivello, *Analisi in tema di ne bis in idem*, in *Riv. it. dir. proc. pen.*, 1991, 479 ss.; E.M. Mancuso, I*l giudicato nel processo penale*, Milano, 2012, 406. Ripercorre le "tappe" dello sviluppo della dimensione individual garantista del principio, storicamente recessiva, G. De Francesco, *Ne bis in idem: evoluzione e contenuti di una garanzia nello scenario dell'integrazione europea*, cit.

[33] Valorizzano il fondamento mataindividuale e pubblicistico del principio, confermato dalla sua operatività anche rispetto ai giudicati di condanna, G. Conso, *I fatti giuridici processuali penali. Perfezione ed efficacia*, Milano, 1955, 101 ss., nonché, più recentemente T. Rafaraci, voce *Ne bis in idem*, in *Enc. Dir., Annali*, vol. III, Milano, 2010, 861 ss.; F. Cordero, *Procedura penale*, Milano, 2012, 1205.

[34] Per una significativa ricostruzione dell'ambito di operatività del *ne bis in idem* sul versante sostanziale e processuale, cfr. G. Lozzi, *Profili di una indagine sui rapporti tra ne bis in idem e concorso formale di reati*, Milano, 1974, 67 ss.; D. Caprioli, *Sui rapporti tra ne bis in idem processuale e concorso formale di reati*, in *Giur. It.*, 2010, 1183 ss.

[35] Autorevolmente, F. Cordero, *Procedura penale*, cit., 1205: «Anche i penalisti postulano un *ne bis in idem*: attribuiremmo due volte lo stesso atto all'autore, se gli applicassimo norme una delle quali sia eclissata dall'altra ("concorso apparente"); la figura legale "omicidio", ad esempio, include "lesioni" e "percossa". Ma il divieto d'un secondo giudizio sulla *eadem res* ha poco da spartire, anzi niente, con queste massime penalistiche (costituenti un capitolo della logica deontica); è puro fenomeno giudiziario, descritto da famose metafore: esercitando l'azione, l'attore la consuma. Assolto N dall'accusa d'avere ucciso colposamente P, nessuna regola penale vieta ridefinizioni dolose: sono figure indipendenti». Sottolinea come «il diverso fondamento del divieto di doppio giudizio […] incide sulla fisionomia delle relative categorie» del *bis* e dell'*idem*, F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 221.

[36] In questi termini, L. Bin, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole*, cit., 100.

[37] Sottolineano l'indubbia diversità del piano operativo della garanzia sostanziale e processuale, e la conseguente separatezza che contraddistingue i relativi spazi di violazione, D. Falcinelli, *Il fatto di reato sullo sfondo del ne bis in idem nazional europeo*, in *Arch. pen.*, *on line*, 1, 2017, 69; F. Gaito - G. Rainaldi, *Introduzione allo studio dei rapporti tra ne bis in idem sostanziale e processuale*, cit., 11 ss. N. Galantini, *Il principio del ne bis in idem tra doppio processo e doppia sanzione*, cit., 222; D. Caprioli, *Sui rapporti tra ne bis in idem processuale e concorso formale di reati*, cit., 1183.

tra i due piani non appena si ponga mente al fatto che «il divieto di *bis in idem* processuale, avendo ad oggetto la duplicazione di procedimenti per un medesimo fatto, non può che ricomprendere in sé – si direbbe, *a fortiori* – il divieto di duplicazione di condanne (distese su due procedimenti) per lo stesso fatto»[38].

2.1.1. Itinerari evolutivi e involutivi nella giurisprudenza della Corti europee: dalla sentenza *Grande Stevens* alla pronuncia *Åkerberg Fransson*

Ancorché il tono e il contenuto degli artt. art. 4 del Protocollo n. 7 CEDU, e 50 della Carta di Nizza, riconoscano la garanzia nella sua ineluttabile dimensione processuale[39], proprio l'indistinzione tra i due piani dello stesso principio rappresenta, se così può dirsi, una costante della giurisprudenza europea le cui pronunce, nell'ultimo decennio, colgono ora la dimensione sostanziale, ora quella processuale ora, indistintamente, una commistione tra ambedue i piani. Per convincersene sarà sufficiente passare in rassegna, sia pur schematicamente, i principali arresti con i quali le due Corti europee sono state chiamate a giudicare la legittimità degli assetti punitivi di doppio binario rispetto al vincolo europeo del *ne bis in idem*.
Il punto di partenza di questa breve digressione non può che essere rappresentato dalla celeberrima sentenza resa della Corte europea nel caso *Grande Stevens c. Ita-*

[38] In questi termini, A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1051, sottolinea come «la regola sostanziale trova riconoscimento in quella processuale». Sul punto, per ulteriori e interessanti spunti di riflessione, cfr. altresì, D. Caprioli, *Sui rapporti tra ne bis in idem processuale e concorso formale di reati*, cit., 1183, il quale rileva che «le istanze garantistiche che ispirano il divieto di secondo giudizio non coincidono con la sola necessità di evitare che sia condannato due volte un soggetto che la legge consente di punire una sola volta. Ovvio, in altre parole, che non si possa instaurare un secondo giudizio quando non vi siano più sanzioni penali legittimamente applicabili: ma sarebbe un errore limitare questi soli casi la sfera di incidenza del *ne bis in idem* processuale».

[39] In tal senso, ancora A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1051, il quale sottolinea come, ancorché le rubriche delle due norme, e i relativi *incipit*, ove si richiama il diritto a non essere giudicato o punito due volte, ovvero a non essere perseguito o condannato due volte, «potrebbero suggestionare l'interprete […] che è fatto divieto di punire due volte *tout court* il medesimo fatto, vale dire anche quando ciò possa verificarsi all'interno di un unico procedimento, e, dunque pure oltre la logica (bi-procedimentale) propria del *ne bis in idem* processuale», tuttavia, tale suggestione «si dilegua leggendo il testo delle norme chiaramente calibrato sulla logica bi-procedimentale propria del divieto processuale». In tal senso, secondo l'Autore i riferimenti contenuti nell'*incipt* delle due norme, ancorché li si voglia intendere come semplici ridondanze «dimostrano come l'esigenza sostanziale di non addivenire a due condanne per lo stesso fatto sia già assolta, nell'ambito del suo specifico *habitat*, vale a dire il doppio procedimento, dal divieto processuale».

lia[40] costituendo, tale arresto, l'«età dell'oro»[41] della garanzia convenzionale, ossia, il momento in cui al *ne bis in idem* è stato riconosciuto il livello di tutela più ampio, corrispondente alla sua dimensione autenticamente processuale. In quel caso – riguardante, come noto, la disciplina italiana in materia di *market abuse* – la Corte di Strasburgo riscontrava in termini perentori la violazione dell'art. 4 del Protocollo n. 7 della CEDU nella mera previsione legislativa – quale, appunto, quella del nostro ordinamento – di due previsioni sanzionatorie (l'una penale, l'altra amministrativa[42]), inevitabilmente destinate a riflettersi in altrettanti procedimenti a carattere punitivo, aventi ad oggetto lo stesso accadimento storico (l'*idem factum,* in quel caso, una falsa comunicazione al mercato). Proprio nella dimensione «bi procedimentale», ad avviso della Corte, si sarebbe annidata l'incompatibilità «strutturale» della normativa interna rispetto al vincolo del *ne bis in idem* europeo[43]: la definitiva conclusione di un procedimento (indifferentemente, quello penale o quello formalmente ammnistrativo) avrebbe irrimediabilmente posto l'altro in frizione con il divieto di *bis in idem* processuale[44]. Una tutela forte, incentrata sull'inammissibile cumulo procedimentale (prima ancora che sanzionatorio) e, soprattutto, «indifferente rispetto a valutazioni di tipo sostanziale sulla proporzionalità del cumulo punitivo»[45].

Valutazioni, queste ultime, ben presenti nel coevo contesto interpretativo maturato a livello europeo ove, sin da allora, la Corte di giustizia aveva offerto una diversa lettura del divieto di *bis in idem* essenzialmente incentrata su un parametro, quello della complessiva adeguatezza del cumulo sanzionatorio, chiaramente ancorato al piano sostanziale della garanzia, più che a quello processuale. Emblematica di quest'orientamento è la sentenza *Åkerberg Fransson* resa, appena qualche mese prima dell'arreso

[40] Corte EDU, 4 marzo 2014, *Grande Stevens e altri c. Italia*, ricc. 18640/10, 18647/10, 18663/10, 18668/10 e 18698/10. Per un commento alla pronuncia, tra i numerosissimi contributi, si vedano: A. Alessandri, *Prime riflessioni sulla decisione della Corte Europea dei Diritti dell'Uomo riguardo alla disciplina degli abusi di mercato*, in *Giur. comm*., 2014, 855 ss.; D'Alessandro, *Tutela dei mercati finanziari e rispetto dei diritti umani fondamentali*, in *Dir pen. e proc*., 2014, 614 ss.; G. De Amicis, *"Ne bis in idem e"doppio binario" sanzionatorio: prime riflessioni sugli effetti della sentenza 'Grande Stevens' nell'ordinamento italiano*, in *Dir. pen. cont., Riv. trim.,* 3, 2014, 201 ss.; G. Flick - V. Napoleoni, *Cumulo tra sanzioni penali e amministrative: doppio binario o binario morto?*, *Riv. AIC*, 3, 2014, 1 ss.; M. Ventoruzzo, *Abusi di mercato, sanzioni Consob e diritti umani: il caso Grande Stevens e altri c. Italia*, in *Riv. soc*., 4, 2014, 693 ss.; F. Viganò, *Doppio binario sanzionatorio e ne bis in idem: verso una diretta applicazione dell'art. 50 della Carta? (a margine della sentenza Grande Stevens della Corte EDU),* in *Dir. pen. cont*., *Riv. trim.,* 3, 2014, 219 ss.

[41] Così, A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1048. In termini analoghi, tra gli altri, F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, in *Dir. pen. e proc*., 2018, 953.

[42] Segnatamente, l'illecito amministrativo di cui all'art. 187-*ter,* d.lgs. 24 febbraio 1998, n. 58, e il reato di manipolazione del mercato di cui all'art. 185, d.lgs. 24 febbraio 1998, n. 58.

[43] A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1062, da cui sono tratte le espressioni riportate nel testo.

[44] Orientamento interpretativo ribadito dalla Corte europea in successivi arresti riguardanti i sistemi di doppio binario tributario vigenti nell'ordinamento di paesi scandinavi, cfr. Corte EDU, 20 maggio 2014, *Nykänen c. Finlandia*, ric. 11828/2011; Corte EDU, 27 novembre 2014, *Luky Dev c. Svezia*, ric. 7356/2010; Corte EDU, 10 febbraio 2015, *Kiiveri c. Finlandia*, ric. 53753/12.

[45] In tal senso, M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario*", cit., 185, il quale, in questa prospettiva, sottolinea come «nessuna rilevanza […] veniva attribuita dalla Corte Europea alla presenza del meccanismo compensatorio dell'art. 187 *terdecies* del TUF, come a riconoscere il carattere inderogabile della garanzia del *ne bis in idem* "processuale"».

Grande Stevens, con riferimento al sistema di doppio binario tributario vigente nell'ordinamento svedese[46]. Con tale pronuncia, in estrema sintesi, la Corte di giustizia aveva ritenuto che la reiterazione di un procedimento sanzionatorio avente carattere punitivo nei confronti di chi, per il medesimo fatto, fosse stato già giudicato in modo definivo, fosse stata da ritenersi in linea di principio preclusa dalla garanzia di cui all'art. 50 della Carta, a patto che – ed è questo il decisivo elemento di novità[47] – le rimanenti sanzioni, vale a dire quelle applicate all'esito del procedimento già definito, fossero state in concreto «effettive, proporzionate e dissuasive»[48] rispetto agli obbiettivi di tutela perseguiti dal diritto dell'Unione. Detto altrimenti, per la Corte di Lussemburgo la mera previsione legislativa di sanzioni e procedimenti aventi natura punitiva per lo stesso fatto non avrebbe costituito, di per sé, automatica violazione del divieto di *bis in idem*, dipendendo tale valutazione dal giudizio sulla complessiva adeguatezza della risposta sanzionatoria applicata, sicché, qualora quest'ultima fosse stata da ritenersi inadeguata rispetto allo scopo di tutela, ben poteva ammettersi il cumulo. Un orientamento «efficientista»[49] foriero di una tutela debole accordata ad un principio, quello del *ne bis in idem*, declassato da garanzia di tipo processuale a mera garanzia di tipo sostanziale[50].

[46] CGUE, 26 febbraio 2013, *Åklagaren c. Hans Åkerberg Fransson,* C-617/10. La pronuncia conseguiva a un rinvio pregiudiziale operato dall'autorità giudiziaria svedese, con riferimento all'interpretazione dell'art. 50 CDFUE, nel contesto di un procedimento penale per frode fiscale instaurato nei confronti di un soggetto già condannato in via definitiva, per lo stesso fatto (inadempimento di obblighi dichiarativi e contributivi in materia di IVA), al pagamento di una sanzione tributaria. Per un commento alla pronuncia, cfr. S. Manacorda, *Dalle carte dei diritti a un diritto penale à la carte. Note a margine delle sentenze Fransson e Melloni della Corte di Giustizia*, in *Dir. pen. con*t., *Riv. trim*., 3, 2014, 247 ss.; E. Scaroina, *Costi e benefici del dialogo tra le Corti in materia penale*, in *Cass. pen*., 2015, 2926; D. Vozza, *I confini applicativi del principio del ne bis in idem interno in materia penale: un recente contributo della Corte di Giustizia dell'Unione Europea*, in *Dir. pen. cont*., *Riv. trim*., 3, 2013, 294 ss.

[47] In tal senso, A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1067, a giudizio del quale «il percorso interpretativo delle due Corti europee divergeva per addizione, nel senso che agli snodi argomentativi propri del Giudice di Strasburgo [Grande Stevens], fondamentalmente condivisi dal Giudice di Lussemburgo [Fransson], se ne aggiungeva per quest'ultimo un altro», quello della complessiva adeguatezza del trattamento sanzionatorio, «capace di rimettere tutto in discussione […] e di conservare l'assetto sanzionatorio originario in coerenza con gli obiettivi della politica eurounitaria, trasfusa nella scelta dello Stato membro».

[48] CGUE, 26 febbraio 2013, *Åklagaren c. Hans Åkerberg Fransson,* cit., § 36.

[49] F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 955, a giudizio del quale la pronuncia in esame si inscrive nel contesto di una giurisprudenza, quella della Corte di giustizia, spesso «non imparziale, *engagè* rispetto all'obiettivo di legittimare l'Unione come attore del dibattito politico-criminale europeo» ossia «alla tentazione di eliminare discipline nazionali ritenute disnomiche nel campo della tutela delle finanze comunitarie (*Taricco docet*)». In termini pressoché analoghi, M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, cit., 184, sottolinea «la decisiva "logica funzionalista" della Corte di Giustizia, da cui deriva la sostanziale subordinazione della garanzia del *ne bis in idem* al raggiungimento degli obiettivi perseguiti dal diritto dell'Unione».

[50] In termini critici rispetto all'orientamento della Corte di giustizia, ancora M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, cit., 184, il quale sottolinea come esso «si presta ad offrire un'impalcatura teorica di sostanziale legittimazione di tali meccanismi punitivi (come in effetti è stato), nonostante la previsione e il pieno riconoscimento del divieto di *bis in idem*»

2.1.2. (segue) Dalla sentenza *A e B c. Norvegia* alle pronunce *Garllson, Menci e Di Puma Zecca*

La divergenza di vedute che si profilava tra l'interpretazione «*maior*» (processuale) della Corte di Strasburgo, e quella «*minor*» (sostanziale) della Corte di Lussemburgo[51], avrebbe potuto e dovuto risolversi – almeno stando al principio di omogeneità delle tutele sancito dall'art. 52 § 3, della Carta dei diritti fondamentali[52] – accordando prevalenza al più elevato *standard* di tutela riconosciuto a livello convenzionale[53]. Il che, come da più parti è stato sottolineato, avrebbe avuto effetti a dir poco dirompenti nei singoli ordinamenti interni, compreso il nostro, strutturati secondo il familiare schema di doppio binario punitivo[54]. E, infatti, così non è stato: complici anche le pressioni provenienti da diversi governi europei, alla fine, la Corte Europea ha "mostrato la corda", ridimensionando il livello di tutela sino ad allora accordato al diritto al *ne bis in idem* processuale[55].

Il "cambio di rotta" è segnato dalla pronuncia resa nel 2016 nel caso *A e B c. Norvegia*, vero e proprio spartiacque quanto al modo di intendere e interpretare il divieto di *bis in idem* europeo[56]. Ridotta all'essenziale la sua *ratio decidendi* è la seguente: l'inizio o

[51] F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 952 ss., da cui sono tratte le espressioni riportate nel testo.

[52] L'art. 52 della Carta, come noto, da un lato (par. 1) definisce i requisiti che devono essere rispettati affinché i diritti e le libertà previsti possano subire legittime restrizioni (le limitazioni devono essere previste dalla legge, e rispettare oltre che il contenuto essenziale dei diritti e libertà, anche il principio di proporzionalità e necessarietà rispetto al perseguimento di finalità di interesse generale dell'Unione) e, dall'altro lato (par. 3) contiene la clausola orizzontale di salvaguardia rispetto ai diritti garantiti dalla CEDU, in forza della quale le garanzie di cui alla Carta non possono mai essere inferiori al corrispondente livello di tutela minimo garantito dalla CEDU, ma possono ovviamente collocarsi ad un livello superiore. Sul principio di omogeneità delle tutele di cui all'art. 52 della Carta, cfr. F. Ferraro - N. Lazzerini, *Art. 52,* in R. Mastroianni - O. Pollicino - S. Allegrezza - F. Pappalardo - O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, cit., 1061 ss.

[53] M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, cit., 185.

[54] In tal senso, anche per un quadro d'insieme delle reazioni della giurisprudenza interna successive alla Sentenza Grande Stevens, cfr. G. Angiolini, *Una questione ancora irrisolta: il principio di ne bis in idem europeo e l'Italia*, in *Riv. it. dir. proc. pen.* 4, 2018, 2109 ss.; A.F. Tripodi, *Corte europea dei diritti dell'uomo e sistemi sanzionatori in materia di abusi di mercato e di violazioni tributarie: la quiete dopo la tempesta?,* in *Le Società*, 1, 2018, 80 ss.

[55] Considerazione condivisa, sia pur con diversità d'accenti, dalla dottrina pressoché unanime. Cfr. M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, cit., 186, a giudizio del quale vi sarebbe stato un «sensibile ridimensionamento» della garanzia rispetto al livello di tutela che traspariva dalla sentenza Grande Stevens. F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 224, secondo cui, con la sentenza *A e B c. Norvegia*, la Corte europea ha compiuto un «passo indietro»; F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 953, evidenzia l'«innegabile ridimensionamento della tutela convenzionale» conseguente alla pronuncia *A e B* della Corte europea.

[56] Corte EDU, Grande Camera, 15 novembre 2016, *A e B c. Norvegia*, ricc. 24130/11 e 29758/11. Per un commento alla pronuncia, nell'amplissima letteratura, si rinvia a: M. Bontempelli, *Verso un adattamento della disciplina italiana delle sanzioni tributarie al diritto europeo?*, in *Rass. Trib.*, 2, 2017, 562 ss.; F. Cassibba, *Ne bis in idem e procedimenti paralleli*, in *Riv. it. dir. proc. pen.*, 2017, 351 ss.; G. De Amicis - P. Gaeta, *Il confine di sabbia: la Corte edu ancora di fronte al divieto del ne bis in idem*, in Cass. Pen., 2017, 469 ss. P. Fimiani, *Market abuse e doppio binario sanzionatorio dopo la sentenza della Corte E.D.U., Grande Camera, 15 novembre 2016, A e B c. Norvegia*, in *Dir. pen. cont.*, *Riv. trim.*, 2, 2017, 5 ss.; R. Rudoni, *Sul ne bis in idem convenzionale: le irriducibili aporie di una giurisprudenza casistica*, in *Quad. cost.*, 4, 2017, 825 ss.; L. Trucco, *Ne bis in idem: la Corte di*

la prosecuzione di un secondo procedimento di carattere sostanzialmente punitivo in relazione a un fatto per il quale una persona sia già stata giudicata in via definitiva nell'ambito di un diverso procedimento, pure di carattere sostanzialmente punitivo, non necessariamente dà luogo a una violazione del *ne bis in idem*, dovendosi escludere che ciò accada ogni qual volta tra i due procedimenti vi sia una «connessione sostanziale e temporale sufficientemente stretta»[57], così che essi rappresentino due facce della stessa medaglia, ossia una risposta coerente e sostanzialmente unitaria al medesimo illecito.

In sostanza, impregiudicate le consolidate certezza sull'*idem*, la Corte europea ha agito sul *bis*[58].

L'essenza del mutato indirizzo interpretativo risiede, infatti, nella compiuta teorizzazione del parametro della «*sufficiently close connection in substance and time*»[59], in virtù del quale si renderebbe ora possibile distinguere i «sistemi sanzionatori integrati» da quelli costituenti mere ipotesi di «reiterazione dell'accusa»[60]. Del resto, consapevole della portata innovativa del principio affermato[61], la Grande Camera non si è fermata al suo enunciato, ma ha cercato di offrirne una più rigorosa definizione attraverso l'analitica indicazione di una serie di parametri di giudizio utili a svolgere la verifica di sufficiente integrazione sostanziale e temporale tra i procedimenti. È stato così inaugurato un vero e proprio *stress test* – l'*A e B test* – in virtù del quale la sufficiente integrazione tra i procedimenti, sotto il profilo sostanziale, andrà valutata alla luce dei seguenti parametri[62]: *i)* la complementarietà degli obiettivi avuti di mira dai differenti procedimenti; *ii)* la prevedibilità *ex ante* del cumulo procedimentale; *iii)* la sussi-

Strasburgo scende a più miti ed ulteriori consigli, in *Quad. cost*., 1, 2017, 173 ss.; F. Viganò, *La Grande Camera della Corte di Strasburgo su ne bis in idem e doppio binario sanzionatorio*, in *Dir. pen. cont*., *on line*, 18 novembre 2016.

57 Corte EDU, Grande Camera, 15 novembre 2016, *A e B c. Norvegia,* cit. § 130.

58 A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1064.

59 Anche la *Guide on art. 4 of protocol n. 7 to the ECHR*, 15 ss., aggiornata a dicembre 2021, e reperibile sul sito della CEDU *echr.coe.int*, che chiarisce i diversi passaggi logici da affrontare per verificare se vi sia o meno una violazione della garanzia prevista dalla Convenzione, cita il *test* di connessione materiale e temporale come elemento necessario da esaminare per riscontrare il mancato rispetto del *ne bis in idem.*

60 Così, F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina (a cura di), *Il ne bis in idem*, cit., 224.

61 A tale ultimo proposito deve tuttavia precisarsi che, sebbene la Sentenza A e B sia stata percepita come un netto *revirement* rispetto al precedente orientamento interpretativo di cui alla sentenza Grande Stevens, il criterio della *close connection in substance and time* era già stato impiegato dalla Corte europea, in risalenti pronunce, quale parametro di giudizio essenziale per accertare o meno la violazione della garanzia convenzionale. Se ne trova una prima declinazione nella pronuncia Corte EDU, 30 maggio 2000, *R.T. c Svizzera*, ric. 31524/96. Successivamente, il criterio del nesso materiale e temporale riemerge nelle sentenze Corte EDU, 13 dicembre 2005, *Nilsson c. Svezia*, n. n. 73661/01; Corte EDU, 21 settembre 2006, *Maszni c. Romania*, ric. 59892/00. Così, ancora, nelle successive pronunce Corte EDU, 30 aprile 2015, *Kapetanios e altri c. Grecia*, ric. nn. 3453/12, 42941/12, 9028/13; Corte EDU, 9 giugno 2016, *Sismanidis e Sitaridis c. Grecia*, ric. nn. 66602/09 e 71879/12, nonché poco prima della sentenza *A e B*, Corte EDU, 4 ottobre 2016, *Rivard c. Svizzera*, ric. 1563/12. Per una più completa rassegna dell'evoluzione del criterio della *close connection*, nelle pronunce della Corte europea, si rinvia a L. Bin, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole,* cit. 104 ss.

62 Per una compiuta disamina dei singoli parametri di giudizio elaborati dalla Corte europea al fine di effettuare la verifica sulla sufficiente integrazione tra i procedimenti, si rinvia a L. Bin, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole,* cit., 116 ss.; A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1064 ss.

stenza di istituti di coordinamento processuale, specie sotto il profilo della raccolta e della valutazione del materiale probatorio, che consentano di contenere "per quanto possibile" gli oneri conseguenti al cumulo; *iv)* infine, e soprattutto, la previsione di un meccanismo compensatorio che consenta di tenere conto delle sanzioni già applicate nel primo procedimento, così da garantire la complessiva proporzionalità del trattamento sanzionatorio.[63] Per la verifica della *connection in time* - requisito che deve sussistere cumulativamente rispetto alla connection in *substance* – nella sentenza non sono indicati parametri particolari: la Corte europea si è limitata a precisare che, a tal fine, non è indispensabile che i due procedimenti avanzino a braccetto, ben potendo l'instaurazione dell'uno essere consecutiva a quella dell'altro purché, tuttavia, la loro durata complessiva non sia tale da esporre chi vi è sottoposto ad una perdurante incertezza circa la propria sorte[64].

Che, per effetto di tale pronuncia, la «forza normativa» del *ne bis in idem* processuale abbia subito un ridimensionamento appare un dato davvero inconfutabile[65].

Sia chiaro, la prospettiva di una tutela processuale non scompare, posto che di *bis in idem* è possibile parlare a condizione che, comunque, vi sia una duplicazione di procedimenti[66].

Semplicemente, ai fini del riconoscimento del divieto di doppio giudizio, può dirsi che ora (*post A e B*) il vero lavoro inizi nel punto esatto in cui prima (*post Grande Stevens*) terminava: non è più sufficiente fermarsi all'accertamento di un cumulo tra due procedimenti sanzionatori aventi entrambi carattere punitivo (*bis in idem*), ma, proprio ai fini della sussistenza di un *bis*, occorrerà anche verificare che gli stessi non siano tra loro connessi al punto da potersi considerare come «aspetti di un unico procedimento»[67], nel contesto di un (legittimo) sistema di «doppio binario cumulativo ma integrato»[68].

Verifica, quest'ultima da svolgersi facendo applicazione del *test di close conntection* secondo i criteri dettati dalla Corte europea: alcuni di essi si prestano ad una valutazione solo in concreto, altri anche in astratto; nell'ambito di questi ultimi, poi, alcuni si pongono come «recessivi», altri ancora come «preminenti»[69]. Il principale di essi

---

63 Corte EDU, Grande Camera, 15 novembre 2016, *A e B c. Norvegia,* cit., §§ 132, 133.

64 Ivi, § 134.

65 In questi termini, M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario*", cit., 199, a giudizio del quale «la garanzia risulta indebolita se si considera che la Grande Camera non solo ammette la deroga alla rigidità del divieto di bis in idem processuale, ma, soprattutto, offre una criteriologia indiziaria della sufficiente integrazione procedimentale dai contorni particolarmente flessibili, quindi facilmente riconoscibili (ed infatti puntualmente riconosciuti[…]) nella predisposizione legislativa del meccanismo di doppio binario».

66 Così, ad esempio, non può esservi violazione della garanzia del *ne bis in idem*, allorché vi sia una duplicazione di sanzioni disposte all'interno di un unico procedimento, v. in tal senso, Corte EDU, 12 aprile 2016, *Dungveckis c. Lituania*, ric. 32106/08, ove è stata esclusa la violazione dell'art. 4 prot. n. 7 CEDU nel caso di un cumulo di sanzioni, conseguenti al riconoscimento del concorso formale di reati, disposte nell'ambito di un unico procedimento.

67 A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1064.

68 L'espressione è di M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario*", cit., 186.

69 Lo rileva F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 956, secondo il quale «tra i preminenti […] compare la proporzionalità […] tra i recessivi è da inquadrare la prevedibilità».

– come segnalato dall'avverbio (*above all*) che lo introduce – senza dubbio è quello che fa riferimento alla proporzionalità del trattamento sanzionatorio.

È questo il punto: esso appartiene più alla logica propria della dimensione sostanziale del principio, posto che – come è stato osservato - «nessuno dei fondamenti della preclusione processuale è sotteso neanche in via mediata al canone della proporzionalità della sanzione»[70]. Detto altrimenti, se si assume il principio come garanzia di tipo processuale, allora il riferimento al canone della proporzionalità della sanzione appare un fuor d'opera. Non per caso, in dottrina, è stata messo in evidenza il pericolo di uno «sviamento»[71], di una «contaminazione»[72], di un l'«ibridazione concettuale»[73], se non di una vera e propria «trasfigurazione»[74] del *ne bis in idem*, a voler sottolineare – quantomeno in astratto – l'«ingerenza del volto sostanziale nella […] dimensione processuale»[75], di un principio che, da «assoluto e inderogabile nella sua dimensione garantistica astratta viene convertito in una prescrizione fondata su requisiti variamente declinabili»[76].

In concreto, tuttavia, appare chiaro che la prospettiva di una reale tutela del principio processuale dipenderà molto, dal modo di svolgere la verifica sulla connessione materiale e temporale tra i due procedimenti e, in particolare, dall'incidenza accordata ai diversi parametri di giudizio: tanto più tale verifica sarà condotta facendo riferimento – esclusivo o preminente – alla proporzionalità delle sanzioni, quanto più evidente sarà «la transizione del principio del *ne bis in idem* da meccanismo di garanzia verso il processo a tutela nei confronti della sanzione indebita»[77]. Per contro tanto più effettiva risulterà la tutela accordata alla garanzia processuale quanto più, nello svolgimento dell'*A e B test*, verranno presi in considerazione gli altri parametri di giudizio e, tra questi, in modo particolare, quello che fa riferimento alla complementarità di scopo in modo da evitare che il cumulo possa comportare oneri ecces-

In termini analoghi, F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 229.

[70] Così F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 225.

[71] A. Vallini, *Tracce di "ne bis in idem" sostanziale lungo i percorsi disegnati dalle Corti*, in *Dir. pen. e proc.*, 4, 2018, 525 ss.

[72] F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 953.

[73] L. Baron, *Test di proporzionalità e ne bis in idem. La giurisprudenza interna alla prova delle indicazioni euroconvenzionali in materia di market abuse*", in *Arch. pen.*, *on line*, 3, 2019, 1 ss.

[74] E. Basile, *Il doppio binario sanzionatorio degli abusi di mercato in Italia e la trasfigurazione del ne bis in idem europeo*, in *Giur. comm.*, 2018, 139 ss. Analogamente, A. Gaito, *La progressiva trasfigurazione del ne bis in idem*, cit.

[75] A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1074. In questo senso, valorizzando il riferimento al canone della proporzionalità del trattamento sanzionatorio, è stato rilevato come la Corte europea, con la pronuncia A e B si sia adeguata alla prospettiva funzionalista o efficientista della Corte di giustizia, così, M.C Carta, *Il principio del ne bis in idem nell'art. 50 della Carta dei diritti fondamentali UE e nella recente giurisprudenza della Corte di giustizia*, cit., 9; analogamente, F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 955.

[76] S. Seminara, *Il divieto di bis in idem: un istituto inquieto*, cit., 1384.

[77] F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 953. In senso analogo, tra gli altri, F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 228.

sivamente gravosi per l'accusato[78].

Proprio quest'ultima, almeno stando alle decisioni sino ad ora valutabili, pare essere la prospettiva interpretativa seguita dalla Corte di Strasburgo la quale, nelle occasioni in cui è stata chiamata a misurarsi con la legittimità dei sistemi punitivi di doppio binario vigenti negli ordinamenti interni, in diversi casi ha riscontrato la violazione della garanzia convenzionale facendo un applicazione seria e completa dell'*A e B test*[79]: nella maggior parte dei casi, valorizzando l'assenza della interconnessione temporale[80], sebbene anche sul piano della connessione materiale, la Corte ha censurato l'assenza della complementarietà dei fini, o il difetto di un sufficiente coordinamento processuale, ancorché – preme sottolinearlo – fossero previsti meccanismi di compensazione del cumulo punitivo, tali da garantirne la proporzionalità complessiva[81].

Insomma, le pronunce immediatamente successive alla sentenza *A e B* non sembrano legittimare i timori della prima ora, legati al pericolo di un eccessivo arretramento del *ne bis in idem* processuale. Il dato che si ricava da tali pronunce, infatti, è che tutti i parametri indiziari definiti nell'*A e B* test debbano egualmente concorrere ai fini del giudizio di connessione tra i procedimenti e che, per contro, il difetto anche di uno solo tra essi, apra la strada alla violazione della garanzia[82].

Coglie nel segno, allora, chi ha giustamente definito «fin troppo avventata l'affermazione […] secondo cui nella stessa prospettiva convenzionale la garanzia del *ne bis in idem* avrebbe ormai natura meramente sostanziale»[83]: è la stessa Corte Edu[84], del resto, ad avere espressamente precisato come il discorso sul *ne bis in idem* non possa ridursi al giudizio di proporzionalità complessiva del trattamento sanzionatorio, ad

---

[78] In tal senso, F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina (a cura di), *Il ne bis in idem*, cit., 229, il quale sottolinea come, per contro, «non dovrebbe rilevare più di tato il criterio cronologico […] né evidentemente quello della prevedibilità della sottoposizione a duplice procedimento (requisito dettato semmai dal principio di legalità)».

[79] Per una panoramica delle decisioni della Corte europea successive alla pronuncia *A e B*, si veda M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, cit., 186.

[80] Cfr., Corte EDU, 18 maggio 2017, *Jóhannesson e altri c. Islanda*, ric. 11828/11, con nota di F. Viganò, *Una nuova sentenza di Strasburgo su ne bis in idem e reati tributari",* in *Dir. pen. cont.*, *on line*, 22 maggio 2017; Corte EDU, 16 aprile 2019, *Bjarni Armannsson c. Islanda*, ric. 72098/14, con nota di A. Galluccio, *Non solo proporzione della pena: la Corte Edu ancora sul bis in idem*, in *Dir. pen. cont.*, *on line*, 7 maggio 2019; Corte EDU, 6 giugno 2019, *Nodet c. Francia,* ric. 47342/14 con nota di M. Scoletta, *Il ne bis in idem "preso sul serio": la Corte EDU sulla illegittimità del doppio binario francese in materia di abusi di mercato (e i possibili riflessi nell'ordinamento italiano)*, in *Dir. pen. cont.*, *on line*, 17 giugno 2019. Più recentemente, cfr. Corte EDU, 21 luglio 2020, *Velkov c. Bulgaria*, ric. 34503/10, con nota di N. Madia, *Ne bis in idem europeo e illeciti da "stadio"*, in *Dir. comp.*, *on line*, 19 ottobre 2020; Corte EDU, 31 agosto 2021, *Bragi Gudmundur Kristjánsson c. Islanda*, ric. 12951/18.

[81] Cfr., Corte EDU, 6 giugno 2019, *Nodet c. Francia*, cit.; Corte EDU, 8 luglio 2019, *Mihalache c. Romania,* ric. 54012/10 con nota di A. Careri*, I presupposti della garanzia convenzionale al ne bis in idem: dalla Grande Camera nuove precisazioni,* in *Sist. Pen., on line, 12 dicembre 2019*; Corte EDU, 6 aprile 2021, *Tsonyo Tsonev c. Bulgaria*, cit., Corte EDU, 21 luglio 2020, *Velkov c. Bulgaria,* cit.; Corte EDU, 31 agosto 202, *Milošević c. Croazia.*

[82] Tra gli altri, lo evidenziano A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1070, nonché F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 956.

[83] F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 228.

[84] Cfr., in particolare, Corte EDU, 6 giugno 2019, *Nodet c. Francia*, cit.; Corte EDU, 8 luglio 2019, *Mihalache c. Romania,* cit.

ulteriore riprova del fatto che – quantomeno a livello convenzionale – la garanzia processuale, per quanto attenuata, continui a trovare tutela effettiva[85].
Diversamente a dirsi a livello euro unitario ove il divieto di *bis in idem* continua a trovare tutela essenzialmente circoscritta al piano sostanziale, ovvero come «congegno volto a prevenire la manifesta sproporzione della risposta sanzionatoria»[86].
Con le tre note sentenze rese nei casi *Garlsson Real Estate*, *Menci* e *Di Puma-Zecca*[87] – rispettivamente concernenti la compatibilità con il diritto dell'Unione del sistema di doppio binario italiano vigente in materia finanziaria e tributaria – la Corte di giustizia solo formalmente ha colto l'occasione per un riallineamento della propria posizione al mutato indirizzo interpretativo della Corte Europea, rimanendo sostanzialmente ancorata sulle proprie posizioni efficientiste, cui si è già fatto riferimento[88].
Le tre decisioni richiamate muovono tutte, infatti, da una comune premessa di fondo: il principio del *ne bis in idem* sancito dall'art. 50 della Carta può legittimamente subire restrizioni purché siano rispettati i fondamentali requisiti previsti dal successivo art. 52 il quale, a sua volta, da un lato richiede che le limitazioni siano previste dalla legge e rispettose del contenuto essenziale del diritto e, dall'altro, impone il rispetto del principio di proporzionalità e adeguatezza delle limitazioni rispetto al perseguimenti di finalità di interesse generale[89]. Nello svolgimento di tale giudizio, ancorché condotto al metro dei parametri di cui all'art. 52 della Carta, la Corte di Lussemburgo non ha fatto che riprendere – parafrasandola – la criteriologia indiziaria compiutamente definita nella pronuncia *A e B* per l'accertamento della connessione materiale e temporale tra i procedimenti, finendo così – quantomeno in astratto – per tratteggiare le stesse condizioni di legittimità dei sistemi di doppio binario cumulativi ma integrati[90]. In concreto, tuttavia, ci si avvede agevolmente come non vi sia affatto,

[85] È quanto sottolineato da A. Galluccio, *Non solo proporzione della pena: la Corte Edu ancora sul bis in idem*, cit.: «Che la pena in concreto inflitta risulti proporzionata alla gravità dell'illecito compiuto (…) è un requisito necessario per evitare il bis in idem, ma non sufficiente».

[86] F. Consulich, *Il prisma del ne bis in idem nelle mani del Giudice eurounitario*, cit., 956.

[87] CGUE, Grande Sezione, 20 marzo 2018, *Menci*, C-524/15; CGUE, Grande Sezione, 20 marzo 2018, *Garlsson Real Estate c. Consob*, C-537/16; CGUE, Grande Sezione, 20 marzo 2018, *Di Puma e Zecca c. Consob*, C-596/16, C-597/16. Per un commento di tali decisioni, cfr. E. Bindi, *Divieto di bis in idem e doppio binario sanzionatorio nel dialogo tra giudici nazionali e sovranazionali*, in *Federalismi.it*, 2018; F. Consulich - C. Genoni, *L'insostenibile leggerezza del ne bis in idem. Le sorti del divieto di doppio giudizio e doppia punizione, tra diritto eurounitario e convenzionale*, in *Giur. pen. web*, 22 aprile 2018; A. Galluccio, *La grande sezione della corte di giustizia si pronuncia sulle attese questioni pregiudiziali in materia di bis in idem,* in *Dir. pen. cont., on line,* 21 marzo 2018; B. Nascimebene, *Il divieto di bis in idem nella elaborazione della Corte di giustizia dell'Unione europea*, in *Sist. Pen*., *Riv. trim.*, 4, 2020, 95 ss.; G. B. Varesano, *Il diritto al ne bis in idem e il doppio binario sanzionatorio: alcune riflessioni a margine della sentenza Garlsson Real Estate*, in *Dir. um. e dir. internaz.*, 2018, 711; N. Recchia, *Note minime sulle tre recenti sentenze della Corte di giustizia dell'Unione europea in materia di bis in idem*, in *eurojus.it.*

[88] Cfr. *supra*, § 2.1.1. Il riferimento è alla pronuncia *Åkerberg Fransson.*

[89] Sull'indicazione dei requisiti che rendono legittima la deroga all'art. 50 della Carta, tratteggiati in termini pressoché identici nelle tre sentenze, cfr. CGUE, Grande Sezione, 20 marzo 2018, *Menci,* §24, nonché §§ 49,52,53 e 55. Per un commento all'art. 52, par. 1, cfr. F. Ferraro - N. Lazzerini, *Art. 52* in R. Mastroianni - O. Pollicino - S. Allegrezza - F. Pappalardo - O. Razzolini (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, cit., 1061 ss.

[90] Sulla sostanziale ricezione dell'*A e B test* da parte della Corte di giustizia, che tuttavia ha interpretato in modo particolarmente debole la criteriologia indiziaria della stretta connessione procedimentale, cfr. M. Scoletta, *Abusi di mercato e ne bis in idem: il doppio binario (e la legalità della pena) alla mercé degli interpreti*, cit.,

tra le due Corti, unanimità di vedute quanto al modo di intendere e interpretare la funzionalità del principio. I giudici di Lussemburgo, infatti, nello svolgere il *test* di *close connection* hanno seguito un approccio decisamente più formalistico, quasi tautologico[91], finendo per appiattirsi – ed è questo il decisivo elemento che continua a marcare il differente livello di tutela accordato al principio sul versante euro unitario - esclusivamente sul requisito della proporzionalità complessiva del trattamento sanzionatorio[92]. In questi termini, pertanto, non appare affatto azzardato concludere nel senso che la Corte di giustizia non si sia discostata poi tanto dal suo pregresso, tradizionale orientamento incline a valorizzare il piano sostanziale del divieto di *bis in idem*: nella prospettiva euro unitaria, infatti, il limite alla reiterazione di procedimenti sanzionatori resta subordinato ad un giudizio di adeguatezza – sebbene ora declinata in termini di proporzionalità (art. 52 CDFUE) – del cumulo di sanzioni rispetto al perseguimento degli interesse comunitari[93].

3. La sentenza costituzionale n. 149/2022: l'ordinanza di rimessione

La questione di legittimità costituzionale trae origine dalla pervicace ordinanza di remissione[94] sollevata dal Tribunale ordinario di Verona nell'ambito di un giudizio in

533 ss., nonché Id., *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, cit., 187. In argomento, per una diversa lettura, cfr. altresì, B. Nascimebene, *Il divieto di bis in idem nella elaborazione della Corte di giustizia dell'Unione europea*, cit., 99 ss.
(2019a), 533 ss.

[91] In tale senso, già M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, cit., 198.

[92] L'assoluta centralità assunta dal requisito della proporzione della sanzione, rispetto agli altri parametri di giudizio – quali, ad esempio, le finalità complementari tra i procedimenti e il loro reciproco coordinamento – è sottolineata, tra gli altri, da N. Recchia, *Note minime sulle tre recenti sentenze della Corte di giustizia dell'Unione europea in materia di bis in idem*, cit., nonché E. Basile, *Il doppio binario sanzionatorio degli "abusi di mercato" in Italia e la trasfigurazione del ne bis in idem europeo*, cit., 139. In proposito, cfr. altresì F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 225, a giudizio del quale «se davvero si intende valutare l'osservanza di tale garanzia sulla base di un giudizio di sola proporzione del trattamento sanzionatorio, viene da chiedersi se non sia allora più sincero affermare che essa semplicemente non opera al di fuori del processo penale *stictu sensu* penale». La centralità del requisito della proporzionalità del trattamento sanzionatorio, peraltro, ha trovato ulteriore conferma nella più recente sentenza Corte Giut. UE, 8 marzo 2022, *BV*, C-205/20, resa con riferimento al sistema di doppio binario tributario vigente nell'ordinamento francese. In tale pronuncia, che sollevava problematiche pressoché analoghe a quelle affrontate nel caso Menci, la Corte di giustizia ha riscontrato la violazione del divieto di *bis in idem* soffermandosi esclusivamente sul requisito della proporzionalità complessiva del trattamento sanzionatorio, senza neppure prendere in considerazione gli ulteriori parametri di giudizio. Cfr., per un maggior approfondimento, J. Della Valentina, *Il paradigma del ne bis in idem tra proporzionalità assorbente, rinnovata concezione processuale e overlapping protection. Osservazioni a margine di Corte cost., sent. n. 149/2022*, in *Sist. Pen.*, *on line*, 24 novembre 2022, 9 ss.

[93] Cfr. in tal senso M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario"*, cit., 188 ss., secondo cui «per come concretizzata nell'argomentazione della Corte di Lussemburgo, la garanzia del ne bis in idem assume una dimensione soprattutto teorica, ma ancora difficilmente azionabile allo scopo di sindacare e censurare in concreto i meccanismi di doppio binario presenti negli ordinamenti nazionali, he facilmente possono essere ricondotti al modello punitivo "proporzionato" e "necessario" ad assicurare gli obiettivi di tutela».

[94] Ordinanza n. 152 del 17 giugno 2021, pubblicata in Gazzetta Ufficiale, 1ª Serie Speciale - Corte

cui, a seguito di opposizione a decreto penale di condanna, il remittente si trovava a giudicare della responsabilità penale dell'imputato in ordine al delitto di cui all'art. 171 *ter*, c. 1, lett. b) della legge n. 633/1941[95] «perché, fuori dal caso di uso personale, a fini di lucro deteneva per la vendita e abusivamente riproduceva opere letterarie fotocopiate oltre il limite consentito presso la copisteria [...] di cui è titolare»[96].

Condotta in relazione alla quale – come rilevato dal Giudice *a quo* – lo stesso imputato era già stato sottoposto ad un precedente procedimento amministrativo per l'illecito di cui all'art. 174 *ter* della medesima legge n. 633/1941[97], definitivamente conclusosi con l'irrogazione della sanzione pecuniaria d'importo pari a € 5.974[98].

In tale contesto, ritenuta l'identità del fatto materiale posto a base dei due procedimenti, in uno con la natura sostanzialmente punitiva della sanzione prevista dall'art. 174 *ter* della legge sul diritto d'autore, il Giudice *a quo*, all'esito di attenta verifica condotta in base ai parametri di giudizio indicati nella sentenza A e B, rilevava altresì la reciproca autonomia dei due procedimenti. Per tutte queste ragioni, quindi, revocava in dubbio la legittimità costituzionale del sistema di doppio binario prefigurato dalle disposizioni vigenti in materia di diritto d'autore, per violazione dell'art. 117, c. 1, Cost. in relazione all'art. 4 del Protocollo n. 7 della CEDU, nell'interpretazione da ultimo offertane dalla Corte di Strasburgo, con la sentenza *A e B*.

Come già in altre occasioni, anche il tal caso il remittente non appuntava le proprie censure sulla coesistenza e la concreta applicabilità delle due disposizioni sanzionatorie, bensì sulla specifica norma che recepisce nell'ordinamento interno il divieto di *bis in idem* processuale – l'art. 649 c.p.p. – censurata nella parte in cui, limitando il divieto di doppio giudizio ai soli casi di giudicato penale formatosi sul medesimo fatto, la disposizione non troverebbe applicazione con riferimento a tutta la "materia penale", non consentendo di estendere la garanzia a tutte le innumerevoli situazioni di doppio binario – tra cui, per appunto, quello in materia di diritto d'autore – che determinano il cumulo, rispetto ad uno stesso fatto, di procedimenti sanzionatori a

Costituzionale, n. 41 del 13 ottobre 2021, 43 ss.

[95] Legge 22 aprile 1941, n. 633, recante "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio". L'art. 171 *ter* - previsto nella Sezione IIª (*Difese e sanzioni penali*), del Capo III° (*Difese e sanzioni giudiziarie*), del Titolo III° (*Disposizioni comuni*) delle citata legge – punisce «se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro: […] b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati […]»

[96] Ordinanza n. 152 del 17 giugno 2021, cit.

[97] Cfr. l. 633/1941, art. 174-*bis* «1. Ferme le sanzioni penali applicabili, la violazione delle disposizioni previste nella presente sezione è punita con la sanzione amministrativa pecuniaria pari al doppio del prezzo di mercato dell'opera o del supporto oggetto della violazione, in misura comunque non inferiore a euro 103,00. Se il prezzo non è facilmente determinabile, la violazione è punita con la sanzione amministrativa da euro 103,00 a euro 1032,00. La sanzione amministrativa si applica nella misura stabilita per ogni violazione e per ogni esemplare abusivamente duplicato o riprodotto».

[98] Importo determinato - secondo i criteri indicati dall'art. 174 *bis*, l. 633/1941 - in misura pari al doppio della sanzione minima prevista per i venticinque libri di testo di prezzo non determinabile (25 x 103 euro x 2) e ad un terzo dell'importo massimo previsto per le opere il cui prezzo di vendita era conosciuto (15 x 103 =1545,00/3).

carattere punitivo appartenenti a diversi ambito del diritto (amministrativo e penale). In definitiva, proprio l'impossibilità di estendere in via interpretativa l'ambito operativo della garanzia di cui all'art. 649 c.p.p. anche ai casi di doppio binario c.d. penale amministrativo[99], è ciò che ha indotto ad eccepire l'incostituzionalità dell'art. 649 c.p.p. posto che, secondo il giudice remittente, solo un intervento additivo su tale disposizione sarebbe stato in grado di neutralizzare la duplicazione dei giudizi e scongiurare la lesione del diritto fondamentale dell'imputato a non essere giudicato due volte per il medesimo fatto.

3.1. (segue) La decisione della Corte

A fronte di una questione così prospettata, in primo luogo, il Giudice costituzionale ha avvertito l'esigenza di definire meglio, e in maniera più puntuale, i limiti del proprio potere decisionale.
In tal senso, dopo aver respinto la nutrita serie di eccezioni preliminari d'inammissibilità[100], la Corte non ha perso occasione di constatare che, nonostante la questione di legittimità costituzionale della norma impugnata fosse stata formulata in termini "ampi" dal giudice remittente[101], un'accurata lettura della parte motiva dell'ordinanza di rimessione, interamente incentrata sul peculiare sistema sanzionatorio vigente in materia di tutela del diritto d'autore, avrebbe consentito di circoscrivere le censure del remittente «con specifico riferimento al regime di doppio binario sanzionatorio previsto in materia di tutela del diritto d'autore», e non anche rispetto «a tutte le variegate altre ipotesi in cui, nel nostro ordinamento, sono disciplinati regimi di doppio binario sanzionatorio per i medesimi illeciti»[102].
Sicché, alla luce di tale premessa la Corte ha avuto buon gioco di richiamare il proprio consolidato orientamento secondo cui «l'oggetto del giudizio costituzionale deve essere individuato interpretando il dispositivo dell'ordinanza di rimessione alla luce della sua motivazione»[103], per giungere a delimitare il *thema decidendum* «come mirante unicamente a estendere la disciplina di cui all'art. 649 cod. proc. pen. all'ipotesi

[99] A sostegno di tale conclusione, nell'ordinanza di rimessione il Giudice *a quo* richiama il consolidato orientamento della giurisprudenza di legittimità secondo cui «gli strumenti preventivi e riparatori che compongono il quadro sistematico all'interno del quale si colloca la disciplina di cui all'art. 649 del codice procedura penale presuppongono tutti la comune riferibilità dei più procedimenti per il medesimo fatto all'autorità giudiziaria penale: è dunque tale quadro sistematico, in uno con la considerazione del tenore letterale della disposizione codicistica, che preclude un'interpretazione di quest'ultima che ne estenda l'ambito applicativo a sanzioni irrogate l'una dal giudice penale, l'altra da un'autorità amministrativa», cfr. Cass. pen., sez. V, 15 gennaio 2015, n. 1782.

[100] Corte cost., 16 giugno 2022, n. 149, cit., §§ 2, 3 del 'considerato in diritto'.

[101] Tali, cioè, da estendere la portata operativa dell'art. 649 c.p.p. «a tutti i casi in cui, con riguardo ad uno stesso fatto, sia stata già irrogata in via definitiva, nell'ambito di un procedimento amministrativo non legato a quello penale da un legame materiale e temporale sufficientemente stretto, una sanzione avente carattere sostanzialmente penale ai sensi della [CEDU] e dei relativi protocolli», Cfr., Corte cost., 16 giugno 2022, n. 149, cit., § 4 del 'considerato in diritto'.

[102] *Ibidem*.

[103] Così, *ex multiis*, Corte cost., 4 marzo 2019, n. 33, in *Foro amm.*, 2020, 1676.

in cui l'imputato di uno dei delitti previsti dall'art. 171-ter della legge n. 633 del 1941 sia già stato sottoposto in via definitiva a sanzione amministrativa per il medesimo fatto ai sensi dell'art. 174-bis della medesima legge»[104].

È in questi termini, in parte diversi e certamente meno ampi rispetto al *petitum* formulato dal remittente, che la questione di legittimità costituzionale è stata accolta: la Corte ha infatti dichiarato costituzionalmente illegittimo l'art. 649 c.p.p. «nella parte in cui non prevede che il giudice pronunci sentenza di proscioglimento o di non luogo a procedere nei confronti di un imputato per uno dei delitti previsti dall'art. 171-*ter* della legge 22 aprile 1941, n. 633 (…), che, in relazione al medesimo fatto, sia già stato sottoposto a procedimento, definitivamente conclusosi, per l'illecito amministrativo di cui all'art. 174-*bis* della medesima legge».

Senza sottovalutare l'importanza del risultato, tuttavia, merita sottolineare il percorso argomentativo seguito dal Giudice delle leggi per giungere a decretare l'incostituzionalità dello specifico sistema normativo di doppio binario oggetto di scrutinio. La motivazione della sentenza, in alcuni passaggi sovrapponibile a quella dell'ordinanza di rimessione, è interamente incentrata sull'autonoma lettura del divieto di *bis in idem* offerta dalla Corte europea, di cui, non a caso, sono richiamati in premessa i principali orientamenti interpretativi, sia per ciò attiene ai presupposti operativi della garanzia[105], sia, e soprattutto, per ciò riguarda l'ulteriore, inedita condizione di compatibilità dei sistemi punitivi di doppio binario puntivi delineata a partire dalla nota sentenza *A e B. c. Norvegia*.[106]

Sotto quest'ultimo aspetto, anzi, non vi è alcun dubbio che la Corte costituzionale abbia assunto il paradigma della *close connection in substance and time*, con l'annessa criteriologia indiziaria definita dalla Corte europea, quale fondamentale punto di riferimento per risolvere la questione sottoposta al suo esame. Con una ulteriore e fondamentale precisazione, inerente al "metodo" di giudizio: prima di entrare nel merito del giudizio di fondatezza, infatti, il Giudice costituzionale ha ritenuto di precisare che, dei differenti parametri di giudizio delineati nella sentenza *A e B* per svolgere la verifica di *close connection in substance and time*, avrebbe preso in considerazione solo quelli che si prestano ad una valutazione di carattere "astratto", coerentemente con la peculiare logica del giudizio innanzi alla Corte, «il cui compito non è quello di verificare la sussistenza di violazioni del diritto fondamentale in esame nel singolo caso concreto, bensì quello di stabilire se il meccanismo normativo disegnato dal legislatore sia tale da determinare violazioni di tale diritto fondamentale in un numero

[104] Corte cost., 16 giugno 2022, n. 149, cit., § 4 del 'considerato in diritto'.

[105] Corte cost., 16 giugno 2022, n. 149, cit., § 5.1.2. del 'considerato in diritto', ove, con specifico riferimento al requisito dell'*idem factum*, la Corte richiama l'ormai consolidato orientamento della giurisprudenza europea che, «a partire almeno dalla sentenza della grande camera del 10 febbraio 2009, *Zolotoukhine contro Russia* (§§ 79-84), identifica nei medesimi fatti materiali sui quali si fondano le due accuse penali, indipendentemente dalla loro eventuale diversa qualificazione giuridica». Con riferimento al requisito del *bis*, ovvero alla valutazione circa la natura sostanzialmente penale dei due procedimenti, nel successivo § 5.1.3, la Corte richiama i «noti criteri *Engel*, da tempo utilizzati dalla Corte EDU per fissare il perimetro applicativo della "materia penale" ai fini degli artt. 6 e 7 della Convenzione».

[106] Cfr., Corte cost., 16 giugno 2022, n. 149, cit., § 5.1.3 del 'considerato in diritto'.

indeterminato di casi»[107].

Facendo in larga proprie le considerazioni già svolte dal Giudice remittente, sul punto, la Corte ha ravvisato la sussistenza sia dell'*idem* che del *bis*: l'uno – la medesimezza del fatto materiale posto a base delle sanzioni penali e amministrative di cui, rispettivamente, agli artt. 171 *ter* e 174 *bis* – desumibile dalla clausola di apertura dell'art. 174 *bis* («ferme le sanzioni penali»), la quale renderebbe non equivoca la «volontà del legislatore di cumulare in capo al medesimo trasgressore le due tipologie di sanzioni» destinate a riflettersi in altrettanti «procedimenti […] che si sviluppano parallelamente o consecutivamente nei confronti del loro autore»[108]; l'altro – il cumulo tra procedimenti sanzionatori aventi entrambi carattere punitivo – reso manifesto dalle modalità di determinazione della sanzione amministrativa pecuniaria di cui all'art. 174 *bis*, la cui entità renderebbe ragione della sua «funzione accentuatamente dissuasiva […] in tutto e per tutto sovrapponibile a quella caratteristica delle sanzioni penali»[109].

Sgomberato il campo da possibili equivoci in ordine all'effettiva sussistenza di un *bis in idem*, la Corte costituzionale si è quindi occupata dell' ulteriore, necessaria verifica che definisce in concreto i limiti di tollerabilità dei sistemi di doppio binario punitivo: quella volta ad appurare se i due procedimenti finalizzati all'irrogazione delle sanzioni punitive di cui agli artt. 171 *bis* e 174 *ter* l. 633/1941, «possano ritenersi avvinti da una connessione sostanziale e temporale sufficientemente stretta», tale da poterli considerare «come parti di un unico sistema integrato di tutela dei medesimi beni giuridici, insuscettibile di produrre effetti sproporzionati sui diritti fondamentali dell'interessato»[110]. Perché – ha chiosato la Corte – è solo in tale ultima eventualità che «il sistema di "doppio binario" disegnato dal legislatore non risulterebbe di per sé incompatibile con l'art. 4 Prot. n. 7 CEDU e, conseguentemente, con l'art. 117, primo comma, Cost.»[111].

Sennonché anche l'*A e B test* ha dato esito negativo.

---

[107] *Ibidem.*

[108] Ivi, § 5.2.1. e § 5.2.2. del 'considerato in diritto', ove, ad ulteriore sostegno del giudizio sulla medesimezza dei fatti materiali posti a base delle disposizioni normative, la Corte sottolinea come «il mero richiamo compiuto dall'art. 174-*bis* della legge n. 633 del 1941 alle «violazioni previste nella presente sezione», e dunque anche a quelle contemplate come delitto dall'art. 171-*ter*, rende gli ambiti dei due illeciti – quello amministrativo e quello penale – in larga misura sovrapponibili». La medesimezza del fatto posto a base degli artt. 171 *bis* e 174 *ter,* l. 633/1941 e, quindi, l'applicazione "cumulativa" delle procedure sanzionatorie, trova conferma nella giurisprudenza di legittimità, cfr. Cass. Civ., sez. II, 18 dicembre 2017, n. 30319, secondo cui l'art. 174-bis, «ha inteso assicurare l'effettività della risposta sanzionatoria per la protezione del diritto d'autore, configurando come illecito amministrativo le stesse condotte che integrano fattispecie autonome di reato».

[109] Cfr., Corte cost., 16 giugno 2022, n. 149, cit., § 5.2.2. del 'considerato in diritto', ove, in particolare, ai fini della valutazione circa la natura sostanzialmente penale della sanzione amministrativa di cui all'art. 174 bis la Corte rileva come le sue modalità di determinazione siano tali «da infliggere al trasgressore un sacrificio economico superiore al profitto ricavato dall'illecito». D'altra parte, la funzione accentuatamente dissuasiva della sanzione – ad avviso della Corte – trova conferma nel disegno di legge A.S. 1496, poi sfociato nella legge n. 248 del 2000 alla quale si dovette l'introduzione dell'art. 174-bis, nella parte in cui si «sottolinea come l'obiettivo perseguito dalla novella fosse quello di incrementare il grado di dissuasività delle misure di contrasto alle violazioni del diritto d'autore, attraverso sanzioni amministrative «che appaiono dotate di autonoma deterrenza in quanto rapidamente applicabili».

[110] Cfr., Corte cost., 16 giugno 2022, n. 149, cit., § 5.2.3. del 'considerato in diritto'.

[111] *Ibidem.*

Tra i diversi parametri di giudizio, infatti, l'unico di cui la Corte ha riconosciuto la sussistenza è quello che fa leva prevedibilità della duplicazione procedimentale e sanzionatoria. Per il resto, il Giudice costituzionale ha rilevato l'assenza di tutti gli ulteriori requisiti sintomatici della sufficiente integrazione procedimentale.

In primo luogo, la Corte ha sottolineato che, nel caso di specie «non può ritenersi che i due procedimenti perseguano scopi complementari o concernano aspetti diversi della medesima condotta illecita», posto che, da un lato entrambe le norme di cui agli artt. 171 *bis* e 174 ter perseguono lo scopo di «dissuadere i potenziali autori dal commettere gli illeciti in parola» e, d'altra parte, le condotte punite sono esattamente le stesse non presentando diversità tali da poter giustificare il cumulo sanzionatorio e procedimentale[112].

In secondo luogo, con riferimento ai profili di coordinamento processuale, il Giudice costituzionale si è limitato a rilevare l'assenza di «alcun meccanismo atto a evitare duplicazioni nella raccolta e nella valutazione delle prove, e ad assicurare una ragionevole coordinazione temporale dei procedimenti»[113].

Infine, anche sotto il profilo della proporzionalità[114] complessiva del trattamento sanzionatorio, l'esito negativo del giudizio è dipeso dalla presa d'atto che il sistema normativo prefigurato dalla legge n. 633/1941 non contempla «alcun meccanismo che consenta al giudice penale (ovvero all'autorità amministrativa in caso di formazione anticipata del giudicato penale) di tenere conto della sanzione già irrogata ai fini della commisurazione della pena, in modo da evitare che una medesima condotta sia punita in modo sproporzionato»[115].

Per inciso: si noti come nella prospettiva del giudicante l'esito negativo dell'*A e B test* è dipeso esclusivamente dal vaglio dei profili di connessione materiale, senza nessuna considerazione rispetto ad eventuali profili di interconnessione temporale. Una circostanza, quest'ultima, che si spiega in ragione del fatto che, il requisito della *connection in time*, prestandosi esclusivamente ad una valutazione di tipo contingente e strettamente dipendente dal caso concreto, diviene parametro di giudizio pressoché ininfluente rispetto alla precipua finalità del giudizio costituzionale che – come si è detto – è quella di accertare "in astratto" la compatibilità strutturale dei sistemi normativi di doppio binario rispetto al vincolo costituzionale e convenzionale del *ne bis in idem*.

È proprio in quest'ottica di giudizio che, constatata assenza di tutti gli indici sintomatici della *close connection in substance*, la Corte ha finito per censurare il sistema di

---

[112] A tale ultimo proposito, in particolare, la Corte sottolinea come non si nemmeno «previsto, come tipicamente avviene nella materia tributaria, un sistema di soglie in grado di selezionare le sole condotte che per la loro gravità appaiano meritevoli anche della sanzione penale», cfr. Corte cost., 16 giugno 2022, n. 149, cit., § 5.2.3. del 'considerato in diritto'.

[113] *Ibidem.*

[114] Rispetto alla proporzionalità «come oggetto di accertamento da parte del giudice, reso così custode e garante di un sistema privo di base legale in ordine ai limiti della pena», v. le preziose considerazioni di S. Seminara, *Il divieto di* bis in idem: *un istituto inquieto*, cit., 1391.

[115] Cfr. Corte cost., 16 giugno 2022, n. 149, cit., § 5.2.3. del 'considerato in diritto'.

"doppio binario" prefigurato dalla legge in materia di tutela del diritto d'autore, il quale non appare normativamente strutturato in modo da «assicurare che i due procedimenti sanzionatori previsti apprestino una risposta coerente e sostanzialmente unitaria agli illeciti in materia di violazioni del diritto d'autore», […] atteso che essi «originano dalla medesima condotta, ma seguono poi percorsi autonomi, che non si intersecano né si coordinano reciprocamente in alcun modo, creando così inevitabilmente le condizioni per il verificarsi di violazioni sistemiche del diritto al ne bis in idem»[116].

Di qui l'accoglimento della questione, attraverso una sentenza additiva il cui effetto è sostanzialmente quello di estendere la portata della garanzia di cui all'art. 649 c.p.p. esclusivamente ai rapporti tra gli illeciti di cui alla legge 633/1941 e, in particolare, al solo caso in cui un soggetto, imputato del reato di cui all'art. 171 *ter*, sia già stato sottoposto ad un procedimento amministrativo definitivamente conclusosi per l'illecito di cui all'art. 174 *bis* della medesima legge[117].

Una soluzione che, peraltro, la stessa Corte costituzionale riconosce essere "parziale" rispetto alla necessità di garantire adeguata tutela al divieto di *bis in idem* nella specifica materia oggetto di scrutinio.

Ciò, sotto due distinti profili. Anzitutto perché la soluzione di risulta, valendo limitatamente alle sole ipotesi in cui il procedimento penale segua il giudicato amministrativo, non consente di estendere la portata del divieto di doppio giudizio all'ipotesi inversa in cui il procedimento amministrativo segua il giudicato penale[118].

In secondo luogo, perché il rimedio apprestato non è «idoneo di per sé a conferire razionalità complessiva al sistema, che consente comunque l'apertura di due procedimenti e il loro svolgimento parallelo, con conseguente duplicazione in capo all'interessato dei costi personali ed economici»[119].

Ecco che allora, con i dovuti distinguo, la Corte non si è discostata poi tanto dall'ormai consueta tecnica "monitoria" già sperimenta in altre occasioni[120]: il consueto in-

[116] *Ibidem.*

[117] Ivi, § 6 del 'considerato in diritto'.

[118] Ivi, § 7 del 'considerato in diritto'. «Questa Corte è, peraltro, consapevole che tale rimedio non è idoneo a evitare tutte le possibili violazioni del diritto al ne bis in idem fisiologicamente create dalla legge n. 633 del 1941, in particolare nell'ipotesi inversa in cui l'autore della violazione sia stato già definitivamente giudicato per uno dei delitti di cui all'art. 171-ter della legge, e sia successivamente sottoposto a procedimento amministrativo ai sensi dell'art. 174-bis.».

[119] *Ibidem.*

[120] Ci si riferisce alla tecnica "monitoria" cui la Corte costituzionale ha fatto ricorso dapprima, nel 2018, in materia di suicidio assistito, (Corte cost 16 novembre 2018, n. 207, in *Giur. cost.*, 2018, 2459 ss., con nota di V. Anzon Demmig, *Un nuovo tipo di decisione di "incostituzionalità accertata ma non dichiarata"*), successivamente, nel 2020, sulla questione c.d. delle pene detentive per i giornalisti responsabili del delitto di diffamazione aggravato dall'uso del mezzo stampa (Corte cost, 26 giugno 2020, n. 132, in *Giur. cost*, 2020, 1457 ss., con commento di N. Recchia, *La previsione della pena detentiva per la diffamazione del giornalista: la Corte costituzionale ripropone la tecnica decisoria del caso Cappato*, 1480 ss.) e, da ultimo, in materia di ergastolo c.d. "ostativo" (Corte cost., ord. 11 maggio 2021, n. 97, in *Giur. Cost.*, 2021, 1169 ss., con nota di A. Pugiotto, *Leggere altrimenti l'ord. n. 97 del 2021 in tema di ergastolo ostativo alla liberazione condizionale*, *ivi*, 1213 ss., nonché, volendo, S. Lonati, *Verso il tramonto dell'ostatività penitenziaria: un'attesa lunga trent'anni,* in *Arch. pen.*, *on line*, 2, 2022). In sintesi, tale tecnica decisoria consente alla Corte di accertare i profili d'illegittimità della normativa sottoposta a scrutinio, senza dichiararne formalmente l'incostituzionalità, al fine di consentire al legislatore di adottare *medio tempore* una nuova disciplina della materia, che tenga

vito alla collaborazione istituzionale rivolto al legislatore, questa volta, è stato quello di «rimodulare la disciplina in esame in modo da assicurare un adeguato coordinamento tra le sue previsioni procedimentali e sanzionatorie, nel quadro di un'auspicabile rimeditazione complessiva dei vigenti sistemi di doppio binario sanzionatorio alla luce dei principi enunciati dalla Corte EDU, dalla Corte di giustizia e da questa stessa Corte»[121].

4. Le "due direttrici fondamentali" della pronuncia: l'adesione alla logica processuale del *ne bis in idem*

Un'approfondita lettura della sentenza consente di cogliere le due direttrici fondamentali lungo le quali si è complessivamente articolato il ragionamento della Corte: l'una corrispondente alla dimensione più innovativa della pronuncia, l'altra di carattere dichiaratamente compromissorio.

La prima emerge leggendo l'intera parte motiva della sentenza dalla quale traspare l'incondizionata adesione alla logica processuale del *ne bis in idem*, secondo l'orientamento inaugurato dalla sentenza *A e B* e, poi, ulteriormente affinato nelle successive pronunce della Corte europea.

La seconda, invece, si può cogliere leggendo il dispositivo della pronuncia dal quale traspare la cautela che, di fatto, ha indotto la Corte a limitare l'effetto additivo della pronuncia al solo sistema di doppio binario in materia di diritto d'autore.

Iniziando dalla prima dimensione, il luogo della sentenza in cui risulta meglio argomentata l'adesione alla logica processuale del diritto al *ne bis in idem*, risiede nella parte in cui ha trovato spazio l'illustrazione delle premesse argomentative al giudizio di fondatezza: lì dove la Corte ha espressamente riconosciuto che «la garanzia convenzionale in parola mira […] a tutelare l'imputato non solo contro la prospettiva dell'inflizione di una seconda pena, ma ancor prima contro la prospettiva di subire un secondo processo per il medesimo fatto: e ciò a prescindere dall'esito del primo processo, che potrebbe anche essersi concluso con un'assoluzione»[122].

L'*overruling* rispetto ai suoi precedenti è indiscutibile e, sotto questo aspetto, certamente può dirsi che la sentenza costituisca un traguardo quantomeno inaspettato[123].

conto delle segnalate frizioni rispetto alla costituzione. Per un commento sull'inedita tecnica decisoria recentemente adottata della Corte costituzionale, tra gli altri, cfr. G. Ruotolo, *L'evoluzione delle tecniche decisorie della Corte costituzionale nel giudizio in via incidentale. Per un inquadramento dell'ord. n. 207 del 2018 in un nuovo contesto giurisprudenziale*, in *Rivista AIC*, 26 giugno 2019, 644 ss. P. Veronesi, *Un'altra incostituzionalità "prospettata" ma non (ancora) dichiarata: la diffamazione a mezzo stampa nell'ord. n. 132 del 2020*, in *Studium Iuris*, 2020, 1359 ss; V. Carucci, *Prove tecniche di collaborazione istituzionale: commento all'ordinanza n. 97 del 2021 della Corte costituzionale*, in *Riv. Corte conti*, 2021, 225 ss.

[121] Cfr., Corte cost., 16 giugno 2022, n. 149, cit., § 7 del 'considerato in diritto'.

[122] Ivi, § 5.1.1. del 'considerato in diritto'.

[123] In tal senso, J. Della Valentina, *Il paradigma del ne bis in idem tra proporzionalità assorbente, rinnovata concezione processuale e overlapping protection. Osservazioni a margine di Corte cost., sent. n. 149/2022*, cit., 3, a giudizio del quale si è trattato di «una pronuncia – per certi versi – inattesa, considerata la tendenza giurisprudenziale degli ultimi anni». Sottolinea il «cambio di rotta» rispetto al passato e, in particolare alla sentenza n. 43/2018., M. Scoletta, *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del*

Basti considerare che nella pronuncia n. 43 del 2018 la Corte sottolineava «il carattere innovativo che la regola della sentenza *A e B contro Norvegia* ha impresso in ambito convenzionale al divieto di *bis in idem* […]» nel senso di rimarcarne il passaggio «dal divieto imposto agli Stati aderenti di configurare per lo stesso fatto illecito due procedimenti che si concludono indipendentemente l'uno dall'altro, alla facoltà di coordinare nel tempo e nell'oggetto tali procedimenti, in modo che essi possano reputarsi nella sostanza come preordinati a un'unica, prevedibile e non sproporzionata risposta punitiva, avuto specialmente riguardo all'entità della pena (in senso convenzionale) complessivamente irrogata»[124]. In sostanza, ponendo l'accento sul parametro della complessiva proporzionalità del trattamento sanzionatorio – non a caso definito come il «criterio eminente per affermare o negare il legame materiale» tra i due procedimenti – la Corte poneva le premesse per confinare la portata della garanzia al piano sostanziale, ossia, come principio volto a garantire la non manifesta sproporzione della risposta sanzionatoria[125].

Ora, *re melius perspecta*, il Giudice costituzionale sposta il baricentro del ragionamento sul piano processuale della garanzia, da intendersi «non quale principio "ordinamentale" a valenza oggettiva, funzionale alla certezza dei rapporti giuridici, ma quale diritto fondamentale della persona», la cui funzione primaria – si legge nella sentenza – è «quella di evitare l'ulteriore sofferenza, e i costi economici, determinati da un nuovo processo in relazione a fatti per i quali quella persona sia già stata giudicata»[126]. L'idea di fondo, dunque, torna ad essere quella di un principio funzionale a garantire l'individuo dalla prospettiva di subire la "pena" di un doppio giudizio, prima, più ed oltre che quella derivante da una doppia sanzione[127].

A dispetto degli enunciati formali, tuttavia, deve sottolinearsi come la Corte non abbia inteso portare sino alle estreme conseguenze le proprie premesse argomentative, aderendo ad una logica processuale pura e incondizionata del *ne bis in idem*, quale, ad esempio, sarebbe stata quella di un divieto inderogabilmente connesso – a mo' di *Grande Stevens* – alla mera presa d'atto della definitività di uno dei due procedimenti punitivi aventi ad oggetto lo stesso fatto[128]. La prospettiva, invece, è rimasta ancorata

doppio binario punitivo in materia di diritto d'autore, cit., 6.

[124] Corte cost., 2 marzo 2018, n. 43, cit., § 7 del 'considerato in diritto'.

[125] In tal senso, *ibidem*, la Corte rilevava come, per effetto della sentenza A e B, il *ne bis in idem* convenzionale avrebbe cessato «di agire quale regola inderogabile conseguente alla sola presa d'atto circa la definitività del primo procedimento […] perché in presenza di una "close connection" è permesso proseguire nel nuovo giudizio ad onta della definizione dell'altro» non potendosi continuare a sostenere il carattere «esclusivamente processuale» della garanzia.

[126] Ivi, § 5.1.1. del 'considerato in diritto'.

[127] In tal senso, v. S. Seminara, *Il divieto di bis in idem: un istituto inquieto*, cit., 1393, secondo il quale «spostando radicalmente l'asse del problema dai criteri di accertamento alla ratio del principio» la Corte «ha il merito di restituire il ne bis in idem al suo rango di diritto fondamentale della persona, per sua natura suscettibile di temperamenti solo in forza di cogenti interessi superiori».

[128] Come sottolineato da J. Della Valentina, *Il paradigma del ne bis in idem tra proporzionalità assorbente, rinnovata concezione processuale e overlapping protection. Osservazioni a margine di Corte cost., sent. n. 149/2022*, cit., 18, «non pare infondato ritenere che se la Corte avesse inteso sviluppare sino in fondo le delimitazioni categoriali assunte nelle premesse argomentative, a rigore si sarebbe dovuti pervenire ad una soluzione analoga all'orientamento Grande Stevens, per il quale – si ricorderà – il ne bis in idem veniva concepito secondo una logica prettamente processuale e, pertanto, scevro da ogni contaminazione 'sostanzializzante'».

ad una tutela processuale che può definirsi relativa o attenuata, perché contaminata alla base dal riferimento al *test* di *close connection* e, soprattutto, al requisito sostanziale della proporzionalità del trattamento sanzionatorio[129]. Eppure, anche entro questo diverso modo di definire e inquadrare la garanzia processuale attenuata, il Giudice costituzionale ha posto le premesse per affrancare la tutela del diritto al *ne bis idem* dalla logica assorbente della proporzionalità sanzionatoria[130], affermando a chiare lettere che quest'ultima è garanzia fondata su basi giuridiche distinte da quelle su cui si fonda il diritto al *ne bis in idem*[131].

Del resto, ben oltre le premesse argomentative, che la logica processuale del *ne bis in idem* – ancorché relativa o attenuata – abbia costituito il vero e proprio *leit motive* della sentenza[132], è un dato che si ricava soprattutto dal modo in cui la Corte ha svolto l'*A e B test*.

Il rischio tangibile, sotto tale ultimo aspetto, era quello di dar luogo ad una sorta di "scollamento" tra le premesse argomentative e la loro concreta applicazione, quale sarebbe stato quello derivante da un approccio "formalistico" al giudizio di *close connection*, essenzialmente incentrato sull'unico parametro di valutazione, quello della proporzionalità del complessivo trattamento sanzionatorio, del tutto indifferente rispetto alle fondamenta processuali del *ne bis in idem*.

Niente di tutto ciò, anzi, l'esatto opposto.

Nel vagliare la sufficiente integrazione tra i due procedimenti sanzionatori prefigurati dalla normativa sottoposta a scrutino, il Giudice costituzionale ha fatto un applicazione scrupolosa dell'*A e B test* prendendo in adeguata considerazione, attraverso argomentazioni reali e non meramente apparenti, tutti i parametri di giudizio – ulteriori rispetto a quello della proporzionalità del trattamento sanzionatorio – e relativi

[129] Sul punto, S. Seminara, *Il divieto di bis in idem: un istituto inquieto*, cit., 1394, secondo il quale «la spiegazione più semplice» del richiamo all'orientamento interpretativo inaugurato dalla sentenza *A e B*, apparentemente contraddittorio rispetto alle premesse argomentative, «potrebbe consistere nel "vincolo" costituito dall'interpretazione dei giudici europei, al quale la nostra Corte ha ritenuto di conformarsi». In senso analogo, cfr. J. Della Valentina, *Il paradigma del ne bis in idem tra proporzionalità assorbente, rinnovata concezione processuale e overlapping protection. Osservazioni a margine di Corte cost., sent. n. 149/2022*, cit., 18 a giudizio del quale si tratta di una cautela «comprensibile» atteso che «la riaffermazione di una logica squisitamente processuale del *ne bis in idem* si sarebbe infatti posta in aperto contrasto con una giurisprudenza ormai consolidata a livello sovranazionale – dal revirement *A e B c. Norvegia* in poi –, oltre a far dubitare della legittimità costituzionale di qualsiasi ipotesi di doppio binario processuale esistente all'interno dell'ordinamento».

[130] Si rinvia, in tal senso, alle autorevoli osservazioni di S. Seminara, *Il divieto di bis in idem: un istituto inquieto*, cit., 1394 ss.

[131] Corte cost., 16 giugno 2022, n. 149, cit., § 5.1.1. del 'considerato in diritto' «Il ne bis in idem non si oppone, invece, alla possibilità che l'imputato sia sottoposto, in esito a un medesimo procedimento, a due o più sanzioni distinte per il medesimo fatto (ad esempio, a pene detentive, pecuniarie e interdittive), ferma la diversa garanzia rappresentata dalla proporzionalità della pena: garanzia, quest'ultima, fondata su basi giuridiche distinte da quelle su cui si fonda il diritto al ne bis in idem (in particolare, sugli artt. 3 e 27 Cost. a livello interno, e sull'art. 49, paragrafo 3, CDFUE a livello unionale)».

[132] Significativo, in tal senso, appare anche il fatto che, nel far propria l'adesione alla logica processuale attenuata della garanzia, la Corte non abbia inteso soffermarsi – se non in un brevissimo passaggio argomentativo (cfr. Corte cost., 16 giugno 2022, n. 149, cit., § 5.1.1. del 'considerato in diritto') – sul diverso orientamento fatto proprio dalla Corte di giustizia la quale – come si è detto – continua proporre una lettura del divieto di bis in idem essenzialmente legata alla complessiva proporzionalità del trattamento sanzionatorio e, dunque, circoscritta al piano sostanziale della garanzia.

alla prevedibilità del cumulo punitivo, alla complementarietà degli scopi e al relativo coordinamento processuale[133]. Un approccio, quest'ultimo, che si pone in linea di continuità con le pronunce della Corte europea[134] e che, al tempo stesso, segna la marcata distanza dall'impostazione «funzionalista» della Corte di giustizia[135] la quale – di fatto – continua a ridurre la valutazione del *ne bis in idem* a mero giudizio sulla proporzionalità complessiva del cumulo sanzionatorio[136].

Insomma, dalla sentenza in commento possono trarsi due indicazioni di massima, da tenere ben presenti nell'eventualità (tutt'altro che remota) in cui analoghe questioni di legittimità costituzionale possano tornare ad occupare i banchi della Consulta.

La prima: il Giudice costituzionale, in astratto, ha accolto un'interpretazione del *ne bis in idem* come principio operante sul piano processuale, ancorché secondo una prospettiva di tutela attenuata dal rifermento al paradigma della sufficiente connessione materiale e, in particolare, al parametro sostanziale della proporzionalità complessiva del trattamento sanzionatorio.

La seconda: in concreto, nello svolgimento del *test* di sufficiente integrazione procedimentale, la Corte ha dissipato ogni dubbio in merito a possibili contaminazioni sostanziali della garanzia, rispristinando la sua più autentica vocazione processuale.

Indicazioni di massima che, ben vedere, la Corte ha inteso rivolgere in prima battuta direttamente al legislatore, il quale – anche sul presupposto della rilevata inadeguatezza della soluzione normativa di risulta[137] – è stato chiamato ad un'auspicabile opera di rimeditazione complessiva dei sistemi di doppio binario punitivo attualmente vigenti in numerosi e variegati settori dell'ordinamento interno. Non vi è chi non veda come proprio il "monito" finale della sentenza costituisce l'ennesima e, se possibile, definitiva dimostrazione del fatto che la Corte costituzionale abbia inteso riconsegnare «il principio del ne bis in idem alla [sua] dimensione processuale», restituendogli «la funzione di garanzia di diritti fondamentali della persona»[138].

4.1. (segue) Il limitato effetto additivo della sentenza di accoglimento

L'adesione alla logica processuale del divieto *bis in idem* non ha comunque impedito alla Corte di contenere gli effetti della pronuncia al solo sistema di doppio binario

[133] Corte cost., 16 giugno 2022, n. 149, cit., § 5.2.3. del 'considerato in diritto'.

[134] Cfr. *supra*, § 2.1.2, spec. note 81, 82.

[135] Cfr. *supra*, § 2.1.2, spec. note 88, 93.

[136] Sottolinea quest'aspetto M. Scoletta, *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario punitivo in materia di diritto d'autore*, cit., 9, a giudizio del quale, «molto opportunamente, pertanto, nella sentenza qui in esame la Corte costituzionale prende le distanze da siffatta tendenza riduttiva della garanzia, dimostrando la limitatezza di tale approccio: la proporzionalità è solo "uno" degli indici che può essere valorizzato al fine di valutare il carattere integrato di un doppio binario sanzionatorio (la *close connection in substance*), *ex se* autonomamente inidoneo a legittimare i cumuli di procedimenti punitivi sullo stesso fatto illecito».

[137] Cfr. *supra*, § 3.1.

[138] In questi termini, S. Seminara, *Il divieto di bis in idem: un istituto inquieto,* cit., 1396.

vigente in materia di diritto d'autore.

Una soluzione che si presta a differenti valutazioni.

Sul piano formale, essa può dirsi soluzione, se non necessitata, quantomeno giustificata. L'esito decisorio della sentenza, infatti, trae le proprie premesse giuridiche nella preliminare opera di ridefinizione del *petitum* che la Corte ha operato al precipuo scopo di porre in chiaro, sin da subito, quale fosse il *thema decidendum*, e quali i limiti del proprio potere decisionale[139]. Sotto tale aspetto, dunque, ancorché limitato, l'esito decisorio appare giuridicamente ineccepibile.

Sul piano della sostanza, non di meno, il dispositivo della sentenza tradisce un certo *self restraint*. Diversamente da quanto le era stato chiesto, infatti, la Corte non ha inteso apportare una modifica di sistema, attraverso un intervento strutturale sull'art. 649 c.p.p. il cui effetto additivo sarebbe stato quello di estendere la portata applicativa della garanzia «a tutti i casi in cui, con riguardo ad uno stesso fatto, sia stata già irrogata in via definitiva, nell'ambito di un procedimento amministrativo non legato a quello penale da un legame materiale e temporale sufficientemente stretto, una sanzione avente carattere sostanzialmente penale ai sensi della [CEDU] e dei relativi protocolli»[140]. Una soluzione di questo genere, generalizzando la portata operativa del divieto di doppio giudizio indistintamente rispetto a tutte le ipotesi di doppio binario penale e amministrativo, avrebbe avuto l'effetto di conferire al giudice ordinario l'arduo compito di accertare i presupposti operativi della garanzia e di svolgere autonomamente l'*A e B test*. Piuttosto, consapevole delle marcate differenze correnti nella disciplina dei regimi di doppio binario vigenti nell'ordinamento interno[141], la Corte ha preferito mantenersi entro il perimetro di un giudizio casistico, limitato cioè alla specifica disciplina oggetto di censura: di essa sono stati vagliati gli specifici profili d'incompatibilità con la garanzia del *ne bis in idem*, e solo rispetto ad essa è stata estesa la garanzia processuale di cui all'art. 649 c.p.p.

Ciò, peraltro, non esclude che le importanti affermazioni di principio enunciate nel testo della sentenza possano essere riproposte per prospettare l'incostituzionalità degli altri sistemi punitivi di doppio binario, attualmente previsti in diversi settori del nostro ordinamento e, almeno formalmente, non interessati dagli effetti additivi della sentenza n. 149/2022[142]. Anzi, sotto quest'ultimo aspetto, appare ragionevole ipotizzare che – non diversamente da quanto accaduto in altre occasioni[143] – dalla

[139] Corte cost., 16 giugno 2022, n. 149, cit., § 4 del 'considerato in diritto'.

[140] *Ibidem*.

[141] In tal senso, M. Scoletta, *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario punitivo in materia di diritto d'autore*, cit., 5 ss., spec. nota 9, sottolinea come l'interesse della Corte sia stato quello di «delegare ai giudici ordinari la delicata valutazione relativa alla sussistenza degli incerti presupposti applicativi del divieto (costituzionale) del secondo giudizio».

[142] Come rilevato da S. Seminara, *Il divieto di bis in idem: un istituto inquieto,* cit., 1395 ss., la pronuncia della Corte costituzionale, sebbene limitata alla specifica questione sottopostale, «elabora un'interpretazione del principio […] valida per tutte le situazioni di duplicazione dei procedimenti con essa incompatibili già in astratto» sicché «il nostro giudice delle leggi presto si troverà dinanzi a questioni di legittimità che rivendicheranno una coerente applicazione dei principi ora enunciati». In senso analogo, J. Della Valentina, *Il paradigma del ne bis in idem tra proporzionalità assorbente, rinnovata concezione processuale e overlapping protection. Osservazioni a margine di Corte cost., sent. n. 149/2022*, cit., 23.

[143] Il parallelismo, ancorché si tratti di una materia affatto diversa da quella in esame, è riferito alle

sentenza sul diritto d'autore possa scaturire una sorta di "effetto domino", attraverso la proposizione di tante altre questioni di legittimità costituzionale, quanti sono i modelli punitivi strutturati secondo lo schema del «doppio binario cumulativo»[144].
Ecco, allora, l'interrogativo che ci si pone: se – in considerazione della portata della pronuncia in commento – i principi generali in essa affermati siano o meno in grado di rimettere in discussione la legittimità strutturale dei sistemi doppio binario.
Ipotizzare i possibili scenari futuri, in una materia complessa e in continuo divenire qual è quella oggetto d'analisi, non è compito semplice. Conviene quindi limitarsi ad alcuni punti fermi.
Il primo è che nella sentenza sul diritto d'autore la Corte si è trovata al cospetto di un regime di doppio binario sanzionatorio strutturato secondo caratteristiche tali da renderlo *ictu oculi* incompatibile con il diritto al *ne bis in idem* convenzionale[145]: basti pensare che la legge n. 633/1941 non prevede alcun sistema di coordinamento processuale, né un meccanismo che consenta al giudice penale di "tener conto" della sanzione comminata all'esito del procedimento già definito. Breve: nel caso di specie, è stato relativamente semplice constatare la reciproca autonomia dei due procedimenti. Il che, del resto, rende ragione di una sentenza ben motivata ma, tutto sommato, concisa.
Di qui, il secondo punto certo è che, nell'eventualità in cui la Corte costituzionale sarà chiamata a giudicare della legittimità costituzionale e convenzionale di altri sistemi di doppio binario – primi tra tutti quelli vigenti in materia tributaria[146] e finan-

vicende che hanno interessato la disciplina della custodia cutelare in carcere di cui l'art. 275, c. 3, c.p.p., norma che a partire dal *leading* case del 2010 (Corte cost., 21 luglio 2010, n. 265, in *Giur cost.*, 2010, 3169 ss) - e poi con le altre declaratorie seriali d'illegittimità costituzionale (Corte cost., 12 maggio 2011, n. 164, in *Giur. cost.*, 2011, 3169; Corte cost., 22 luglio 2011, n. 231, in *Giur. cost.*, 2011, 2950; Corte cost. 16 dicembre 2011, n. 331, in *Giur. cost.*, 2011, 4554; Corte cost., 3 maggio 2012, n. 110, in *Dir. pen. e proc.*, 2012, 985 ss.; Corte cost., 29 marzo 2013, n. 57, in *Giur. cost.*, 2010, 863; Corte cost., 18 luglio 2013, n. 213, in *Dir. & Giust.*, 2013, 995; Corte cost., 23 luglio 2013, n. 232, in *Dir. pen. e proc.,* 2014, 430 ss.; Corte cost., 26 marzo 2015, n. 48, in *Giur. cost.*, 968 ss.) – è stata dichiarata incostituzionale nella parte in cui, con riguardo alle ipotesi criminose che venivano di volta in volta in considerazione, prevedeva una presunzione assoluta, anziché relativa, di adeguatezza della custodia cautelare in carcere.

144 L'espressione, in contrapposizione a quella di «sistemi di doppio binario alternativo», è impiegata da A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1056, per indicare quei sistemi di doppio binario sanzionatorio che pongono i maggiori problemi di compatibilità con il divieto di bis in idem in quanto caratterizzati dalla «convergenza», per espressa previsione di legge, di entrambe le sanzioni rispetto al medesimo fatto.

145 In senso analogo, J. Della Valentina, *Il paradigma del ne bis in idem tra proporzionalità assorbente, rinnovata concezione processuale e overlapping protection. Osservazioni a margine di Corte cost., sent. n. 149/2022*, cit., 19, spec. nota 83.

146 In ambito tributario, come noto, la configurazione del sistema di doppio binario discende dalla coesistenza delle sanzioni penali e amministrative rispettivamente previste dal d.lgs. 10 marzo 2000 n. 74, e dal d.lgs. 18 dicembre 1997 n. 471. In tale settore, tuttavia, deve darsi conto del fatto che la scelta di fondo del legislatore sia stata quella di riservare al diritto penale (d.lgs. 74/2000) la repressione degli illeciti più gravi, prevalentemente concernenti gli obblighi di dichiarazione e autoliquidazione dell'imposta dovuta – con un giudizio di gravità essenzialmente incentrato sul superamento di determinate soglie quantitative – lasciando al sistema delle sanzioni amministrative (art. 13, d.lgs. 471/1997) il contrasto alle violazioni meno gravi. Tale scelta, coerente con l'intenzione di dar luogo ad un doppio binario alternativo (e non cumulativo), ha trovato confronto nella previsione del criterio di specialità di cui all'art. 19 del d.lgs. 74/2000 («Quando uno stesso fatto è punito da una delle disposizioni del titolo II e da una disposizione che prevede una sanzione amministrativa, si applica la disposizione speciale»)

ziaria[147] – il suo compito sarà meno agevole di quanto lo sia stato nella sentenza sul diritto d'autore[148]. A tale ultimo proposito, infatti, non può passare inosservato che «quando il legislatore ha intenzionalmente previsto e regolamentato sistemi a doppio binario […] (come nel caso, appunto, dei doppi binari in materia finanziaria e tributaria) ha contestualmente disciplinato una qualche forma di collegamento tra autorità procedenti nella fase di accertamento del fatto, preoccupandosi altresì di predisporre meccanismi che impedissero o almeno temperassero il cumulo punitivo secco tra le sanzioni irrogati all'esito dei due procedimenti»[149].

Ebbene, ancorché si tratti di conclusioni opinabili, la semplice previsione norma-

volto proprio ad evitare il rischio di una possibile sovrapposizione tra i due binari punitivi. In concreto, tuttavia, il rischio di dar luogo ad un sistema di doppio binario cumulativo (e non alternativo) non è stato evitato posto che, a partire dalle note "sentenze gemelle" delle Sezioni Unite (Cass. pen., sez. un., 28 marzo 2013, n. 37425 e 28 marzo 2013 n. 37424, rispettivamente riguardanti i reati di omesso versamento di ritenute e di omesso versamento dell'IVA) la giurisprudenza di legittimità (Cass. pen., sez. III, 8 aprile 2014, n. 20266), si è mostrata restia a guardare oltre i limiti insiti nel criterio di "specialità in astratto", ricostruendo il rapporto tra fattispecie penali (artt. 10 *bis* e 10 *ter*, d.lgs. 74/2000) e amministrative (art. 13, d.lgs. 471/1997) in termini di progressione criminosa, con la conseguenza di ammettere pacificamente il concorso tra sanzioni e procedimenti penali e amministrativi. Per una compiuta analisi del sistema di doppio binario tributario italiano, si vedano: A. Ingrassia, *Ragione fiscale vs 'illecito penale personale'*, Milano, 2016; E.M. Mancuso, *Ne bis in idem e giustizia sovrannazionale*, A. Giarda - G. Varraso - A. Perini (a cura di) *La nuova giustizia penale tributaria*, Padova, 2016, 533 ss.; A.F. Tripodi, *Ne bis in idem e reati tributari*, in A. Cadoppi - S. Canestrari - A. Manna - M. Papa (a cura di), *Diritto penale dell'economia*, vol. I°, Torino, 2017, 684 ss.

[147] L'apparato punitivo delineato per gli abusi di mercato dal T.U.F. (d.lgs. 24 febbraio 1998 n. 58 e succ. mod.), come noto, è costituito da un sistema integrato di sanzioni amministrative e penali. Nel recepire la direttiva 2003/6/Ce, con la riforma del 2005 (l. 18 aprile 2005, n. 62) il legislatore italiano ha «elaborato un microcosmo normativo dove alle fattispecie penali di *market abuse* (artt. 184 e 185 t.u.f.), si affiancano delle fattispecie a rilevanza amministrativa (artt. 187 bis e 187 *ter* t.u.f.), le quali si pongono in un rapporto di coincidenza oggettiva pressoché completa con le prime; da ciò ne è derivata l'applicazione di un sistema sanzionatorio penale e amministrativo insieme, ispirato a un meccanismo cumulativo», così F. Mazzacuva - E. Amati, *Doppio binario sanzionatorio" e ne bis in idem*, in Id., *Diritto penale dell'economia*, IV ed., Milano, 2019, 351. In questi termini, allora, può dirsi che - diversamente da quanto avviene in ambito tributario - nel settore del *market abuse* il sistema di doppio binario cumulativo rappresenti «il frutto di una precisa scelta legislativa, che emerge anzitutto dalla clausola di riserva "salve le sanzioni penali" con cui esordiscono, all'esito della riforma del 2005, le fattispecie di illecito amministrativo di cui agli artt. 187-bis e 187 ter t.u.f.», così F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 206 Per un maggior approfondimento sul sistema di doppio binario in materia di *market abuse*, tra gli altri, si vedano: A. Alessandri, *Attività d'impresa e responsabilità penali*, in *Riv. it. dir. proc. pen*., 2005, 555 ss.; Id., *Prime riflessioni sulla decisione della Corte europea dei diritti dell'uomo riguardo alla disciplina italiana degli abusi di mercato*, in *Giur. comm*., 2014, 864 ss.; F. D'Alessandro, *Tutela dei mercati finanziari e rispetto dei diritti umani fondamentali*, in *Dir. pen. proc*., 2014, 614 ss.; M. Scoletta, *Doppio binario sanzionatorio e ne bis in idem nella nuova disciplina eurounitaria degli abusi di mercato*, in *Le Società*, 2016, 218 ss.

[148] Cfr., in senso analogo, S. Seminara, *Il divieto di bis in idem: un istituto inquieto,* cit., 1394 ss., al quale si rinvia soprattutto per l'indicazione dei possibili interventi legislativi che, in ambito tributario e finanziario, varrebbero a ricondurre i sistemi di doppio binario «entro i canoni stabiliti dalla sentenza della Corte costituzionale».

[149] In questi termini M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario*", cit., 191.

tiva di tali strumenti di coordinamento processuale[150] e sanzionatorio[151], potrebbe

[150] In linea di principio appaiono funzionali a soddisfare il requisito del coordinamento procedimentale, le norme che prevedono, a vario titolo, forme di raccordo tra i due binari (penale e amministrativo) così da ridurre a quanto strettamente necessario l'onere supplementare derivante dal cumulo dei procedimenti. In ambito tributario, oltre alle disposizioni che prevedono istituti premiali subordinati all'estinzione del debito tributario (art. 13, d.lgs. 274/2000, cfr. *infra*) così da creare "indirettamente" una forma di raccordo tra adempimento del debito tributario e processo penale, vengono in considerazione le norme che introducono reciproci obblighi di comunicazione degli illeciti tributari tra le autorità investigative e giudiziarie coinvolte (cfr. art. 331 c.p., nonché art. 36 del d.P.R. 29 settembre 1973 n. 600, e art. 14, c. 4, l. 24 dicembre 1993 n. 537), le norme che disciplinano forme di reciproca circolazione del materiale probatorio raccolto nell'indagine penale e in quella tributaria (cfr. art. 63, c. 1, d.P.R. 26 ottobre 1972, n. 633, nonché art. 33, c. 3, d.P.R. 29 settembre 1973 n. 600 e, specularmente, art. 220 disp. att. c.p.p.) e che, anche in forza della giurisprudenza relativa all'utilizzabilità degli atti, consentono al giudice (penale o tributario) la possibilità di utilizzare, come elemento di prova, il materiale istruttorio raccolto nell'altro procedimento (in tal senso, Cass civ., sez. V, 20 marzo 2013, n. 6918, nonché Cass. pen., sez. III, 5 dicembre 2018, n. 54379). Per un maggior approfondimento, si rinvia a P. Corvi, *I rapporti tra accertamento tributario e accertamento penale*, nonché G. Bocellari, *La reciproca utilizzabilità degli atti nell'accertamento tributario e nel procedimento penale*, entrambi in A. Giarda - G. Varraso - A. Perini (a cura di) *La nuova giustizia penale tributaria*, cit., 462. Per un giudizio critico, tra gli altri sottolineano come le disposizioni citate non siano idonee a costituire effettivi strumenti di raccordo procedimentale tra i due binari, P.P. Rivello, *I rapporti tra giudizio penale e tributario ed il rispetto del principio del ne bis in idem*, in *Dir. pen. cont.*, *Riv. trim.*, 2, 2018, 101 ss. M. Tortorelli, *L'illecito penale tributario e il suo doppio. Dal dialogo (mancato) tra le Corti ad un auspicabile intervento legislativo*, in *Arch. pen.*, 2, 2018, 9 ss.; F. Colaianni - M. Monza, *Il problema del "conflitto" tra ne bis in idem "internazionale" e doppio binario tributario. La parabola del principio verso l'eclisse*?, in *Riv. dir. trib.*, 2, 2017, 39 ss. In ambito finanziario, invece, si ha riguardo alle disposizioni del d.lgs. 58/1998 che prevedono l'autorizzazione del Procuratore della Repubblica per l'esercizio di specifiche attività investigative da parte della Consob (art. 187-*octies*, c. 5, T.U.F), ovvero alla norma che disciplina i rapporti collaborativi tra autorità amministrative e giudiziarie in sede di accertamento (art. 187-*decies* T.U.F.), ovvero, ancora, alla disposizione che disciplina le facoltà della Consob nel procedimento penale (art. 187-*undecies* T.U.F), nonché all'utilizzabilità incrociata del materiale istruttorio raccolto in ciascun procedimento (in tal senso, Cass. pen., sez. V, n. 29 gennaio 2013, n. 4324). In argomento, P. Fimiani, *Market abuse e doppio binario sanzionatorio dopo la sentenza della corte E.D.U.., Grande camera, 15 novembre 2016, A e B c. Norvegia*, in *Dir. pen. cont.*, *Riv. trim.*, 2, 2017, 11 ss. In chiave critica, nel senso di escludere che tali strumenti di raccordo siano suscettibili di dar luogo al requisito della sufficiente integrazione procedimentale, E. Basile, *Una nuova occasione (mancata) per riformare il comparto penalistico degli abusi di mercato*, in *Dir. pen. cont.*, *Riv. trim.*, 5, 2017, 279 ss., nonché F. Viganò, *Ne bis in idem e doppio binario sanzionatorio: nuovo rinvio pregiudiziale della cassazione in materia di abuso di informazioni di privilegiate*, in *Dir. pen. cont.*, *on line*, 28 novembre 2016; F. Cassibba, *Disorientamenti giurisprudenziali in tema di ne bis in idem e "doppio binario" sanzionatorio*, in *Proc. pen. e giust.*, 6, 2017, 1098 ss.

[151] Nel settore tributario il vincolo della proporzionalità complessiva del trattamento sanzionatorio è (o dovrebbe essere) assicurato "a valle" dal peculiare meccanismo di cui all'art. 21 del d.lgs. 74/2000 che prevede l'ineseguibilità delle sanzioni amministrative in caso di fattispecie legate da un rapporto di specialità ai sensi dell'art. 19 del d.lgs. 74/2000. Senonché – come si è detto (cfr. *supra*, nota 146) – la giurisprudenza di legittimità si è mostrata nel tempo (ed è tutt'ora) piuttosto restia ad inquadrare il rapporto tra le fattispecie penali e amministrative in termini di specialità, ragion per cui il peculiare meccanismo di ineseguibilità di cui all'art. 21, operando «in funzione servente del principio di specialità di cui all'art. 19», appare destinato a non trovare applicazione, aprendo alla possibilità di dar luogo al cumulo materiale delle sanzioni punitive, cfr. in tal senso, A. F. Tripodi, *Ne bis in idem e sanzioni tributarie: la Corte di Cassazione sfonda il test della sufficiently close connection in substance and time*, in *Dir. pen. cont.*, *Riv. trim.*, 3, 2018, 275. In questi termini, allora, è stato criticamente osservato come «proprio i limiti di operatività di tale meccanismo restituiscono anche i profili di perdurante illegittimità del sistema», così M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario*", cit., 193. Parte della dottrina, allo scopo di assicurare comunque il risultato utile costituito dalla neutralizzazione a "valle" del cumulo sanzionatorio, ha proposto una lettura «disgiunta degli artt. 19 e 21 tale da rendere quest'ultima previsione operativa indipendentemente dalla sussistenza di un rapporto di specialità tra le fattispecie», in tal senso cfr. F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 215 ss. Rimanendo in ambito tributario, tra gli strumenti volti a prevenire il possibile

essere valorizzata dal Giudice costituzionale per ritenere accertata, sotto i rispettivi profili, la sufficiente integrazione materiale tra i due procedimenti. Tuttavia, ciò non permetterà comunque di ritenere concluso il giudizio di *close connection in substance* tra i due procedimenti e, di conseguenza, per concludere nel senso della compatibilità strutturale del sistema normativo con il divieto di *bis in idem*. La Corte costituzionale, esattamente come i giudici della Corte europea[152], ha infatti mostrato di tenere in adeguata considerazione tutti i diversi parametri di giudizio delineati nell' *A e B test* e, tra questi, anche quelli che fanno leva, rispettivamente, sulla prevedibilità del cumulo punitivo e procedimentale e sulla complementarità degli obiettivi avuti di mira[153].

cumulo delle sanzioni penali e amministrative e, quindi, a garantire la proporzionalità complessiva del trattamento sanzionatorio, deve annoverarsi anche la causa di non punibilità prevista dall'art. 13 del d.lgs. 74/2000, ai sensi del quale i reati di omesso versamento e indebita compensazione non sono punibili se, prima della dichiarazione di apertura del dibattimento di primo grado, i debiti tributari - comprensivi di sanzioni amministravi e interessi - sono stati estinti mediante integrale pagamento del dovuto, anche a seguito di procedure conciliative, adesione all'accertamento o ravvedimento operoso (per un commento alla norma, introdotta dal d.lgs. 158/2015, cfr. A. Giarda - M. Alloisio, *Le nuove cause di estinzione del reato e di esclusione della punibilità. Le circostanze del reato*, in A. Giarda - G. Varraso - A. Perini (a cura di) *La nuova giustizia penale tributaria*, cit., 440 ss.) Ancorché la causa di non punibilità di cui all'art. 13 del d.lgs. 74/2000 non risponde direttamente all'esigenza di garantire il rispetto del *ne bis in idem* (sotto il profilo sostanziale della proporzionalità del trattamento sanzionatorio), in dottrina è stato messo in evidenza come essa, potrebbe costituire un rimedio indiretto consentendo comunque a colui che abbia corrisposto le sanzioni amministrative di evitare l'applicazione di quelle penali: in tal senso, *ex multiis*, M. Dova, *Art. 19. Principio di specialità*, in S. Putinati - C. Nocerino (a cura di) *La riforma dei reati tributari. Le novità del d.lgs n. 158/2015*, Torino, 2015, 388 ss. D'altra parte, se ne sono evidenziati i limiti applicativi discendenti dal fatto che la non punibilità (penale) è subordinata alla condizione del pagamento del debito tributario (sanzioni amministrative e interessi) entro la dichiarazione di apertura del dibattimento, quando invece «il ne bis in idem sostanziale imporrebbe che il pagamento della sola sanzione amministrativa, in qualsiasi momento avvenga condizioni l'applicazione di quella penale»: così, tra gli altri, F. Mazzacuva, *Ne bis in idem e diritto penale dell'economia: profili sostanziali e processuali*, in A. Mangiaracina, *Il ne bis in idem*, cit., 216. In ambito finanziario, invece, il requisito sostanziale della proporzionalità complessiva del trattamento sanzionatorio derivante dal cumulo dei binari penale e amministrativo, trova riconoscimento nel meccanismo di scomputo punitivo previsto dall'art. 187 *terdecies* del d.lgs. 58/1998 che, a dispetto della sua originaria formulazione, in seguito alle modifiche apportate dal d.lgs. 107/2018, prevede oggi il dovere, in capo al "giudice" del secondo processo (sia esso l'autorità giudiziaria o la Consob), di «tenere conto» delle sanzioni (siano esse penali o amministrative) già in precedenza irrogate all'esito del primo processo (penale o amministrativo). Tale disposizione normativa e, in particolare, l'espressione «tenere conto» è stata interpretata dalla giurisprudenza di merito e di legittimità come attributiva del potere di disapplicazione delle sanzioni penali, ove quelle amministrative già applicate siano di per sé proporzionate al disvalore del fatto, ovvero del potere di derogare *in mitius* i minimi edittali previsti dalla norma incriminatrice, così da riportare il trattamento sanzionatorio complessivo entro i limiti di proporzionalità compatibili con il ne bis in idem sostanziale (in tal senso, cfr. Cass. pen., sez. V, 21 settembre 2018, n. 49869; Cass. pen., sez. V, 30 settembre 2019, n. 39999, in *Giur. it.*, 2020, 932, con nota di A.F. Tripodi, *Ne bis in idem e insidere trading: dalla Cassazione i criteri per una risposta sanzionatoria proporzionata*. Nella giurisprudenza di merito, cfr. Trib. Milano, 15 novembre 2018, in *Dir pen cont.*, *on line*, 15 marzo 2019, con nota di F. Mucciarelli *"Doppio binario" sanzionatorio degli abusi di mercato e ne bis in idem: prime ricadute pratiche dopo le sentenze della CGUE e la (parziale) riforma domestica*). Per un maggior approfondimento in ordine al peculiare meccanismo di scomputo punitivo di cui all'art. 187 *terdecies* T.U.F., cfr., con diversità di vedute: L. Baron, *Test di proporzionalità e ne bis in idem. La giurisprudenza interna alla prova delle indicazioni euro-convenzionali in materia di market abuse*, in *Arch. pen.*, *on line*, 3, 2019, 31 ss.; E. Desana, *Ne bis in idem: l'infinito dialogo tra Corti e legislatore*, in *Giur. it.*, 2019, 354 ss.; M. Scoletta, *Abusi di mercato e ne bis in idem: il doppio binario (e la legalità della pena) alla mercè degli interpreti*, in *Le Società*, 2019, 544 ss.

[152] Cfr. *supra*, § 2.1.2, spec. note 81 ss.

[153] Cfr., M. Scoletta, *Uno più uno anche a Roma può fare due: la illegittimità costituzionale del doppio binario*

Parametro, quest'ultimo, che nella valutazione della Corte europea viene a dipendere anche dalla valorizzazione di profili di disvalore del fatto che – «non solo in *abstracto* ma anche in *concreto*»[154] – devono essere almeno in parte diversi.

Ora, se il requisito della prevedibilità costituisce un criterio di valutazione pressoché «ininfluente»[155], facilmente riconoscibile, ed infatti puntualmente riconosciuto, ne discende che molto dipenderà dall'approccio rispetto alla complementarità degli scopi. Parametro di giudizio d'incerto significato e che, tra tutti, costituisce forse il meno intellegibile: indifferentemente riferibile (e infatti riferito) ora alle sanzioni, ora ai procedimenti,[156] le interferenze con il giudizio circa la natura delle sanzioni sono tangibili[157], ed altrettanto chiaro è rischio di incorrere in contraddizioni[158].

Sta di fatto che, sul terreno della complementarità di scopo, l'esito negativo del giudizio – ovvero l'accertamento dell'identità di obbiettivi avuti di mira dai due procedimenti – appare meno improbabile con riferimento al sistema di doppio binario finanziario, di quanto non lo sia in materia tributaria.

In quest'ultimo ambito, infatti, la non perfetta sovrapponibilità strutturale degli illeciti amministrativi e penali rende, almeno in astratto, più agevole argomentare in merito alla alterità delle funzioni rispettivamente assegnate alle sanzioni amministrative (scopo deterrente e compensatorio) e penali (finalità punitiva rispetto a fatti dolosi) e, quindi, più semplice ravvisare la non perfetta sovrapponibilità teleologica

punitivo in materia di diritto d'autore, cit., 10.

154 Corte EDU, Grande Camera, 15 novembre 2016, *A e B c. Norvegia,* § 132.

155 Così, A. F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1066, nel senso che «posto l'onere conoscitivo della legge in capo ad ogni cittadino, non si vede come mai potrebbe essere imprevedibile uno dei due procedimenti sanzionatori […]». In questi termini, allora, è stato giustamente osservato come «la impossibilità per il singolo di prevedere ciascuno dei due cumuli (sanzionatorio e processuale) determinerebbe, rispettivamente, una violazione degli artt. 7 e 6 CEDU, prima ancora che dell'art. 4 Prot. 7», così J. Della Valentina, *Il paradigma del ne bis in idem tra proporzionalità assorbente, rinnovata concezione processuale e overlapping protection,* cit., 9, spec. nota 28.

156 Mentre nella giurisprudenza della Corte di giustizia il parametro della complementarità degli scopi, ancorché sia solo accennato e non adeguatamente approfondito, viene riferito direttamente alle sanzioni (cfr. CGUE, Grande Sezione, 20 marzo 2018, *Menci,* §§ 44 e 63) la Corte europea – almeno in astratto - riferisce la complementarità degli obiettivi alle procedure, anche se nel vagliare il requisito – in concreto – torna a fare riferimento agli scopi perseguiti dalle sanzioni, più che dai procedimenti (cfr., Corte EDU, Grande Camera, 15 novembre 2016, *A e B c. Norvegia,* § 144). Cfr., *amplius*, L. Bin, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole*, cit., 116 ss.

157 In tal senso, L. Bin, *Anatomia del ne bis in idem: da principio unitario a trasformatore neutro di principi in regole*, cit., 117; S. Quattrocolo, *La giurisprudenza della Corte europea dei diritti dell'uomo in materia di ne bis in idem e i suoi effetti sull'ordinamento italiano*, in M. Donini – L. Foffani (a cura di), *La materia penale tra diritto nazionale ed europeo* Torino, 2018,148;

158 Sottolinea quest'aspetto, tra gli altri, A.F. Tripodi, *Cumuli punitivi, ne bis in idem e proporzionalità*, cit., 1065 ss.: «Se si ammette che la sanzione amministrativa presenta uno scopo […] non punitivo, così da rendere il relativo procedimento complementare a (ossia, un *unicum* con) quello penale, non si dovrebbe altresì porre in dubbio la sua stessa natura penale e quindi escludere in radice la violazione del ne bis in idem? Oppure, correlativamente: se si è qualificata la sanzione amministrativa come sostanzialmente penale, in quanto punitiva, non si dovrebbe allora, in sede di giudizio di connessione sostanziale e temporale dei procedimenti, riscontrare la presenza di due procedimenti e pertanto concludere nel senso del bis in idem?». In senso analogo, tra gli altri, R.A. Ruggiero, *Il ne bis in idem: un principio alla ricerca di un centro di gravità permanente*, in *Cass. pen.*, 2017, 3837.

tra il procedimento amministrativo e quello penale[159].

Viceversa, in materia finanziaria, alla perfetta identità strutturale tra illeciti penali e amministrativi diretti a punire essenzialmente le stesse condotte[160], fa da *paindant* l'omogeneità teleologica delle sanzioni penali e amministrative. Tutto ciò non può che riflettersi sul giudizio di non complementarità degli scopi dei due procedimenti, i quali appaiono entrambi indirizzati al medesimo scopo funzionale a tutelare l'«integrità dei mercati finanziari dell'Unione e la fiducia del pubblico negli strumenti finanziari»[161]. Detto altrimenti, in quest'ambito il "binario penale" non costituisce che una modalità più incisiva di protezione del medesimo interesse giuridico.

A conferma di quanto sin qui sostenuto, depongono essenzialmente due "indizi".

Innanzitutto, quando è stata chiamata a valutare la compatibilità dei sistemi di doppio binario rispetto al vincolo del *ne bis in idem*, la giurisprudenza europea si è mostrata più sensibile rispetto alla materia del *market abuse*, nella quale l'esito negativo dell'*A e B test*, quindi l'assenza del carattere sufficiente integrato tra i due procedimenti, è dipeso non solo dai profili di interconnessione cronologica, ma anche dal riscontro di una disconnessione sostanziale e, sotto tale ultimo aspetto, proprio dalla carenza

---

[159] Secondo l'orientamento interpretativo già fatto proprio dalla Corte europea a partire dalla sentenza A e B, e successivamente ribadito Corte di Cassazione la quale, in alcuni recenti arresti ha riconosciuto la sufficiente integrazione tra il procedimento penale e quello tributario rilevando, sotto lo specifico profilo della complementarità degli scopi, che il procedimento amministrativo «è volto al recupero a tassazione delle imposte non versate», mentre il procedimento penale «è teso alla prevenzione e alla repressione dei reati in materia tributaria», così Cass. pen., sez. III, 4 febbraio 2021, n.4439, in *Riv. dott. comm.,* 2021, 267 ss., con nota di L. Troyer, *Non viola il ne bis in idem l'irrogazione di sanzione formalmente amministrativa alla quale è riconosciuta natura sostanzialmente penale.* Cfr., in senso critico rispetto a tale orientamento, M. Scoletta, *Il principio di ne bis in idem e i modelli punitivi "a doppio binario",* cit., 199, spec. nota 74, a giudizio del quale si tratta di un di un'«affermazione – funzionale a legittimare il doppio binario – che risulta corretta solo in linea di principio, ma che non tiene conto del carattere punitivo via via assunto (anche) dal procedimento amministrativo tributario, attraverso la previsione di severe sanzioni pecuniarie per i fatti oggetto di accertamento». In senso analogo, cfr. A. F. Tripodi, *Ne bis in idem e sanzioni tributarie: la corte di cassazione "sfronda" il test della sufficiently close connection in substance and time,* in *Dir. pen. cont*., *on line,* 16 marzo 2018; S. Colaianni - M. Monza, *Il problema del "conflitto" tra ne bis in idem "internazionale" e doppio binario tributario. La parabola del principio verso l'eclisse?,* cit*., 38;* G. Melis*, Ne bis in idem con il nodo della connessione,* in *Il sole 24 ore, Norme e tributi,* 15 ottobre 2017; F. Gallo*, Il ne bis in idem in campo tributario: un esempio per riflettere sul "ruolo" delle Alte Corti e sugli effetti delle loro pronunzie,* in *Rass. trib.,* 2017, 923.

[160] Come confermato dalla clausola d'apertura "le sanzioni penali quando il fatto costituisce reato" con cui esordiscono, rispettivamente, gli articoli 187 *bis* e 187 *ter* del d.lgs. 58/1998.

[161] Così, M. Scoletta, *Il ne bis in idem "preso sul serio": la Corte EDU sulla illegittimità del doppio binario francese in materia di abusi di mercato (e i possibili riflessi nell'ordinamento italiano)*, cit., secondo cui, in materia di *market abuse*, l'unicità teleologica dei due procedimenti costituirebbe un dato davvero «inconfutabile» come dimostrato anche dalla motivazione intimamente «tautologica» fornita dalla Corte di giustizia la quale, nella sentenza *Garlsson*, ha espressamente riconosciuto «legittimo che uno Stato membro voglia, da un lato, scoraggiare e reprimere ogni violazione, intenzionale o meno, del divieto di manipolazione del mercato applicando sanzioni amministrative stabilite, se del caso, in maniera forfettaria e, dall'altro, scoraggiare e reprimere violazioni gravi di tale divieto, che sono particolarmente dannose per la società e che giustificano l'adozione di sanzioni penali più severe» (cfr. CGUE, Garlsson, cit., § 47:). *Contra*, nel senso di ritenere integrato il requisito della differenziazione degli scopi delle risposte sanzionatorie, sia in astratto, che in concreto, cfr. P. Fimiani, *Market abuse e doppio binario sanzionatorio dopo la sentenza della Corte E.D.U., Grande Camera, 15 novembre 2016, A e B c. Norvegia*, cit., 12, a giudizio del quale «le sanzioni amministrative pecuniarie sono versate alla Consob e quindi all'Autorità di controllo, assumendo pertanto una valenza anche compensatoria rispetto all'attività istituzionale dalla stessa svolta, che si aggiunge a quella generale retributiva caratteristica esclusiva, invece, della sanzione penale»

della complementarietà di scopo[162].

Viceversa, in ambito tributario, le due Corti europee si sono mostrate decisamente più indulgenti rispetto alla valutazione delle soluzioni di doppio binario prefigurate nei singoli ordinamenti interni. In tale settore, impregiudicato il riscontro della effettiva complementarità di scopo tra procedimento tributario e quello penale[163], l'esito negativo dell'*A e B test* e la conseguente violazione della garanzia – quando è stata riconosciuta – è dipesa essenzialmente dall'assenza di una sufficiente connessione temporale[164], ossia dall'unico parametro che non si presta ad essere preso in considerazione nell'ambito del giudizio di legittimità costituzionale.

A ciò si aggiunga che la stessa Corte costituzionale sembrerebbe aver già posto una seria ipoteca sulla legittimità strutturale del sistema di doppio binario tributario. Con la sentenza n. 222/2019[165], infatti, il Giudice costituzionale ha già svolto, sia pure

[162] Emblematica, in tal senso, la sentenza Corte EDU, 6 giugno 2019, *Nodet c. Francia*, cit., In quell'occasione – investita del riscorso presentato da un cittadino francese (il sig. Nodet) inizialmente condannato dall'Autorità amministrativa al pagamento di una sanzione per l'illecito di manipolazione del mercato, e successivamente, per i medesimi fatti, sottoposto a nuovo procedimento penale conclusosi con la condanna alla pena detentiva di otto mesi di reclusione – la Corte si trovava a giudicare della legittimità convenzionale del sistema di doppio binario punitiva in materia di illeciti finanziari. Nel decidere la questione, dopo avere riscontrato i presupposti operativi della garanzia (tanto l'*idem factum* quanto la natura sostanzialmente punitiva delle sanzioni applicate) la Corte europea ha fatto applicazione dell'*A e B test* onde verificare se i due binari potessero effettivamente considerarsi come parti di un unico procedimento sanzionatorio integrato: al riscontro della prevedibilità della duplicazione sanzionatoria e procedimentale, e dalla complessiva proporzionalità del trattamento sanzionatorio, tuttavia, si è accompagnato il rilevo dell'assenza di complementarietà di scopo, il difetto di una sufficiente integrazione procedimentale e, sotto il profilo cronologico, il difetto di una sufficiente connessione temporale. In particolare, sotto il profilo della complementarietà di obiettivi, la Corte europea ha sottolineato come i due procedimenti non potessero considerarsi "complementari" rispetto agli scopi perseguiti, essendo entrambi finalizzati a reprimere i medesimi profili di dannosità del fatto di manipolazione del e a tutelare i medesimi interessi sociali (Corte EDU, 6 giugno 2019, *Nodet c. Francia*, cit., § 48).

[163] Già a partire dalla pronuncia *A e B*, resa proprio con riferimento al sistema di doppio binario prefigurato dall'ordinamento norvegese in materia fiscale, l'esito positivo dell'A e B test – sotto il profilo dell'interconnessione materiale – era dipeso dal riconoscimento della complementarietà degli scopi perseguiti dai due procedimenti sanzionatori, rispettivamente intesi, l'uno – quello amministrativo-tributario – ad uno scopo deterrente e, assieme, compensatorio rispetto ai considerevoli sforzi, umani e finanziari, profusi dall'l'amministrazione fiscale per scoprire e sanzionare le evasioni fiscali; l'altro – quello *stictu sensu* penale – votato ad una finalità dichiaratamente punitiva rispetto ad una condotta antisociale, caratterizzata da una componente aggiuntiva di tipo doloso o fraudolento, cfr. Corte EDU, *A e B c. Norvegia*, cit., § 144.

[164] Si vedano, in tal senso, Corte EDU, 18 maggio 2017*, Johansson e a. c. Islanda*, cit., e Corte EDU, 16 aprile 2019, *Bjarni Armannsson c. Islanda*, cit. In ambedue le sentenze, rese con riferimento al sistema di doppio binario tributario vigente nell'ordinamento islandese, l'esito negativo dell'*A e B test*, quindi l'accertamento della violazione della garanzia, è dipeso essenzialmente dall'assenza di una *connection in time*: nel caso *Johansson,* infatti, la Corte ha avuto buon gioco di constatare come, dopo un primo inziale periodo di svolgimento parallelo, il secondo procedimento si era protratto per ulteriori cinque anni dopo la chiusura del primo, con il risultato di tenere in gioco l'autore della condotta illecita per un periodo complessivo di nove anni; similmente, nel caso *Bjarni Armannsson,* la Corte ha censurato l'assenza di sovrapposizione cronologica poiché i due procedimenti – che avevano avuto una durata complessiva di circa cinque anni - erano avanzati in parallelo solo per poco più di cinque mesi, e quello penale era continuato autonomamente per un anno e mezzo.

[165] Corte cost., 24 ottobre 2019, n. 222, cit. (per un commento, v. M. Scoletta, *Legittimità in astratto e illegittimità in concreto del doppio binario punitivo in materia tributaria al cospetto del ne bis in idem europeo*, cit., 2649 ss.). La sentenza, con la quale la questione di legittimità costituzionale dell'art. 649 c.p.p. è stata dichiarata inammissibile per insufficiente descrizione della fattispecie oggetto di giudizio e per difetto

incidenter tantum, la verifica sulla sufficiente integrazione tra il procedimento penale e quello tributario, riscontrando tutti i diversi parametri significativi di tale connessione, *ivi* compreso quello della complementarità di scopo[166].

In definitiva, volendo riavvolgere i fili del discorso, se da un lato può certamente dirsi che la sentenza n. 149/2022 della Corte costituzionale appaia quantomeno in grado di rimettere in discussione la tenuta strutturale dei sistemi di doppio binario vigenti nell'ordinamento interno, d'altra parte, se due o più indizi fanno una prova, dovrà anche riconoscersi che attualmente il sistema di doppio binario vigente in materia finanziaria appaia maggiormente esposto alle censure dei giudici, di quanto non lo sia quello vigente in materia tributaria.

di motivazione in punto di rilevanza e non manifesta infondatezza, si inscrive nel noto *affaire* Menci essendo scaturita dall'ordinanza di rimessione sollevata dallo stesso Giudice *a quo* del caso Menci, il quale, nonostante la Corte di giustizia avesse già riconosciuto la compatibilità del sistema di doppio binario tributario rispetto alla garanzia di cui all'art. 50 (CGUE, Grande Sez., 20 marzo 2018, *Menci*, cit), ha egualmente chiesto alla Corte costituzionale di dichiarare l'illegittimità della norma impugnata per contrasto con gli artt. 3 e 117 Cost., quest'ultimo in relazione all'art. 4, prot. 7, CEDU e all'art. 50 CDFUE, nella parte in cui non estende il divieto di doppio giudizio anche ai casi di doppio binario penale e amministrativo.

[166] Corte cost., 24 ottobre 2019, n. 222, cit., § 2.2.1.del 'considerato in diritto', ove, in particolare, la Corte costituzionale sottolinea come nell'ordinanza di rimessione il Giudice *a quo* non adduca sufficienti argomentazioni per confutare la complementarietà degli scopi tra i due procedimenti (amministrativo-tributario e penale) già riconosciuta dalla Corte di giustizia, limitandosi ad affermare «apoditticamente l'identità di scopo, senza però chiarire – in particolare – le ragioni per cui dovrebbe escludersi che la minaccia di una sanzione detentiva per l'evasione di importi IVA annui superiori – oggi – a 250.000 euro, in aggiunta a una sanzione amministrativa pecuniaria calcolata in misura percentuale rispetto all'importo evaso, possa perseguire i legittimi scopi di rafforzare l'effetto deterrente spiegato dalla mera previsione di quest'ultima, di esprimere la ferma riprovazione dell'ordinamento a fronte di condotte gravemente pregiudizievoli per gli interessi finanziari nazionali ed europei, nonché di assicurare ex post l'effettiva riscossione degli importi evasi da parte dell'amministrazione grazie ai meccanismi premiali connessi all'integrale saldo del debito tributario».

Avvertenze per il consumatore e obblighi delle piattaforme del commercio elettronico. Alcune osservazioni sulla sentenza *Lee v. Amazon**

Rosario Petruso

Abstract

La *Proposition 65* è una legge californiana che attribuisce ai consumatori il diritto ad essere informati circa l'esposizione a sostanze cancerogene o che possano dar luogo a malformazioni congenite o ad altri danni riproduttivi: ai sensi della legge, tutti gli attori del circuito distributivo sono tenuti a fornire un'avvertenza «chiara e ragionevole» del relativo rischio. La sezione 230 del *Communications Decency Act* esonera da responsabilità gli intermediari della rete relativamente ai contenuti dei terzi. Le piattaforme del commercio elettronico, nel facilitare l'interazione di venditori ed acquirenti, rischiano di mettere a repentaglio la salute dei consumatori, portando loro prodotti vietati, non sicuri o etichettati in modo errato. Alla luce di tale scenario, in *Lee v. Amazon* è stato chiesto alla *Court of Appeal* della California di individuare chi - nell'economia di piattaforma - sia chiamato a fornire le avvertenze ex *Proposition 65*. Dal punto di vista delle tutele spettanti al consumatore, questa domanda è fondamentale: considerato che molti venditori terzi operano dall'estero, le piattaforme di *e-commerce* potrebbero essere gli unici attori della catena negoziale tenuti a conformarsi agli obblighi discendenti dalla *Proposition 65*. Alla luce della recente sentenza della *Court of Appeal* californiana, questo scritto prende in esame un cambiamento significativo nella giurisprudenza statunitense relativa alla regolazione della rete.

Proposition 65 is a Californian "right to know" statute, requiring companies that expose consumers to chemicals known to cause cancer, birth defects, or other reproductive harm to provide a «reasonable and clear» warning associated with the products they supply. Section 230 of the Communications Decency Act provides immunity to online intermediaries from liability based on third-party content. As marketplace facilitators, e-commerce platforms put consumers at risk by bringing in their hands thousands of banned, unsafe or mislabeled products formally sold by third-party sellers.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

In that scenario, in Lee v. Amazon the California Court of Appeal has been asked to determine who is responsible for providing the Proposition 65 disclosures. From the perspective of consumer safety, this question is pivotal: many vendors are overseas, so e-commerce platforms seem the only entities that could be forced to comply with Proposition 65. Taking into consideration the ruling of the Court of Appeal, this article analyzes a significant shift in the U.S. case-law regarding the Internet governance.

Sommario

1. Osservazioni introduttive. – 2. Le avvertenze a tutela del consumatore previste dalla *"Proposition 65"*. – 3. L'esenzione da responsabilità per i fornitori di "servizi informatici interattivi" nella normativa federale statunitense. - 4. Il caso *Lee v. Amazon:* la decisione della *Trial Court*. – 5. La sentenza resa dalla *Court of Appeal* l'11 marzo 2022. – 6. Una traiettoria giurisprudenziale proclive a individuare strumenti di regolazione delle piattaforme digitali. – 7. Brevi e conclusive osservazioni comparatistiche sulla portata delle trasformazioni in atto nel governo delle piattaforme digitali.

Keywords

Proposition 65 - avvertenze per il consumatore - piattaforme di *e-commerce* - sezione 230 del *Communications Decency Act* - *sharing economy*

1. Osservazioni introduttive

Nell'economia di piattaforma[1], accanto a piattaforme di pubblicità, piattaforme di servizi e piattaforme della *sharing economy*, si sono affermate imprese che intermediano lo scambio di beni e servizi: con una terminologia ormai collaudata, ci si riferisce sinteticamente ad esse, pur nella eterogeneità dei modelli di profitto alle stesse sottostanti, con la locuzione "piattaforme di *e-commerce*". Come ben messo in rilievo dalla dottrina[2], tali piattaforme realizzano mercati virtuali, coordinando l'incontro di domanda ed offerta tra chi vende beni e chi li acquista, diffondendo le informazioni rilevanti e attuando strumenti per la creazione del clima di fiducia necessario alla conclusione delle transazioni.

I compiti appena descritti sono assolti dagli intermediari digitali secondo modalità proprie dell'economia di piattaforma, che (in quanto tali) tendono a sfuggire alle logiche tipiche dell'impresa tradizionale. Così, ad esempio, può capitare che l'incontro tra domanda ed offerta sia organizzato grazie alla enorme mole di dati in possesso dell'intermediario digitale, il quale può procedere financo a sofisticatissime politiche di

[1] L'economia di piattaforma è un'economia a struttura tripartita, che si caratterizza, cioè, per la presenza di tre attori distinti che partecipano alla transazione: il venditore, l'acquirente (o il prestatore d'opera e il committente) e la piattaforma digitale.

[2] G. Smorto, in A. Quarta - G. Smorto, *Diritto privato dei mercati digitali*, Milano, 2020, 120; D. McKee, *The platform economy: natural, neutral, consensual and efficient?*, in *Transnational Legal Theory*, 8, 2017, 457 ss.

discriminazione di prezzo[3]; che le informazioni rilevanti per la conclusione dell'affare siano fornite attraverso sistemi di *feedback* e *rating*, i cui giudizi sono profusi dagli stessi consumatori che abbiano utilizzato la piattaforma per i precedenti acquisti[4]; che la fiducia di questi ultimi all'interno del mercato virtuale sia conquistata dall'intermediario attraverso la predisposizione di strumenti alternativi di composizione delle eventuali controversie[5] (facili politiche di reso, garanzie complementari o sostitutive rispetto a quelle fornite dal diritto statuale, etc.).

Alla luce di questo quadro, con un'espressione di sintesi, si potrebbe sostenere che l'obiettivo principale delle piattaforme del commercio elettronico (le cui strategie di remunerazione sono incentrate, secondo prassi diverse, sui volumi di vendite) sia facilitare gli scambi a distanza garantendo il buon funzionamento del mercato digitale.

Nella logica appena descritta, l'intermediario tende a presentarsi come soggetto terzo rispetto alla transazione conclusa all'interno dei propri spazi digitali tra chi vende e chi acquista: secondo la narrazione corrente[6], in questo scenario trilaterale, le piattaforme del commercio elettronico limiterebbero il loro compito a quello di mettere a disposizione dei venditori una mera "vetrina digitale" e agli acquirenti una "piazza virtuale" in cui poter riporre fiducia.

Da questa impostazione, seguono importanti conseguenze per il consumatore: ad esempio, e giusto per soffermarsi su due questioni di recente esaminate dalla giurisprudenza d'Oltreoceano, gli attori digitali negano la loro convenibilità in giudizio per l'eventuale danno arrecato ai singoli dai prodotti difettosi acquistati per via telematica da venditori indipendenti[7] (in quanto - è il punto di vista fatto valere dagli intermediari stessi - si collocherebbero al di fuori della catena di approvvigionamento) e si sottraggono agli obblighi di informazione e di segnalazione (eventualmente gravanti sulla

[3] Sul punto G. Smorto, *Protecting the Weaker Parties in the Platform Economy*, in N. M. Davidson - M. Finck - J. J. Infranca (a cura di), *The Cambridge Handbook of the Law of the Sharing Economy*, 2018, 431 ss.; S. K. Mehra, *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, in *Minnesota Law Review*, 100, 2016, 1323; S. Levmore - F. Fagan, *The End of Bargaining in the Digital Age*, in *Cornell Law Review*, 103, 2018, 1469 ss.; Dirk Bergemann, *The Limits of Price Discrimination*, in *American Economic Review*, 105, 2015, 921; R. Calo - A. Rosenblat, *The Taking Economy: Uber, Information, and Power*, in *Columbia Law Review*, 117, 2017, 1623 ss.

[4] Per un primo approccio al tema dei sistemi reputazionali e di *rating* G. Smorto, *Reputazione, fiducia e mercati*, in *Europa e diritto privato,* 1, 2016, 199 ss., nonché i diversi contributi pubblicati in H. Masum - M. Tovey, (a cura di), *The Reputation Society: How Online Opinions Are Reshaping the Offline World*, Boston, 2011.

[5] Sul punto S. Casabona, *Intermediazione digitale e composizione delle controversie: dall'Alternative Dispute Resolution all'alien dispute resolution*, in *Il Diritto dell'Informazione e dell'Informatica*, 32, 2017, 497 ss.

[6] È questa, ad esempio, la descrizione dei servizi prestati da Amazon nei "Termini e condizioni dell'Account Amazon", ove si legge che: «Amazon non assume alcuna responsabilità per le azioni, i prodotti e i contenuti di tutti i venditori terzi e di altre terze parti, né funge da agente del venditore. Il venditore è responsabile della vendita dei prodotti e della gestione di eventuali reclami dell'acquirente o di qualsiasi altro problema derivante da o in connessione con l'accordo tra te e il venditore».

[7] Sul tema, si registra già una nutrita casistica negli Stati Uniti. Le due antitetiche posizioni assunte dalla giurisprudenza nordamericana – l'una proclive a ritenere che l'intermediario, nonostante le apparenze, si inserisca all'interno del giro distributivo (rispondendo del danno subito a causa della difettosità del prodotto a titolo di *strict liability*), l'altra incline a valorizzare gli elementi di novità sottostanti al modello di business adottato dalle piattaforme di *e-commerce* (che si sottrarrebbero, pertanto, al regime del danno da prodotti) sono ben riassunte rispettivamente dalla pronuncia resa dalla *Court of Appeal* californiana nel caso *Bolger v. Amazon.com*, 53 Cal. App. 5th 43 1 (2020) e dalla pronuncia resa dalla *Supreme Court* del Texas nel caso *Amazon.com, Inc. v. McMillan*, 625 S.W.3d 101.

filiera distributiva) relativamente alla nocività dei prodotti compravenduti per mezzo del loro apporto facilitatore.

È proprio quest'ultimo - la soggezione all'obbligo di informare il consumatore circa la pericolosità di un prodotto - l'oggetto della decisione resa l'11 marzo 2022 dalla *Court of Appeal* della California nel caso che qui si commenta[8]. Segnatamente si trattava di stabilire se l'intermediario digitale - nella specie la piattaforma di commercio elettronico Amazon - fosse da considerarsi soggetto, ai sensi della *Proposition 65*[9], all'obbligo di avvertire adeguatamente i consumatori relativamente all'esposizione a sostanze chimiche, pericolose per la salute.

Nelle osservazioni che seguono si prenderà, pertanto, in esame la regolamentazione californiana relativa alle informazioni da fornire ai consumatori con riguardo ai prodotti che possono accrescere il rischio di tumore o di danni all'apparato riproduttivo (la c.d. *Proposition 65*). Si passerà, poi, all'analisi del regime di esonero da responsabilità previsto per gli intermediari digitali dalla normativa federale statunitense approvata nel 1996 con il *Communications Decency Act* (CDA)[10]. Chiarito il quadro statutario di riferimento, sarà possibile procedere alla disamina della decisione resa dalla *Court of Appeal* e alle implicazioni che da essa sembrano discendere nel governo degli spazi digitali. L'analisi di alcuni tra i più rilevanti (e noti anche per l'eco mediatica che hanno suscitato) casi giurisprudenziali sul tema servirà a porre a raffronto le soluzioni adottate dalle Corti statunitensi con la giurisprudenza della Corte di giustizia dell'Unione europea relativa alla individuazione dei criteri per appurare se le piattaforme digitali eroghino, oltre che i servizi tipici della società dell'informazione (consentendo l'interazione tra agenti economici indipendenti), anche il servizio sottostante[11]. L'impressione, da verificare, è, infatti, che le due linee argomentative condividano un nucleo comune che segna, nelle due sponde dell'Atlantico, l'avvio di una svolta regolativa ed il tramonto dell'approccio eccezionalista e non interventista nella regolamentazione della rete adottato sul finire degli anni '90 del secolo scorso.

2. Le avvertenze a tutela del consumatore previste dalla *"Proposition 65"*

Per meglio comprendere la sentenza resa dalla *Court of Appeal* californiana e le importanti implicazioni che ne possono discendere nella regolamentazione dei mercati digitali, occorre preliminarmente descrivere nei suoi tratti essenziali la normativa statale fatta valere dal consumatore nei confronti dell'intermediario digitale.

[8] *Lee v. Amazon.com, Inc.*, 76 Cal. App. 5th 200.

[9] Si tratta, come meglio si dirà più avanti nel testo, di una legge californiana del 1986, formalmente intitolata "*Safe Drinking Water and Toxic Enforcement Act*".

[10] 47 U.S. Code 230 "*Protection for private blocking and screening of offensive material*".

[11] Ci si riferisce alla ormai corposa giurisprudenza che vede nel caso CGUE, C-434/15, *Asociación Profesional Elite Taxi v. Uber Systems Spain SL* (2017). Gli arresti successivi di questa parabola giurisprudenziale sono costituiti dai casi, CGUE, C-320/16, *Uber France* (2018), CGUE, C-390/18, *Airbnb Ireland* (2019) e *i*, CGUE, C-62/19, *Star Taxi App SRL v. Unitatea Administrativ Teritorială Municipiul București prin Primar General e Consiliul General al Municipiului București* (2020).

Il *Safe Drinking Water and Toxic Enforcement Act* (meglio conosciuto come "*Proposition 65*") è una legge californiana del 1986, approvata su iniziativa popolare, volta a proteggere il singolo dall'esposizione a particolari sostanze chimiche, note come causa di cancro, di malformazioni congenite e di tossicità riproduttiva.

La normativa in parola mira a salvaguardare la salute dei singoli garantendo loro un diritto ad essere informati (c.d. "*right to know*"), sì da consentire scelte di consumo o, più in generale, comportamenti maggiormente consapevoli[12].

Più in particolare, la legge attribuisce a ciascun consumatore[13] una situazione soggettiva di natura pretensiva, azionabile contro il produttore e contro ogni altro attore della rete di distribuzione che immetta "consapevolmente" nel mercato prodotti contenenti le sostanze indicate in un'apposita lista (la c.d. "*Prop. 65 list*") senza prima informare adeguatamente (con un'«avvertenza chiara e ragionevole») dei rischi connessi alla relativa esposizione[14].

La *Proposition 65*, dunque, non vieta l'utilizzo di determinate sostanze[15]: i prodotti che presentano avvertenze ex *Proposition 65* non sono per ciò solo da considerarsi pericolosi. Il consumatore, però, deve essere informato e messo in condizione di decidere autonomamente se limitare l'esposizione alle sostanze pericolose in essi contenute.

L'inserimento di una determinata sostanza nella lista (curata ed aggiornata annualmente dall'*Office of Environmental Health Hazard Assessment*, *OEHHA*) impone che tutti i soggetti che concorrono alla immissione nel giro distributivo (produttori, confezionatori, importatori, distributori, rivenditori al dettaglio, ma anche titolari di impianti industriali, di parchi giuoco e di altri locali[16]) di un qualsiasi prodotto che contenga tali ingredienti[17] siano tenuti - entro un anno dalla pubblicazione nell'elenco - ad informare adeguatamente il consumatore (prima della relativa esposizione) in merito alla presenza di siffatta sostanza e dei correlati rischi per la salute.

L'attuazione degli scopi soggiacenti alla legge del 1986 è per lo più affidata (sia pure in via sussidiaria[18]) alla iniziativa dei singoli. Previa verifica della mancanza di interesse

---

[12] Come chiarito dalla giurisprudenza, lo scopo della *Proposition 65* è, infatti, facilitare la comunicazione al pubblico dell'esposizione a potenziali sostanze nocive, sì da consentire ai consumatori di prendere decisioni informate. In questi termini, *DiPirro v. Bondo Corp.*, 153, Cal. App. 4th 150, 183 (2017) ove si legge che la *Proposition 65* mira a «*facilitate the notification of the public of potentially harmful substances, so informed decisions may be made by consumers on the basis of disclosure*».

[13] Si noti che ai sensi del Cal Health & Safety Code 25249.11 i legittimati attivi all'azione non sono solo i consumatori. Nella norma citata si legge che: «*For purposes of this chapter: (a) "Person" means an individual, trust, firm, joint stock company, corporation, company, partnership, limited liability company, and association*».

[14] Questa la parte rilevante della norma (Cal Health & Safety Code 25249.6): «*Required warning before exposure to chemicals known to cause cancer or reproductive toxicity. No person in the course of doing business shall knowingly and intentionally expose any individual to a chemical known to the state to cause cancer or reproductive toxicity without first giving clear and reasonable warning to such individual, except as provided in Section 25249.10*».

[15] In dottrina, «*The California 65 Proposition is a right to know law warning, not a ban or restrictions law*». In questi termini, D. Gartner, *California Proposition 65: The Right to Know Law*, in *International Chemical Regulatory and Law Review*, 1, 2018, 156 ss.

[16] Con un'espressione volutamente generica la normativa californiana in Cal Health & Safety Code 25249.6, si riferisce, infatti, a «[*any*] *person in the course of doing business*».

[17] Attualmente la lista include oltre 1.000 sostanze chimiche, tra cui arsenico, piombo, mercurio, cadmio, etc.

[18] Il singolo che intenda convenire in giudizio il trasgressore è tenuto, infatti, a notificare la violazione

delle autorità pubbliche (statali e locali) competenti a promuovere l'azione *ex Proposition 65*[19], ciascun consumatore può, infatti, citare in giudizio («*in the public interest*[20]») il produttore e tutti i soggetti che concorrano, nell'ambito della rispettiva attività di impresa, alla circolazione del prodotto in assenza delle relative avvertenze.
Il promovimento della relativa azione (volta ad ottenere l'irrogazione di una sanzione civile e un ordine inibitorio diretto all'apposizione delle relative avvertenze) da parte del singolo è incentivato dalla legge attraverso vari accorgimenti. Ed invero, per intentare un'azione ai sensi della *Proposition 65*, non è necessario che il consumatore abbia subito un danno: il ricorso può essere promosso per il solo fatto di non esser stati correttamente informati del rischio connesso all'esposizione alle sostanze tossiche[21].
Occorre considerare, inoltre, il fatto che, al verificarsi di determinati presupposti, il ricorrente non è chiamato a sostenere le spese del giudizio; infine, chi promuove l'azione gode di un incentivo economico molto allettante: nel caso in cui l'azione sia ritenuta fondata, ha diritto al 25% della sanzione irrogata al trasgressore[22].
Quest'ultimo, su cui grava l'onere della prova che le sostanze non siano dannose[23] o che siano presenti in quantità irrilevanti e tali da non cadere sotto la scure della *Proposition 65*[24], si espone a costi importanti: può essere sanzionato, infatti, fino a 2.500 dollari al giorno per ogni violazione ed in relazione a ciascun prodotto immesso nel mercato californiano[25].
Conclusivamente sul punto, si può dire che - sebbene tale legge non abbia riscosso favori unanimi e sia regolarmente soggetta a serrate critiche che mettono in dubbio la

(«*notice of violation*») allo stesso trasgressore e a tutti i soggetti pubblici che ai sensi della Cal Health & Safety Code 25249.7 (c) possono proporre l'azione. Solo allo scadere di 60 giorni da tale notifica (ed in caso di mancato promovimento dell'azione da parte dei soggetti indicati nella sezione 25249.7 (c)) il singolo potrà agire autonomamente. Come notato in dottrina, benché siano numerose le azioni promosse dalle autorità pubbliche, l'implementazione della *Proposition 65* è sostanzialmente affidata all'iniziativa privata: per maggiori approfondimenti sul tema C. Polsky - M. Schwarzman, *The Hidden Success of a Conspicuous Law: Proposition 65 and the Reduction of Toxic Chemical Exposures*, in *Ecology Law Quarterly*, 47, 2020, 833.

[19] Cal Health & Safety Code 25249.7 (c) «*Actions pursuant to this section may be brought by the Attorney General in the name of the people of the State of California, by a district attorney, by a city attorney of a city having a population in excess of 750,000, or, with the consent of the district attorney, by a city prosecutor in a city or city and county having a full-time city prosecutor, or as provided in subdivision (d)*».

[20] Ivi, (d).

[21] Cal. Health & Safety Code 25249.6 (a), (b). In dottrina T.J.K. Schick, *Proposition 65: Why Coffee in California May Come with a Cancer Warning*, in *Loyola Consumer Law Review*, 30, 2018, 475.

[22] Cal Health & Safety Code 25249.12 (d) «*Twenty - five percent of all civil and criminal penalties collected pursuant to this chapter shall be paid to the office of the city attorney, city prosecutor, district attorney, or Attorney General, whichever office brought the action, or in the case of an action brought by a person under subdivision (d) of Section 25249.7, to that person*».

[23] In questi termini, *Consumer Cause, Inc. v. SmileCare*, 91 Cal. App. 4th 454.

[24] Sebbene solo l'utilizzo al di sopra di certi livelli di concentrazione determinati per legge (il c.d. "*safe harbor level*") richiedano l'apposizione dell'avviso, tali soglie sono state mantenute precauzionalmente basse, sì da ricondurre un numero enorme di prodotti nell'ambito delle avvertenze dovute in forza della legge. Sul punto, C. Polsky - M. Schwarzman, *The Hidden Success of a Conspicuous Law*, cit., 830.

[25] Ben si comprende, dunque, come l'ammontare della sanzione possa crescere in modo esponenziale, soprattutto nell'economia di piattaforma: ed invero, limitando le nostre osservazioni alla sola piattaforma digitale convenuta, basta riflettere sulla circostanza che il mercato gestito da Amazon annovera circa 2,5 milioni di venditori indipendenti che, a propria volta, espongono circa 600 milioni di prodotti unici.

sua efficacia (sia in punto di metodo[26] sia relativamente ai risultati attesi[27]) - si ritiene dai più[28] che abbia avuto il merito di aver indotto un gran numero di produttori ad adottare comportamenti virtuosi, a tutela della propria immagine. I timori di incorrere nelle spese di giudizio, di perdere la fiducia dei consumatori e di spostare le scelte di acquisto verso le alternative offerte dal mercato[29] avrebbero portato molti produttori a riformulare i processi di fabbricazione per ridurre (e, ove possibile, eliminare) l'uso di sostanza tossiche o, quantomeno, a fornire le avvertenze necessarie prescritte dalla legge, sì da consentire al singolo, correttamente informato, di limitare l'esposizione alle sostanze più nocive.

3. L'esenzione da responsabilità per i fornitori di "servizi informatici interattivi" nella normativa federale statunitense

Occorre ancora fissare un punto centrale dal quale si diramerà l'indagine che segue. La promessa di un potenziamento dei valori democratici (e, in particolare, della libertà di espressione), trainati da un Internet deregolato, ha fatto sì che la prima fondamentale - e tuttora cruciale - disciplina legislativa statunitense riguardante gli intermediari della rete telematica abbia predisposto per essi un regime esonerativo da responsabilità senza precedenti. Nell'ambito di una più vasta riforma del settore delle telecomunicazioni, il legislatore federale statunitense ha articolato, alla sezione 230 del *Communications Decency Act* del 1996[30], una tutela per i fornitori di "servizi informatici interattivi" che ruota intorno a tre punti fondamentali: innanzitutto (ai sensi della sub-sezione 230 (c)(1), il fornitore dei servizi telematici non potrà essere "trattato" alla stregua del

[26] In chiave critica, si sostiene come l'approccio al problema della tutela dei consumatori adottato dalla *Proposizione 65* ed "incentrato sul rischio" sia errato in quanto «il semplice fatto che un prodotto contenga una sostanza chimica non equivale a esporre il singolo ad una sostanza pericolosa»: in questi termini, R. Trager, *California's Prop 65 Controversy*, in *chemistryworld.com*, 16 giugno 2016.

[27] *Consumer Defense Grp. v. Rental Housing Indus. Members*, 137 Cal. App. 4th 1185, 1208 (2006) in cui *l'Attorney General* californiano ha sostenuto che «*it does not serve the public interest to have almost the entirety of the state of California swamped in a sea of generic warning signs*». In questo senso, anche l'editoriale apparso sul *Los Angeles Times* il 30 settembre 2017, ove si fa notare come riempire il consumatore di inutili avvertenze - non correlate alla serietà del rischio - possa avere l'effetto di assuefare il singolo e di non fargli percepire il pericolo proprio nei casi in cui esso sia maggiormente rilevante: *Warning: Too Many Warning Signs are Bad for Your Health*.

[28] Per tutti, C. Polsky - M. Schwarzman, *The Hidden Success of a Conspicuous Law*, cit., 830 e la dottrina ivi citata.

[29] Come notato in dottrina (C. Polsky - M. Schwarzman, *The Hidden Success of a Conspicuous Law*, cit., 839), infatti, il modo in cui i consumatori reagiscono alle avvertenze apposte in forza della *Proposition 65* non dipende solo dalla personale tolleranza al rischio, ma anche dalle alternative disponibili sul mercato: se l'opzione che si pone al consumatore è, ad esempio, tra un pesce che contiene mercurio ed una specie che mostra una minore concentrazione di tale elemento, è probabile che la decisione di acquisto si sposti su quest'ultima.

[30] Denominazione attribuita al Titolo V del *Telecommunication Act* del 1996 che ha inserito una nuova sezione 230 al *Communications Act* del 1934 (47 U.S.C. 230) rubricata «*Protection for private blocking and screening of offensive material*».

"*publisher*" relativamente alle informazioni fornite da terzi[31]; in secondo luogo (ai sensi della sezione 230 (c)(2)), il regime di favore è espressamente esteso a quei prestatori intermedi che operano una moderazione di tali contenuti[32]; infine (ai sensi della sezione 230 (e)(3)), le responsabilità dei prestatori intermedi sono sottratte agli interventi normativi dei governi territoriali: in forza del secondo periodo della sezione 230 (e)(3), infatti, «nessuna responsabilità può essere imposta sulla base di disposizioni statali o locali che non siano conformi a questa sezione[33]».

Con queste poche battute è stata assicurata dal legislatore federale agli intermediari digitali la più ampia possibilità di regolamentare, in piena ed insindacabile autonomia, il flusso dei contenuti generati dai propri utenti, sottraendosi alle doglianze di chi fosse stato danneggiato dalla relativa pubblicazione.

Tale posizione di estremo favore non ha trovato smentite nel momento applicativo. La giurisprudenza statunitense, infatti, ha ininterrottamente interpretato la sezione 230 del CDA come una "*broad immunity*"[34]: sul piano assiologico, le necessità di non indurre forme di censura (la prospettiva è quella del "libero mercato delle idee[35]") e di garantire un Internet sicuro (offrendo agli operatori dell'infrastruttura digitale la possibilità di autoregolamentare l'organizzazione dei contenuti immessi nei propri spazi virtuali) hanno indotto, infatti, i giudici nordamericani ad attribuire agli intermediari della rete poteri di moderazione dei contenuti che sfuggono a ogni tipo di controllo nel merito[36].

Esula dai confini del presente studio l'esame delle diverse implicazioni discendenti dalla sezione 230 CDA nel governo della sfera digitale. E tuttavia, al fine di restituire

---

[31] 47 U.S.C. 230 (c)(1): «*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*».

[32] 47 U.S.C. 230 (c)(2): «*No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (A)*».

[33] 47 U.S.C. 230 (e)(3): «*Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section*».

[34] Nell'elaborazione giurisprudenziale, la sezione 230 CDA è etichettata alternativamente come "*broad immunity*" (*Fair Housing Council v. Roommates.com*, 521 F.3d 1157 9th 1176, Cir. 2008 o "*robust immunity*" (*Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1123 9th Cir. 2003.

[35] Si noti, però, che giurisprudenza e dottrina maggioritaria concordano sul fatto che la sezione 230 CDA non merita necessariamente una copertura costituzionale ai sensi del Primo Emendamento: essa è piuttosto considerata come il frutto di una scelta di *policy* del legislatore tra le tante altrimenti possibili. Sul punto, in giurisprudenza, *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 421 (S.D.N.Y. 2001). In dottrina, R. Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, in *George Washington Law Review*, 76, 2008, 986, 1008; J. M. Balkin, *The Future of Free Expression in a Digital Age*, in *Pepperdine Law Review*, 36, 2009, 427, 434; J. Kosseff, *Defending Section 230: The Value of Intermediary Immunity*, in *Journal of Technology Law & Policy*, 15, 2010, 123, 136; K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in *Harvard Law Review*, 131, 2018, 1598, 1613. Di contro, nel senso, cioè, che la sezione 230 CDA sia una norma sostanzialmente costituzionale, in Note, *Section 230 as First Amendment Rule*, in *Harvard Law Review*, 131, 2018, 2027 ss.

[36] Già l'anno successivo all'entrata in vigore della novella statutaria, con la decisione del caso *Zeran v. America Online Inc*, 958 F. Supp. 1124 (E.D. Va. 1997), si afferma in giurisprudenza un fermo orientamento tendente ad esonerare gli intermediari della rete da qualunque responsabilità, anche ove questi ultimi fossero a conoscenza del fatto illecito dei propri utenti.

almeno l'idea del significato complessivo sottostante a tale norma - ricordata ora come «la legge più importante tra le disposizioni poste a protezione della libertà di espressione in Internet[37]» altre volte come «una vera e propria Magna Carta dell'impunità d'impresa[38]» - e di comprendere appieno la ventata di novità registrabile nella pronuncia da cui questo studio prende le mosse, pare utile accennare ad un recente caso deciso dalla *Supreme Court of California*. Ci si riferisce alla importante decisione resa il 2 luglio 2018 nel caso *Hassell v. Bird*[39], che si mantiene in un ambito di sostanziale continuità interpretativa con una linea giurisprudenziale (federale e statale) ormai ultraventennale e che ben sintetizza la posizione di indiscusso favore garantita ai prestatori dei servizi della rete telematica.

La sentenza, per un osservatore europeo, è degna di nota per almeno due motivi: essa testimonia, infatti, per un verso, quanto la sezione 230 CDA[40] si allontani dall'attuale regolamentazione europea delle responsabilità degli intermediari (incentrata, ai sensi dell'art. 14 della direttiva 2000/31, sulla conoscenza del fatto illecito del terzo da parte dell'intermediario[41]) e, per l'altro, come le prospettive rimediali del singolo siano di fatto limitate - ancora una volta a differenza di quanto avviene nei Paesi membri dell'Unione europea[42] - alla sola reazione che l'ordinamento garantisce nei confronti dell'autore diretto del fatto illecito. Gli intermediari della rete (alla stregua dell'orientamento di favore consolidatosi nella giurisprudenza statunitense che ha ampliato per via interpretativa la portata applicativa della sezione 230 CDA nella direzione che si sta per accennare) non possono, infatti, essere destinatari di alcun ordine di rimozione, nemmeno con riferimento a contenuti già giudicati illeciti.

---

37 A. Kamdar, *CDA 230: The Most Important Law Protecting Internet Speech*, in *Electronic Frontier Foundation*, 6 dicembre 2012; M. Ammori, *The "New" New York Times: Free Speech Lawyering in the age of Google and Twitter*, in *Harvard Law Review*, 127, 2014, 2290.

38 F. Pasquale, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, in *Theoretical Inquiries in Law*, 17, 2016, 494.

39 *Hassell v. Bird*, 5 Cal.5th 522 (Cal. 2018).

40 Giova segnalare come, con riferimento alla tutela dei diritti d'autore, la normativa statunitense di esonero da responsabilità degli intermediari della rete non sia quella della sezione 230 CDA, ma quella della sezione 512 del *Digital Millennium Copyright Act* del 1998. Tale disciplina costituisce un raffinato tentativo di bilanciamento dei diversi interessi giuridicamente rilevanti implicati nell'attuazione dei diritti d'autore nell'ambiente digitale: con riguardo a questo profilo, i diritti protetti, la cui lesione è normativamente contemplata, non sono esclusivamente quelli dell'autore e dell'industria culturale, ma anche quelli degli operatori dell'infrastruttura della rete e quella dei fornitori dei contenuti.

41 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico"). Si noti che il regime di esonero da responsabilità degli intermediari della rete di cui alla direttiva 2000/31/CE è stato pressoché mantenuto inalterato nel nuovo regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali ("Regolamento sui servizi digitali"). Nell'ambito del Regolamento – che si applicherà a decorrere dal 17 febbraio 2024 – sono, infatti, sostanzialmente riprodotte (agli artt. 4 ss.) le disposizioni di esonero da responsabilità per i prestatori dei servizi di base della rete contenute nella direttiva 2000/31/CE.

42 Come precisato sin dal considerando 45 della direttiva 2000/31/CE, infatti, le limitazioni alla responsabilità dei prestatori intermedi lasciano impregiudicata la possibilità di azioni inibitorie: «siffatte azioni inibitorie possono, in particolare, essere ordinanze di organi giurisdizionali o autorità amministrative che obbligano a porre fine a una violazione o impedirla, anche con la rimozione dell'informazione illecita o la disabilitazione dell'accesso alla medesima». Anche la possibilità di esperire azioni inibitorie nei confronti dei prestatori di servizi intermediari è confermata dal regolamento (UE) 2022/2065 sui servizi digitali: in particolare, il considerando 25.

È proprio questo il punto su cui la sentenza californiana fa definitiva chiarezza. In *Hassell v. Bird* la fattispecie aveva ad oggetto il danno causato al singolo da diverse recensioni diffamatorie pubblicate da un terzo su *Yelp.com*, un sito web per la valutazione di attività commerciali e servizi professionali, noto per i giudizi negativi molto personali ed estremi dei propri utenti. Le recensioni in questione concernevano l'attività professionale prestata da un avvocato, il quale, a tutela della propria immagine aveva ottenuto, nei confronti dell'autore diretto del fatto illecito (convenuto per *false light* e per *intentionally inflicted emotional distress*), una sentenza di condanna al risarcimento del danno e un ordine di rimozione delle affermazioni ingiuriose. L'ordine di rimozione, rivolto in prima battuta all'autore dei commenti diffamatori, estendeva la propria portata applicativa anche al sito web (non convenuto), il quale avrebbe dovuto eliminare i commenti già giudicati illeciti entro un tempo prestabilito.

Su ricorso promosso da *Yelp.com* (diretto all'annullamento dell'*injunction*), la *Supreme Court* della California ha chiarito la portata applicativa della immunità concessa dal legislatore federale del 1996 agli intermediari della rete. La posizione assunta dal Collegio è che la difesa ad essi spettante si estende tanto ad ogni profilo risarcitorio, quanto alla soggezione ad ordini inibitori.

Il ragionamento sotteso a questa impostazione è, invero, che il profilo rimediale dell'azione inibitoria con imposizione di obblighi di fare (anche limitati alla rimozione di contenuti già giudicati diffamatori) potrebbe avere - al pari della tipica reazione aquiliana consistente nel risarcimento del danno - l'effetto di incentivare affrettate forme di censura.

Anche nel caso in cui fosse operativamente semplice attuare un ordine di fare puntuale e mirato (consistente nella semplice rimozione di specifici contenuti già giudicati diffamatori) - è l'intelaiatura logica dell'intera decisione -, la relativa esecuzione potrebbe minacciare la capacità di sopravvivenza dell'intermediario digitale, che si troverebbe esposto a "*contempt proceedings*[43]" in caso di inottemperanza: ordini di rimozione apparentemente semplici - è il percorso argomentativo dei giudici di vertice - potrebbero generare un contenzioso importante su questioni quali la loro validità, la rispettiva portata o il modo in cui debbano essere concretamente attuati[44].

Da quanto precede, ben si comprende come le conseguenze dirette di una siffatta impostazione siano univoche (nonostante uno strisciante disagio espresso, più o meno velatamente, tra le righe della decisione[45]): nella normativa statunitense, la tutela del singolo (danneggiato dall'uso che i terzi abbiano fatto degli spazi telematici) è, dunque, esclusivamente affidata ai profili rimediali esperibili nei soli confronti degli autori diretti del fatto illecito.

---

[43] Sull'istituto del *contempt of court,* si veda V. Varano, *Contempt of Court*, in *Digesto/Pen.*, III, 1989, 107 ss.; *Injunction*, in *Digesto/Priv.*, 1993, 487 ss.; A. Frignani, *L'injunction nella Common Law e l'inibitoria del diritto italiano*, Milano, 1974.

[44] *Hassell v. Bird*, cit., 545.

[45] (Oltre all'opinione dissenziente), la seguente affermazione resa in chiusura dell'*opinion* di maggioranza (*Hassell v. Bird*, 5 Cal. 5th 522, 548): «*Even as we conclude that Yelp is entitled to immunity, we echo Barrett […] in emphasizing that our reasoning and result do not connote a lack of sympathy for those who may have been defamed on the Internet. Nevertheless, on this record it is clear that plaintiffs' legal remedies lie solely against Bird, and cannot extend - even through an injunction - to Yelp*».

4. Il caso *Lee v. Amazon*: la decisione della *Trial Court*

Acquisiti tutti i dati normativi rilevanti, è ora possibile passare all'esame della fattispecie posta all'attenzione del giudice californiano nel caso *Lee v. Amazon*[46]. Il giudizio ha tratto spunto dall'iniziativa di un consumatore che ha fatto valere il "*right-to-know*" attribuitogli dalla *Proposition 65* relativamente alla presenza di mercurio in alcune creme schiarenti per il viso, acquistate sul sito web di Amazon da venditori indipendenti.
L'elemento che rende importante, dal punto di vista della tutela del consumatore, l'azione intentata dall'acquirente, diretta a far valere le sanzioni civili ed i provvedimenti inibitori previsti dalla normativa statale, è la circostanza che quest'ultimo abbia fatto valere la propria situazione giuridica pretensiva nei confronti non dei produttori, dei distributori o degli importatori dei cosmetici, ma direttamente della piattaforma di *e-commerce*.
Si tratta, dunque, del primo tentativo di cooptare direttamente nella tutela offerta al consumatore dalla *Proposition 65* proprio quel soggetto che - permettendo un accorciamento della catena di commercializzazione - ha reso possibile ad un numero senza precedenti di produttori e di venditori (che difficilmente sarebbero riusciti a piazzare i rispettivi beni attraverso l'apparato distributivo tradizionale) di avere accesso ad una enorme platea di potenziali acquirenti. Non a caso, i cosmetici caduti sotto i riflettori dell'attenzione del circuito giudiziale californiano erano tutti fabbricati in Paesi lontani e - prima ancora che essere assoggettati al regime informativo della *Proposition 65* - non avrebbero potuto essere importati nel mercato statunitense, stante un divieto federale di produzione di creme per il viso contenenti, come principio attivo, mercurio.
Il giudice di primo grado[47] ha ritenuto che l'azione promossa dal consumatore non fosse accoglibile. A giudizio della *Trial Court*, la piattaforma digitale sarebbe stata protetta dall'insorgere di qualsivoglia forma di responsabilità ai sensi della sezione 230 CDA. Le responsabilità fatte valere dal consumatore, secondo il giudice di prime cure, sarebbero discese, infatti, proprio dal "trattare" l'operatore digitale alla stregua di un editore ("*publisher*"), che dà diffusione a contenuti altrui: responsabilità, pertanto, escluse dalla normativa federale del 1996. L'obbligo che il consumatore afferma essere stato violato sarebbe, infatti, ricollegabile - secondo questa prospettiva - al mancato monitoraggio dei contenuti generati da un versante dei propri utenti (i venditori terzi che affollano, con i propri annunci di vendita, la piattaforma Amazon).

5. La sentenza resa dalla *Court of Appeal* l'11 marzo 2022

La domanda che si pone, su ricorso del consumatore, alla *Court of Appeal* californiana è se l'obbligo di avvertenza eventualmente gravante in capo al prestatore di servizi telematici discenda dal ruolo intermedio da esso assunto nel dare diffusione a contenuti altrui (e, dunque, dall'aver rivestito, rispetto a questi ultimi, le funzioni del

[46] *Lee v. Amazon.com, Inc.*, 76 Cal. App. 5th 200.

[47] *Superior Court of Alameda County*, RG. 14738130, Giudice R.D. Mc Guiness (gennaio 2019)

"*publisher*") o, piuttosto, da una fonte diversa e, in particolare, dal ruolo attivamente svolto, nell'ambito della propria attività di impresa, nella immissione del bene nel giro distributivo.

Posta sotto questa seconda luce, la questione relativa alle responsabilità dell'intermediario acquista per il giudice dell'impugnazione una nuova consistenza. Ed invero, non si tratta più di verificare quali azioni l'intermediario – nella sua veste di "*publisher*" – sia chiamato ad adottare (nell'ambito della sua discrezionalità editoriale) relativamente ai contenuti riferibili a terzi: «decidere se pubblicare, rimuovere o ritardare la pubblicazione[48]» (nel caso esaminato, le descrizioni dei prodotti in vendita, prive degli avvisi ex *Proposition 65*); azioni, queste, tutte protette dalla sezione 230 del CDA. Si tratta, piuttosto, di appurare se l'intermediario, per il fatto "proprio" di concorrere - insieme ad altri soggetti - alla immissione nel giro distributivo del singolo bene, possa essere inteso come autonomo destinatario degli obblighi informativi previsti dalla normativa californiana.

Analizzando il problema da questa diversa prospettiva, ben ci si accorge, infatti, come l'inserimento dell'annuncio di vendita da parte del venditore terzo costituisca, sul piano causale, solo il lontano antecedente logico di una eventuale responsabilità della piattaforma, chiamata a rispondere per il fatto proprio, posto in essere in un momento successivo alla pubblicazione dell'inserzione.

L'inquadramento della questione nei termini appena indicati è in qualche modo facilitato dalla circostanza che la *Proposition 65* è stata pensata, sin dalla sua formulazione originaria risalente al 1986, in termini molto ampi, atti a includere nel proprio bacino operativo una cerchia quanto più estesa di soggetti che rischiano di esporre il consumatore a certe sostanze tossiche. Ai sensi della legislazione del 1986, infatti, destinataria, dal lato passivo, dell'obbligo di avvertire il consumatore è, infatti, «[*any*] *person in the course of doing business*[49]».

L'alternativa tra la responsabilità e l'irresponsabilità del prestatore intermediario corre, dunque, sul filo di una distinzione molto sottile, ma non per questo meno importante. Se è vero, infatti, che la responsabilità di Amazon è correlata alle informazioni fornite da terzi (e, in particolare, alla descrizione dei prodotti offerta dai venditori indipendenti senza le dovute avvertenze[50]), è anche vero che tale responsabilità è fatta valere non nella veste editoriale della piattaforma (per mancato controllo dei contenuti altrui), ma nella veste di un operatore commerciale che abbia assunto obblighi indipendenti ai sensi della *Proposition 65* per il fatto proprio.

A questo punto, è ben chiaro, allora, come il dovere violato (che può dar luogo alle sanzioni civili ed all'ordine inibitorio di non mettere in commercio il bene se non con la prescritta avvertenza) non consista nel non aver intrapreso azioni quali, a titolo meramente esemplificativo, il ritiro o la modificazione dei contenuti forniti dai venditori

---

48 In questi termini, *Zeran v. America Online Inc*, 129 F.3d, cit., 330. Nello stesso senso, *Stoner v. eBay, Inc.* (56 USPQ2d 1852 (2000, Cal Super Ct) (

49 Cal Health & Safaty Code 25249.6, cit.

50 Ed invero, se si scorrono le clausole contrattuali che vincolano piattaforma e venditori indipendenti, ci si avvede di come Amazon, nei formulari contrattuali predisposti unilateralmente, renda questi ultimi unicamente responsabili dell'apposizione delle avvertenze di cui alla *Proposition 65*.

terzi (azioni che equivarrebbero all'«esercizio delle tradizionali funzioni editoriali»). Il dovere la cui violazione fa scattare la sanzione dell'ordinamento consisterebbe, piuttosto, nell'obbligo di avvertire il consumatore, indipendentemente dalle omissioni altrui. Da questa prospettiva, secondo i giudici d'Appello, non rileverebbe neppure il fatto che Amazon non sarebbe stata sanzionabile, ove il venditore avesse correttamente adempiuto al proprio dovere di informare compiutamente il singolo in ottemperanza alla *Proposition 65*.

Ciò che si chiede alla piattaforma non è, infatti, verificare se, nelle specifiche tecniche del prodotto o nella pagina web dedicata, il fornitore abbia inserito le relative avvertenze; si richiede, piuttosto, ove Amazon abbia una conoscenza (effettiva o "costruttiva"[51]) del potenziale rischio per il consumatore, di adempiere autonomamente al relativo obbligo. Che poi la piattaforma decida - prima di fornire essa stessa l'avvertenza - di controllare l'inserzione del prodotto per verificare se il venditore terzo abbia effettivamente adempiuto a tale dovere o (per propria scelta commerciale) di rimuovere il prodotto dai propri cataloghi non significa che la normativa statuale abbia imposto al fornitore del "servizio informatico interattivo" di operare alla stregua di un editore relativamente ai contenuti generati dai propri utenti: la *Proposition 65* non richiede ad Amazon di agire nei sensi appena indicati.

La soggezione della piattaforma di *e-commerce* agli obblighi di cui alla *Proposition 65* trova la propria scaturigine nella condotta dello stesso intermediario. Ed invero, la soluzione adottata dal giudice del gravame, in maniera conforme alla richiesta dell'istante, è orientata sulla circostanza che la stessa piattaforma avrebbe "spinto" il prodotto sino a farlo arrivare al consumatore finale. Ed infatti, Amazon - si legge nella pronuncia - si è inserita tra venditore e consumatore nella catena di distribuzione del prodotto: la piattaforma ha attirato il secondo sul proprio sito web, gli ha fornito un elenco dettagliato delle creme schiarenti per la pelle disponibili sul mercato, ha ricevuto il pagamento del prezzo, ha applicato le commissioni di vendita, ha imposto che le eventuali comunicazioni con il venditore passassero attraverso il filtro della piattaforma, ha gestito i resi e le restituzioni di prezzo, ha accettato il possesso del prodotto, lo ha stoccato nei propri magazzini e lo ha spedito al consumatore.

A tale stregua, è la conclusione dei giudici dell'impugnazione, la tesi della piattaforma di porsi all'esterno della catena distributiva è semplicemente «insostenibile[52]»: al di là di ogni dato puramente nominalistico («non importa se il fornitore del "servizio informatico interattivo" possa essere propriamente definito come "rivenditore", "distributore"

[51] L'elemento soggettivo necessario ad integrare la condotta sanzionata è un punto molto dibattuto nella giurisprudenza californiana: in particolare, non vi è uniformità di vedute, in assenza di definizioni normative che chiariscano cosa debba intendersi con la locuzione "esporre consapevolmente" il consumatore alle sostanze tossiche individuate dall'*Office of Environmental Health Hazard Assessment*. Segnatamente, non è chiaro se sia necessaria, in capo al soggetto obbligato, una "conoscenza effettiva" o se invece sia sufficiente una conoscenza solo "presumibile" ("*constructive knowledge*"); conoscenza, quest'ultima, attribuibile a chi sia chiamato ad agire con "*reasonable care or diligence*" nei confronti dei consumatori. Riguardo a questo punto, il giudice di prime cure – contrariamente alla posizione maggiormente favorevole al consumatore poi accolta dalla *Court of Appeal* (*Lee v. Amazon.com, Inc.*, cit., 228) – ha ritenuto che destinatario dell'obbligo di avvertenza fosse esclusivamente colui che avesse una conoscenza effettiva.

[52] *Lee v. Amazon.com, Inc.*, cit., 243

o semplice "facilitatore" [53]»), la condotta di Amazon è ritenuta «indispensabile[54]» nel far circolare il prodotto e nell'accompagnarlo sino al consumo finale.

Residuano, nell'impianto argomentativo della sentenza, almeno altre due ragioni che convergono verso l'esito finale della imposizione della responsabilità, che vale la pena riportare.

Innanzitutto, ove si accettasse una lettura della sezione 230 CDA nel senso di schermare i fornitori dei "servizi informatici interattivi" dagli obblighi che su di essi gravano in forza della *Proposition 65* per le azioni a loro direttamente riferibili, si attribuirebbe a tali operatori commerciali un indiscutibile vantaggio competitivo che falserebbe la concorrenza: si allevierebbero, infatti, a vantaggio dei soli intermediari digitali, quegli oneri che gravano, invece, su qualunque altro venditore caratterizzato da strutture aziendali fisiche in cui i clienti possono recarsi di persona per vedere ed acquistare i prodotti («*brick-and-mortar purveyor of the same product*[55]»). L'attribuzione di un vantaggio concorrenziale di questo tipo non è riconducibile, secondo i giudici dell'impugnazione, alle finalità della norma esonerativa da responsabilità del 1996[56].

Inoltre - e così passiamo all'esame della seconda ragione - una siffatta interpretazione si porrebbe in stridente contrasto con la salvaguardia degli interessi pubblici tutelati dalla *Proposition 65* proprio in quei casi in cui ve ne sarebbe più di bisogno. Ed infatti - è il ragionamento della *Court of Appeal* -Amazon rende possibile ad un numero incalcolabile di venditori (che non sarebbero nelle condizioni di piazzare i propri prodotti nei negozi al dettaglio tradizionali) di raggiungere un vasto pubblico di potenziali clienti: Amazon metterebbe, pertanto, a disposizione dei consumatori – ed in particolare dei consumatori più vulnerabili - beni insicuri prodotti in Paesi lontani. In tali circostanze, tale operatore economico - che trae profitto anche grazie alla vendita di beni potenzialmente nocivi per la salute dei singoli - è l'unico attore del ciclo produttivo e di commercializzazione che può essere effettivamente perseguito per la violazione dell'obbligo di fornire le avvertenze previste dalla legge[57]. A tale stregua, è la conclusione della *Court*

[53] Ivi, 249

[54] *Ibidem.*

[55] Ivi, 259.

[56] Ivi, 258.

[57] Vale la pena di segnalare un argomento che non trova espressa menzione nella pronuncia, ma che potrebbe avere influito sulla decisione finale: la circostanza, cioè, che nel caso affrontato, la Corte, nell'esaminare la portata applicativa della sezione 230 CDA, non si sia occupata della libertà di espressione in generale, ma di una sua manifestazione ben precisa: il cosiddetto "*commercial speech*". Com'è noto, nel diritto statunitense la libertà di parola si atteggia a diritto incomprimibile e le eventuali restrizioni ad essa apposte, altre rispetto alle poche forme di espressione vietate, sono ammesse solo in casi limite; casi limite da vagliare alla luce del cosiddetto *strict scrutiny test*: segnatamente, tali ipotesi eccezionali devono perseguire un «pressante interesse pubblico» ed essere «strettamente cucite intorno ad esso» (sul punto, *Time, Inc. v. Hill*, 385 U.S. 374 (1967)). Destinatario di una soglia di tutela relativamente inferiore rispetto a quella assicurata in generale alla libertà di espressione dallo *strict scrutiny test* è, invece, il "*commercial speech*", ovvero quella forma di espressione che – secondo quanto si legge in *Virginia Pharmacy Board v. Virginia Citizens Consumer Council*, 425 U.S. 748 (1976) – appare «*related solely to the economic interests of the speaker and its audience*». La protezione da accordare in tale caso dipende sia dalla natura dell'espressione (e, in particolare, dalla funzione informativa riconnessa alla pubblicità), sia dagli eventuali interessi pubblici sottesi alla sua regolamentazione: a tale stregua possono essere immaginabili forme di restrizioni nei confronti di comunicazione suscettibili di ingannare il consumatore ovvero attinenti ad attività illecite. Ove, però, la comunicazione non sia né fuorviante, né correlata ad attività

of Appeal, «isolare Amazon dalle responsabilità per il fatto proprio, riconnesse agli obblighi discendenti dalla *Proposition 65* […] sarebbe anomalo[58]».

6. Una traiettoria giurisprudenziale proclive a individuare strumenti di regolazione delle piattaforme digitali

Per comprendere la diversa prospettiva adottata dalla *Court of Appeal* californiana rispetto alla decisione del giudice di prime cure, è utile richiamare una linea di decisioni, rese negli ultimi tre lustri, che, sulla base di questo originale modo di argomentare, tendono a discostarsi dalla lettura tradizionale della sezione 230 CDA (quale normativa volta a stabilire una sorta di immunità generale per gli intermediari digitali) e a rimettere in discussione l'approccio "eccezionalista[59]" (sotteso alla normativa federale del 1996), che affida il governo del cyberspazio all'autoregolamentazione.

Il punto di partenza di questa carrellata giurisprudenziale può essere rintracciato nella sentenza della *United States Court of Appeals for the Ninth Circuit* nel caso *Barnes v. Yahoo!*[60], in cui è stata aperta per la prima volta una frattura nel classico modo di intendere il settore della intermediazione digitale come un ambiente completamente protetto dalla regolamentazione statale.

Nella decisione resa il 7 maggio 2009 l'intermediario digitale (la piattaforma *Yahoo!*) è stato, infatti, condannato al risarcimento del danno per non aver soppresso dai propri spazi digitali i nudi fotografici caricati dall'ex partner dell'attrice, che aveva visto la propria immagine, violata nella propria sfera più intima, diffondersi in maniera "virale".

A determinare la risposta sanzionatoria dell'ordinamento non è stato, però, l'inadempimento del generico dovere gravante sull'editore di non dar corso alla pubblicazione di contenuti ricattatori (e, dunque, la scelta editoriale di *Yahoo!* di non oscurare gli scatti fotografici pubblicati da un terzo per perpetrare una vendetta sessuale: così argomentando il sentiero rimediale sarebbe stato sbarrato dalla sezione 230 CDA), ma l'inadempimento di una specifica promessa contrattuale che la piattaforma aveva assunto nei confronti della ricorrente. Ed infatti, il giorno prima che un'emittente televisiva

illecite, i poteri di regolamentazione del "*commercial speech*" sono destinati ad assottigliarsi. Nella sentenza resa nel caso *Central Hudson Gas & Elec. v. Public Svc. Comm'n*, 447 U.S. 557 (1980), infatti, è stato precisato che, per verificare la legittimità dell'intervento pubblico diretto a limitare il "*commercial speech*", occorre appurare che sussista un rapporto di proporzionalità tra gli interessi da proteggere ed i mezzi prescelti e che questi ultimi siano effettivamente in grado di perseguire lo specifico interesse generale cui la libertà di espressione si trova ad essere subordinata: non sarebbe, infatti, sufficiente che essi forniscano un contributo inefficace o indiretto.

[58] *Lee v. Amazon.com, Inc.*, cit., 259, ove si legge «*Insulating Amazon from liability for its own Proposition 65 obligations in these circumstances would be anomalous*».

[59] Per tutti, E. Goldman, *Why Section 230 is Better than the First Amendment*, in *Notre Dame Law Review Reflection*, 95, 2020, 33 ss.; *California Courts Continue to Trim Section 230's Protection for Amazon's Marketplace (and Everyone Else) - Lee v. Amazon*, in *Technology and Marketing Law Blog*, 16 marzo 2022. Più in generale, sulle giustificazioni sottese a questo approccio, M. Tushnet, *Internet Exceptionalism: An Overview from General Constitutional Law*, in *William & Mary Law Review*, 1637, 2015, 1665.

[60] *Barnes v. Yahoo!*, 570 F. 3d 1096 9th Cir. 2009.

denunciasse l'accaduto, l'intermediario promise alla vittima della vendetta sessuale la rimozione dei contenuti segnalati.

In questo primo tentativo di elaborare strumenti di regolazione delle piattaforme, l'obiettivo è, pertanto, raggiunto dalla *Court of Appeal* configurando una responsabilità dell'intermediario a titolo di inadempimento contrattuale: a tale stregua, il mancato adempimento della promessa (e, dunque, dell'obbligo volontariamente assunto di rimozione) ha determinato indirettamente il superamento della regola di irresponsabilità fissata alla sezione 230 CDA.

Alla medesima logica (l'inadempimento di un obbligo non direttamente ricollegabile ai doveri gravanti sull'editore), risponde la sentenza resa dalla *United States Court of Appeals for the Ninth Circuit* nel caso *Doe v. Internet Brands, Inc.*[61].

Con la pronuncia resa il 31 maggio 2016, la *Court of Appeal* ha ribaltato la decisione di primo grado, secondo cui l'azione intentata a titolo di *negligence* da un'aspirante modella nei confronti di un sito web per non averla avvertita del fatto che la piattaforma fosse adoperata da due noti predatori sessuali (che la avevano convocata per una falsa audizione al fine di violentarla) fosse impedita dalla sezione 230 CDA. Per i giudici dell'impugnazione, infatti, la doglianza dell'attrice - a differenza di quanto deciso dal primo giudice - non era incentrata sul ruolo di "*publisher*" della piattaforma convenuta: l'azione era stata, infatti, intentata non per non aver rimosso i contenuti dei propri utenti o per non aver effettuato alcuna moderazione di essi, ma per non aver adempiuto ai doveri di avvertimento che il diritto statutario californiano[62] impone a chiunque (ivi incluse, dunque, le piattaforme elettroniche), al corrente di un determinato pericolo (nella fattispecie affrontata, il fornitore del "servizio informatico interattivo" era a conoscenza dello schema criminale più volte messo in atto dai due stupratori), si trovi in una "*special relationship*" con la vittima potenziale del fatto illecito altrui.

Una volta enunciata questa preliminare regola operativa, il consequenziale passo successivo fu quello di chiarire come un obbligo siffatto non avrebbe influito in alcun modo sul ruolo editoriale dell'intermediario: il dovere di mettere in guardia i propri utenti non avrebbe comportato per l'intermediario l'obbligo né di rimuovere i contenuti dei terzi né tantomeno di modificarli. L'obbligo di avvertire le potenziali vittime dello schema criminale avrebbe potuto essere facilmente soddisfatto pubblicando un avvertimento sullo stesso sito web o inviando un'*e-mail* ai propri iscritti.

Sulla base di un ragionamento affine, in *HomeAway.com v. City of Santa Monica*[63] la *United States Court of Appeals for the Ninth Circuit*, con sentenza resa il 12 ottobre 2018, ha respinto il ricorso proposto congiuntamente da *HomeAway.com* e *Airbnb Inc* contro la decisione di primo grado che aveva riconosciuto la validità dell'ordinanza emessa dal comune di Santa Monica che, al fine di impedire una deregolamentazione nel mercato del turismo, prescriveva che le piattaforme digitali per gli affitti a breve termine auto-

[61] *Doe v. Internet Brands, Inc.*, 824 F.3d 846, 2016 U.S. App. LEXIS 9969.

[62] Tali doveri hanno trovato consacrazione per la prima volta sul piano giurisprudenziale *Tarasoff v. Regents of Univ. of California*, 17 Cal.3d 425, 435, 131 Cal. Rptr. 14, 551 P.2d 334 (1976)) e trovano oggi fondamento nel diritto statutario, ai sensi del Cal. Civ. Code 43.92; normativa, quest'ultima, che crea una «*special relationship to either the person whose conduct needs to be controlled or […] to the foreseeable victim of that conduct*».

[63] *HomeAway.com v. City of Santa Monica*, 918 F.3d 676.

rizzassero le transazioni esclusivamente con i locatori che risiedessero nell'unità abitativa locata. A tal fine, le piattaforme - prima di autorizzare la conclusione dell'affare - avrebbero dovuto verificare se i locatori figurassero o meno in un apposito registro pubblico.

Gli obblighi posti dall'ordinanza comunale in capo ai fornitori del "servizio informatico interattivo" (tali sono sicuramente, per il giudice di secondo grado, gli intermediari digitali che permettono l'incontro tra chi offre in locazione breve il proprio appartamento e chi è alla ricerca di una tale soluzione abitativa) non avrebbero prescritto l'adozione di alcuna scelta editoriale relativamente ai contenuti pubblicati in autonomia dai locatori: qualsiasi annuncio di affitto a breve termine (anche l'inserzione di chi non figurava nel registro dei residenti) avrebbe potuto permanere sul sito e la scelta editoriale di non intervenire su di essi o di non rimuoverli non avrebbe potuto far insorgere alcuna responsabilità in capo alle piattaforme ricorrenti. Queste ultime sarebbero state tenute esclusivamente a non autorizzare la conclusione delle transazioni con i locatori non figuranti nell'apposito registro.

In questa logica, il mero fatto che la "rimozione" degli annunci dei non residenti fosse (dal punto di vista del modello imprenditoriale adottato dalle due piattaforme) la scelta maggiormente conforme alla ragionevolezza commerciale («il buon senso spiega» - fu la tesi sostenuta dagli intermediari - come non si possa «lasciare un sito web pieno zeppo di annunci non prenotabili[64]») non avrebbe mutato la sostanza dell'obbligo imposto dall'ordinanza municipale: quest'ultima non imponeva alcuna precisa scelta editoriale con riferimento ai singoli annunci. A tale stregua, la decisione, adottata in piena autonomia dalle due piattaforme, di rimuovere le inserzioni di coloro che non risiedessero nel comune non avrebbe potuto avere l'effetto indiretto di richiamare l'operatività della sezione 230 CDA. L'ordinanza non richiedeva alle piattaforme di monitorare i contenuti dei terzi (le inserzioni fornite dagli *host*[65]), ma solo un controllo incrociato, prima della conclusione della transazione, con un registro pubblico su cui le piattaforme non avevano «alcun controllo editoriale[66]». Come schiettamente affermato dai giudici di secondo grado, la radice di questa impostazione va colta nella esigenza di non creare nella sfera digitale «una terra di nessuno, senza regole, né controlli[67]».

Per chiudere sul punto, conviene indirizzare l'attenzione su un recente caso, in cui traspare nettamente l'atteggiamento proclive ad elaborare (a legislazione federale invariata) strumenti di regolazione delle piattaforme digitali. In *Bolger v. Amazon.com*[68], la giurisprudenza californiana si è trovata ad affrontare il tema della imputabilità della responsabilità da prodotto difettoso alle piattaforme del commercio elettronico. Il

---

64 Ivi, 683.

65 Ivi, 683: «*The Ordinance does not proscribe, mandate, or even discuss the content of the listings that the Platforms display on their website*».

66 *Ibidem:* «*While keeping track of the city's registry is "monitoring" third-party content in the most basic sense, such conduct cannot be fairly classified as "publication" of third-party content. The Platforms have no editorial control over the registry whatsoever*».

67 Ivi, 681.

68 *Bolger v. Amazon.com, LLC* (2020) 53 Cal. App.5th 431.

problema fu dibattuto, con esiti opposti a quelli cui era pervenuta la *Trial Court*[69], dalla *Court of Appeal*[70]. Nell'ambito di un'azione intentata da un consumatore nei confronti di Amazon per le lesioni personali subite a causa della esplosione della batteria acquistata per il proprio computer portatile sulla omonima piattaforma digitale da un venditore cinese, i giudici statali di secondo grado[71] hanno ritenuto che l'intermediario dovesse rispondere a titolo di *strict liability* per il danno cagionato dalla difettosità del prodotto e che - elemento che maggiormente rileva dal nostro punto di vista - la relativa azione non fosse preclusa dalla sezione 230 CDA.

Nell'impianto motivazionale della sentenza, infatti, la responsabilità della piattaforma nei confronti del danneggiato è messa in correlazione non con il ruolo da essa assunto nella disseminazione di informazioni fornite da terzi (le offerte e le schede prodotto direttamente riferibili al venditore terzo), ma con la partecipazione "attiva" alla vendita, attraverso azioni, quali l'elaborazione dei pagamenti, l'immagazzinamento e la spedizione[72].

La pubblicazione dell'annuncio di vendita sta, per così dire, sullo sfondo; non in primo piano come l'elemento che conduce *recta via* alla responsabilità. La doglianza del consumatore, per la *Court of Appeal*, è, infatti, incentrata sulla partecipazione diretta della piattaforma allo scambio e sul ruolo da essa svolto nella catena negoziale nel portare il prodotto al consumatore finale[73].

In questa prospettiva, si mette in risalto, in primo luogo, come Amazon abbia agito da intermediario tra un fornitore a monte e il consumatore a valle esercitando un controllo "fisico" sul prodotto rivelatosi difettoso: la piattaforma ha evaso direttamente l'ordine del consumatore finale, è entrata in possesso del bene difettoso, lo ha immagazzinato presso un proprio deposito, lo ha imballato e lo ha consegnato al consumatore[74]. In secondo luogo, sono le circostanze peculiari della regolazione dei rapporti intercorrenti con il venditore del prodotto difettoso e con il consumatore finale che meritano, per la Corte, la massima considerazione per procedere all'espansione della cerchia dei soggetti responsabili in *tort* per il danno subito dal singolo. Per la *Court of*

---

[69] *Bolger v. Herocell Inc*, *Superior Court of San Diego County*, No. 37-2017-00003009-CU-PL-CT Giudice R. Trapp. (7 febbraio 2019)

[70] *Bolger v. Amazon.com, LLC*, cit.

[71] In primo grado, la piattaforma fu estromessa dal processo, sostenendosi che la responsabilità oggettiva da prodotto difettoso non avrebbe potuto trovare applicazione nei confronti di un mero fornitore di servizi che non aveva distribuito, prodotto o venduto il bene in questione.

[72] A titolo chiarificatore, la *Court of Appeal* ha precisato la differenza intercorrente tra il caso adesso esaminato e la nota decisione resa in *Gentry v. eBay* 121 Cal. RPTR. 2d 703 (Cal. Ct. App. 2002): in quella fattispecie era caduto sotto le lenti di osservazione del circuito giudiziale il sistema di valutazione di *eBay*, che aveva attribuito giudizi positivi a chi vendeva memorabilia sportive riportanti firme falsificate e certificati di autenticità contraffatti. Nel lontano 2002, la *Court of Appeal*, non condivise la tesi dell'acquirente deluso, secondo cui *eBay* fosse un fornitore di contenuti (e non un mero intermediario), quantomeno con riferimento ai sistemi di valutazione dell'affidabilità dei venditori. Per la Corte, infatti, i meccanismi di attribuzione dei *feedback* adottati dalla piattaforma erano incentrati esclusivamente sui giudizi forniti dagli utenti. Giocoforza la 230 del *Communications Decency Act* avrebbe immunizzato la piattaforma da responsabilità: quest'ultima, infatti, si era fatta "portavoce" di contenuti confezionati da terzi.

[73] *Bolger v. Amazon.com, LLC*, cit., 438.

[74] Ivi, 452.

Appeal, la piattaforma "controlla", infatti, ogni aspetto della transazione dal versante sia del consumatore sia del venditore[75].
Riguardata da questo punto di osservazione, la mera indicizzazione dei prodotti del venditore terzo non è certo il titolo della responsabilità di Amazon: le rivendicazioni dell'attore - è il ragionamento della *Court of Appeal* - non richiedono che l'interprete "tratti" Amazon come "*speaker*" o "*publisher*" dei contenuti forniti dal venditore. A tale stregua, lo stesso annuncio di vendita non è determinante ai fini della responsabilità: non si chiede alla piattaforma di accertare se esso sia falso o fuorviante[76]. La fondatezza della pretesa risarcitoria si giustifica esclusivamente in funzione della partecipazione diretta di Amazon alla catena di produzione e distribuzione del prodotto difettoso.

7. Brevi e conclusive osservazioni comparatistiche sulla portata delle trasformazioni in atto nel governo delle piattaforme digitali

La sentenza esaminata in questo studio e le decisioni considerate nel paragrafo precedente sembrano indicare, se non una vera e propria svolta regolatoria nel complesso tema della *governance* di internet, l'apertura (nel momento applicativo) di una importante frattura nella visione *cyber libertarian* delle politiche digitali adottata in chiusura del secolo scorso dal legislatore statunitense.
Sebbene vada debitamente segnalato in forma chiarificatrice che i casi prima riportati costituiscono, in ultima analisi, circoscritte eccezioni al principio di ordinaria irresponsabilità, non si può non registrare una importante novità nel governo della sfera digitale: l'apertura di una crepa nel *laissez-faire* cibernetico della prima ora.
Occorre ancora dire che il principio di *self-regulation*, sottostante alla riforma del 1996, era stato elaborato per proteggere i fornitori di servizi di *hosting* e gli *Internet service providers* dalle responsabilità relative ai dati e ai contenuti pubblicati dagli utenti sui *server host* o scambiati attraverso le reti di telecomunicazione; non invece per tutelare altri attori economici, che in quegli anni non erano ancora compiutamente apparsi sulla scena dell'innovazione trainata da Internet: le piattaforme digitali.

[75] Con riguardo al consumatore, la Corte osserva che «*Amazon* "*owns*" *the customer*»: ed invero, la piattaforma attrae i consumatori sul proprio sito, proponendo offerte speciali e programmi in abbonamento ("Amazon Prime") che permettono l'accesso a offerte esclusive e consegne celeri e gratuite; li vincola ad interagire direttamente con la piattaforma per effettuare l'ordine del prodotto e per pagare il prezzo di acquisto; ne gestisce le comunicazioni con il venditore sia nella fase che precede l'acquisto (nel caso in cui abbia una domanda da porre al venditore) sia in quella successiva (nel caso in cui sia sorto un problema). Relativamente al venditore, il ruolo di Amazon è ritenuto ancora più pervasivo. Il venditore che utilizza la logistica della piattaforma – pone in rilievo la Corte – non ha un rapporto né diretto né indiretto con il consumatore: nella maggior parte dei casi, tra venditore e acquirente non intercorrono comunicazioni; il venditore apprende che una vendita è stata effettuata semplicemente da una notifica da parte della piattaforma; Amazon decide in autonomia se consentire o meno il completamento della transazione; le eventuali domande del consumatore rivolte al venditore sono anonimizzate e gestite attraverso un servizio di messaggistica interno; è fatto divieto al venditore di comunicare altrimenti con il consumatore, di richiedere forme alternative di pagamento, di influenzare le decisioni di acquisto di quest'ultimo o di utilizzare le sue informazioni per scopi promozionali.

[76] *Bolger v. Amazon.com, LLC*, cit., 465.

Se osservata con specifico riferimento a questo aspetto dell'innovazione digitale, la traiettoria giurisprudenziale esaminata in questo studio sembra prestarsi ad una lettura unitaria. Ed in effetti, a ben guardare ciò che sta accadendo nel momento applicativo, ci si accorge che è il concetto stesso di intermediazione ad essere messo in dubbio nel modello dell'economia di piattaforma.

Sembra potersi affermare, infatti, che le imprese che operano sfruttando tale modello di business non vengano, cioè, più viste - almeno nelle pronunce che si sono passate in rassegna in questa seconda parte dello studio - come meri intermediari neutrali di informazioni, che facilitano le interazioni digitali e le transazioni tra i rispettivi utenti; si va facendo strada, piuttosto, la convinzione che la capacità delle grandi imprese della sfera digitale di raccogliere, analizzare e mettere in relazione tra loro un'enorme mole di dati si risolva in una posizione di notevole vantaggio rispetto ai propri utenti o a danno di essi (*Bolger v. Amazon.com* e *Amazon v. Lee*) o dei terzi che, esercitando professioni regolamentate, subiscono la concorrenza sleale di chi, invocando il carattere innovativo del servizio offerto, tenta di sottrarsi alla relativa regolamentazione (*HomeAway.com v. City of Santa Monica*).

Lo stesso fenomeno - da alcuni definito «*a turn to regulation*[77]», «*a regulatory turn*[78]», o ancora «*a procedural turn*[79]» - che qui si sta registrando con riferimento alla giurisprudenza statunitense si è realizzato, con caratteri forse più espliciti, nel Vecchio Continente.

Per rendersi conto di ciò, basta volgere lo sguardo alla giurisprudenza della Corte di giustizia dell'Unione europea, che sembrerebbe aver intrapreso un processo di "demitizzazione" delle dinamiche sottostanti ai modelli di profitto adottati nell'economia digitale, volto a eliminare dalla narrazione proposta dalle stesse piattaforme quegli aspetti che hanno contribuito a camuffare la reale consistenza delle strategie imprenditoriali adottate.

Il punto è stato ampiamente dimostrato dal giudice europeo con riferimento alla piattaforma *Uber*. In due diverse occasioni la Grande Sezione della Corte di giustizia[80] è stata chiamata a chiarire la natura del servizio prestato dall'intermediario digitale (servizio della società dell'informazione o attività di trasporto[81]).

Dalla qualificazione accolta ne sarebbe discesa o meno la necessità per la piattaforma di munirsi di previe autorizzazioni e licenze amministrative al fine di non violare, nel primo caso, la disciplina sulla concorrenza sleale e, nel secondo, la normativa penale

---

77 M. Santaniello, *La regolazione delle piattaforme e il principio della sovranità a digitale*, in *Rivista di Digital Politics*, 3, 2021, 579 ss.; M. Santaniello, *From Governance Denial to State Regulation. A Controversybased Typology of Internet Governance Models*, in B. Haggart - N. Tusikov - J. A. Scholte (a cura di), *Power and Authority in Internet Governance. Return of the State?*, London, 2021, 15 ss.

78 T. Flew - R. Gillett, *Platform Policy: Evaluating Different Responses to the Challenges of Platform Power*, in *Journal of Digital Media and Policy*, 12, 2021, 231 ss.

79 C. Busch, *The P2B Regulation (EU) 2019/1150: Towards a "Procedural Turn" in EU Platform Regulation?*, in *Journal of European Consumer and Market Law*, 9, 2020,133 ss.

80 Ci si riferisce alle sentenze rese nei casi *Uber Spain* e *Uber France,* cit.

81 La definizione della nozione di «servizio della società dell'informazione», di cui all'art. 2, lett. a), della Direttiva sul commercio elettronico, fa riferimento alla direttiva 98/34/CE, art. 1, c. 1, punto 2, ed ora alla direttiva (UE) 2015/1535, art. 1, c. 1, lett. b), ove si legge che il «servizio della società dell'informazione» comprende «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi».

posta a presidio della sicurezza del servizio di trasporto di persone su strada[82]. Ed invero, il dubbio era se la tesi fatta valere dalla piattaforma - secondo cui quest'ultima collegherebbe unicamente l'offerta di trasporto urbano alla relativa domanda (conformemente alla natura trilaterale dei rapporti che sorgono nell'economia di piattaforma) - fosse una visione troppo riduttiva del ruolo da essa assunto nella transazione e correlativamente dei rispettivi obblighi.

E così, nelle sentenze rese rispettivamente il 20 dicembre 2017 ed il 10 aprile 2018, l'attenzione del giudice europeo, diretta ad identificare colui che effettivamente eroga il servizio all'utente finale (il conducente o la stessa piattaforma), si è incentrata su due diversi elementi: il livello di controllo esercitato dall'impresa digitale sul servizio sottostante e la creazione del relativo mercato[83].

Con riferimento al primo polo dell'indagine, la Corte di giustizia ha ritenuto che fosse *Uber* e non il singolo autista ad erogare il servizio di trasporto argomentando sulla «influenza decisiva» che la piattaforma aveva esercitato sulle modalità concrete di effettuazione del trasporto. In questa logica, l'elemento centrale nell'impianto motivazionale delle sentenze è la capacità dell'attore digitale di controllare l'intera costruzione dello spazio virtuale e di quello fisico soggiacente all'interno del quale si muovono gli altri attori del mercato (gli autisti e i potenziali passeggeri). Rileva, in particolare, il rapporto che essa aveva instaurato con chi eseguiva materialmente il servizio sottostante e segnatamente la possibilità di attuare una strategia di «controllo […] sul comportamento» dei conducenti che potesse «portare, se del caso, alla loro esclusione»[84].

L'altro elemento cruciale nell'argomentare della Corte è la indispensabilità della piattaforma nell'erogazione del servizio di trasporto. *Uber*, infatti, aveva creato il mercato sottostante: essa aveva fornito un'applicazione senza la quale, da un lato, i conducenti non professionisti non sarebbero stati indotti ad effettuare il trasporto e, dall'altro, le persone che avessero inteso spostarsi nell'aerea urbana non avrebbero fatto ricorso ai servizi di tali conducenti.

Il ragionamento seguito dalla Corte - il cui impianto è rimasto immutato nella giurisprudenza successiva[85] - si disvela in tutta la sua chiarezza e si conforma al monito

[82] Com'è noto, l'assoggettamento delle piattaforme telematiche alla regolamentazione sull'intermediazione digitale porta con sé - nel mercato unico europeo - una serie di benefici innegabili: i servizi della società dell'informazione sono, infatti, destinatari di una disciplina speciale di estremo favore rispetto ai servizi dell'economia tradizionale. Ci si riferisce alla direttiva 2000/31/CE e in particolare ad uno degli elementi più innovativi della regolamentazione del commercio elettronico, consistente nel principio, di cui all'art. 4 della direttiva in parola, dell'assenza di autorizzazione preventiva: la regola cioè in base alla quale l'accesso all'attività di prestatore di un servizio della società dell'informazione ed il suo esercizio non sono soggetti, in quanto tali, ad autorizzazione preventiva o ad altra misura di effetto equivalente. Su tale principio, V. Zeno Zencovich, *Note critiche sulla nuova disciplina del commercio elettronico dettata dal d.lgs 70/2003*, in *Il Diritto dell'informazione e dell'informatica*, 19, 2003, 505; C. Rossello, *La nuova disciplina del commercio elettronico. Principi generali e ambito di applicazione*, in *Diritto del commercio internazionale*, 1, 2004, 43.

[83] La Corte è così andata ad articolare un vero e proprio test ("*test Uber*") a cui sottoporre le piattaforme digitali. Sul punto, D. McKee, *The platform economy*, cit., 456.

[84] CGUE, *Uber Spain*, cit., 39; *Uber France*, cit., 21

[85] CGUE, *Airbnb Ireland*, cit. e CGUE, *Star Taxi App SRL v. Unitatea Administrativ Teritorială Municipiul Bucureşti prin Primar General e Consiliul General al Municipiului Bucureşti*, cit.

dell'Avvocato Generale: «non ci si deve […] far ingannare dalle apparenze»[86]. Come dire: al di là dell'illusione creata dalla piattaforma, il rapporto non è affatto trilaterale (connotato tipico, come si è prima riferito, dell'economia di piattaforma), ma bilaterale e conforme al modello di impresa tradizionale. Nulla di nuovo sotto il sole, dunque.

Da queste brevi osservazioni relative alla giurisprudenza europea, si evince come il percorso argomentativo adottato dalla Corte di giustizia non paia coincidere con quello della giurisprudenza d'Oltreoceano esaminata in questo studio: la prima incentrandosi sul livello di controllo esercitato dalla piattaforma sul servizio sottostante e sulla creazione del relativo mercato (al fine di individuare l'elemento principale della prestazione economica[87]); la seconda sul fatto proprio dell'intermediario, che non sia riconducibile alle scelte editoriali relative ai contenuti pubblicati dai propri utenti.

Al di là di queste differenze di approccio, sembra, però, potersi affermare conclusivamente ed in prospettiva comparatistica che traspare una novità comune di non poco momento. Le Corti - su entrambe le sponde dell'Atlantico – sembrano convergere verso il medesimo traguardo: l'urgenza di una svolta regolativa nelle politiche digitali; svolta regolativa che consenta di allocare correttamente il rischio di impresa e le relative responsabilità e che eviti che le piattaforme scarichino impropriamente i costi sugli utenti e ancora che si scongiuri il pericolo che, con l'ingresso dei nuovi attori economici digitali su mercati fortemente regolati, si dia luogo ad "una terra di nessuno, senza regole, né controlli[88]".

[86] Conclusioni dell'Avvocato Generale Maciej Szpunar, presentate l'11 maggio 2017 in C-434/15, *Asociación Profesional Elite Taxi contro Uber Systems Spain SL*, § 52.

[87] Ivi, § 35.

[88] *HomeAway.com v. City of Santa Monica*, cit., 681.

La normativa a tutela dei minori nel Testo Unico per la fornitura di servizi di media audiovisivi con uno sguardo rivolto al regolamento (UE) 2022/2065*

Marco Orofino

Abstract

Lo scritto mira ad indagare le innovazioni introdotte dal d. lgs. 208/2021 recante il Testo Unico sui servizi di media audiovisivi (cd. TUSMA) in materia di tutela dei minori. Nella prima parte sono oggetto di analisi le norme sui poteri di sospensione delle trasmissioni transfrontaliere, sulle trasmissioni pubblicitarie, sui divieti e i vincoli alla trasmissione di contenuti audiovisivi potenzialmente lesivi e, soprattutto, le nuove norme applicabili ai servizi di piattaforma per la condivisione di video. Nella seconda parte, l'analisi ha ad oggetto i temi trasversali della protezione dei dati dei minori e del ruolo dell'AGCOM nel nuovo quadro normativo. In conclusione si prende brevemente in esame l'impatto che il nuovo regolamento europeo sui servizi digitali avrà sul TUSMA.

This paper examines the innovations regarding the protection of minors, introduced by the legislative decree no. 208 of 2021 containing the Audiovisual Media Services Code (so-called TUSMA). In the first part, the writing considers the rules on the powers to suspend cross-border broadcasts, on advertising broadcasts, on the prohibitions and restrictions regarding the broadcasting of potentially harmful audiovisual content and, above all, the new rules applicable to video sharing platform services. In the second part, the analysis concerns the issues of the protection of minors' data and the role of the Italian Communications Authority in the new regulatory framework. In conclusion, it briefly observes the impact that the new European Regulation on digital services will have on TUSMA.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Marco Orofino

Sommario

1. Premessa. - 2. Il potere di sospensione delle trasmissioni frontaliere al fine di tutelare il minore dall'esposizione ai contenuti inappropriati. - 3. La specifica attenzione garantita ai minori nell'ambito delle nuove norme poste "a tutela dei diritti fondamentali". - 4. La realizzazione di iniziative scolastiche e programmi per un uso corretto e consapevole del mezzo televisivo e la riserva di programmazione a favore dei minori. - 5. Le norme a tutela dei minori applicabili ai servizi di piattaforma per la condivisione di video. - 6. Norme a tutela dei minori in ambito pubblicitario. - 7. Il divieto di trattamento dei dati personali a fini commerciali dei dati dei minori raccolti. - 8. Il ruolo dell'AGCOM nel nuovo quadro normativo con specifica attenzione all'attuazione delle norme poste a tutela dei minori. - 9. L'ampliamento delle competenze del Comitato Media-Minori - 10. Osservazioni conclusive.

Keywords

tutela dei minori - fornitori di servizi media audiovisivi - piattaforme per la condivisione video - TUSMA - servizi di media audiovisivi

1. Premessa

Con il d.lgs. 208/2021, l'Italia ha adottato il nuovo Testo Unico dei servizi di media audiovisivi (cd. TUSMA), recependo così nell'ordinamento interno la direttiva (UE) 2018/1808 "recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato"[1].

La direttiva (UE) 2018/1808 prendeva le mosse dalla profonda evoluzione del mercato dei servizi di media audiovisivi determinata dall'attuale convergenza tra la televisione e i servizi internet. Un'evoluzione che richiedeva «un quadro giuridico aggiornato onde riflettere l'evoluzione del mercato e raggiungere un equilibrio tra l'accesso ai servizi di contenuti online, la tutela dei consumatori e la competitività»[2].

L'obiettivo del Legislatore europeo era duplice.

Da un lato, la nuova direttiva mirava all'attenuazione della differenziazione normativa tra servizi media audiovisivi lineari e non lineari ossia tra la televisione tradizionale e la fornitura di contenuti a catalogo. Una differenziazione che era a fondamento del precedente quadro normativo, ma che alla luce delle innovazioni tecnologiche e delle ibridazioni in atto appariva sempre meno giustificata e sempre più foriera di rappresentare un ostacolo al funzionamento del mercato unico.

Da un altro lato, la direttiva puntava alla definizione di regole applicabili ai fornitori

[1] Il recepimento italiano della direttiva (UE) 2018/1808 nel nuovo Testo Unico è giunto, in modo non dissimile da quanto avvenuto in molti altri Stati membri in grande ritardo sia per la pandemia sia, e soprattutto, per il livello degli interessi coinvolti e la rilevanza delle innovazioni messe in atto.

[2] Così considerando 1 della direttiva (UE) 2018/1808.

di piattaforme per la condivisione di contenuti media audiovisivi *online*[3]. Rispetto a questo secondo obiettivo vale la pena, fin da subito, osservare come esso rappresenti un primo tentativo rispetto al pacchetto digitale che l'Unione europea sta portando avanti[4]. Un pacchetto di riforme volte a disciplinare la società digitale che si compone di numerosi atti, sia già approvati sia in via di approvazione che incideranno anche sulle norme che sono qui oggetto di esame. Tra di essi, in particolare occorre segnalare il regolamento (UE) 2022/2065 "relativo a un mercato unico dei servizi digitali (che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)". Tale regolamento (cd. Regolamento DSA) definisce regole, anche in materia di minori, per le piattaforme online[5].

Pertanto tutte le innovazioni, di cui alla direttiva (UE) 2018/1808, riguardanti le piattaforme di condivisione dovranno essere oggetto di verifica in maniera da tale da trovarsi pronti nel momento in cui a far data dal 17 febbraio 2024 il regolamento diverrà integralmente applicabile[6].

In questo contributo si procederà all'esame delle norme riguardanti i minori contenute nel Testo Unico dei servizi di media audiovisivi adottato in recepimento della direttiva (UE) 2018/1808[7]. Si darà quindi conto di come il *favor minoris* di cui l'Unione europea si è fatta, negli ultimi anni fondamentale sostenitrice in tanti settori, si è concretizzato in quello dei media audiovisivi[8].

Nelle conclusioni si darà anche conto se tali norme nazionali possano o meno considerarsi compatibili con il Regolamento DSA, se è lecito attendersi delle disapplicazioni e se siano necessarie integrazioni alle norme interne.

---

[3] Per «servizio di piattaforma per la condivisione di video» la direttiva (UE) 2018/1808 intende un servizio il cui «obiettivo principale […], di una sua sezione distinguibile o di una sua funzionalità essenziale sia la fornitura di programmi, video generati dagli utenti o entrambi per il grande pubblico, per i quali il fornitore della piattaforma per la condivisione di video non ha responsabilità editoriale, al fine di informare, intrattenere o istruire attraverso reti di comunicazioni elettroniche e la cui organizzazione è determinata dal fornitore della piattaforma per la condivisione di video, anche con mezzi automatici o algoritmi, in particolare mediante visualizzazione, attribuzione di tag e sequenziamento».

[4] Cfr. sul "pacchetto digitale" proposto dalla Commissione europea a dicembre 2020 ed in particolare sulla necessità di una maggiore responsabilizzazione degli intermediari digitali per i contenuti prodotti e diffusi dagli utenti finali dei loro servizi, prestando particolare attenzione alle piattaforme di grandi dimensioni, M.R. Allegri, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Rivista italiana di Informatica e di Diritto*, 2, 2021, 7 ss.

[5] Per piattaforme *online* il regolamento (UE) 2022/2065 intende, con formula piuttosto ampia, un servizio di memorizzazione di informazioni che, su richiesta di un destinatario del servizio, memorizza e diffonde informazioni al pubblico.

[6] Solo l'art. 24, par. 2, 3 e 6, l'art. 33, par. da 3 a 6, l'art. 37, par. 7, l'art. 40, par. 13, l'art. 43 e il capo IV, sez. 4, 5 e 6, sono già in vigore a far data dal 16 novembre 2022.

[7] Cfr. sulle innovazioni introdotte dalla direttiva in materia di tutela dei minori, F. Donati, *La tutela dei minori nella direttiva 2018/1808*, in questa *Rivista*, 1, 2019, 59 ss. Sulla compatibilità delle nuove norme europee rispetto al *favor costitutionis* per il minore nell'ordinamento italiano G. De Minico, *Il Favor Minoris: Un orizzonte Lontano*, in *Astridonline*, 4, 2019.

[8] Una ricostruzione assai accurata è quella di G. Pesci, *Prospettive e recenti sviluppi della tutela dei minori online*, in *Ciberspazio e diritto: Rivista internazionale di informatica giuridica*, 2022, 311. Con specifico riferimento al settore della protezione dati il GDPR contiene norme importantissime a tutela dei minori. Sia consentito sul punto il rinvio a M. Orofino, *Minori e diritto alla protezione dei dati personali*, in M. Orofino – F.G. Pizzetti, *Privacy, minori e cyberbullismo*, Torino, 2018, 1 ss.

2. Il potere di sospensione delle trasmissioni frontaliere al fine di tutelare il minore dall'esposizione ai contenuti inappropriati

Il primo punto in cui i minori sono espressamente presi in considerazione dal nuovo T.U. è nell'art. 7, rubricato "Trasmissioni transfrontaliere". La norma è posta tra i Principi del nuovo Testo Unico.

Il primo comma afferma, infatti, il principio della libertà di ricezione di servizi di media audiovisivi provenienti da altri Stati membri dell'Unione europea e, specifica che non è ostacolata la loro ritrasmissione sul territorio nazionale italiano.

Il principio generale è temperato dall'espressione «salvo i casi previsti» che apre a possibili interdizioni. I casi che possono giustificare la deroga al principio generale sono elencati nel comma 2 dell'art. 7.

Tra di essi al primo punto, lett. a), del c. 2, è espressamente citata la circostanza di violazione manifesta, seria e grave del divieto di trasmettere programmi che possano «nuocere gravemente allo sviluppo fisico, mentale o morale dei "minori di diciotto anni"». La norma prosegue con la specificazione, da intendersi come non esaustiva, di programmi che contengano scene pornografiche o di violenza gratuita e con l'ulteriore precisazione che il divieto scatta a meno che la scelta dell'ora di trasmissione o qualsiasi altro accorgimento tecnico escludano che i minori che si trovano nell'area di diffusione assistano normalmente a tali programmi.

La norma presenta un certo grado di indeterminatezza. Il compito di dare attuazione alle previsioni è rimesso all'AGCOM. A tal fine l'Autorità stipula protocolli d'intesa con il Ministero della Salute, il Ministero della Difesa, il Ministero dell'Interno e il Ministero della Giustizia.

La medesima Autorità è, inoltre, incaricata di disporre la sospensione provvisoria della trasmissione o della ritrasmissione dei servizi di media audiovisivi erogati da un fornitore sottoposto alla giurisdizione di un altro Stato membro in tutti i casi elencati nel c. 2[9].

In ogni caso, la sospensione disposta dall'AGCOM è da intendersi come *extrema ratio*, comunque, subordinata al verificarsi di una serie di condizioni elencate al c. 3 dell'art. 7 del T.U.

La prima è che il fornitore abbia nei dodici mesi precedenti già tenuto, in almeno due occasioni, il comportamento ritenuto illegittimo. La seconda è che l'Autorità abbia notificato, per iscritto, le presunte violazioni e le misure che intende adottare. La terza è che il fornitore ricevuta contestazione abbia avuto la possibilità di rappresentare nell'ambito di un contradditorio le proprie osservazioni rispetto alle singole violazioni

[9] Gli altri casi che possono condurre a tale interruzione sono: a) la violazione manifesta, seria e grave del divieto di trasmissione di programmi che contengono incitamento alla violenza o all'odio nei confronti di un gruppo di persone o di un membro di un gruppo, per motivi di razza, sesso, religione o nazionalità; b) l'erogazione di servizi di media audiovisivi tali da rappresentare un rischio serio e grave di pregiudizio per la salute pubblica; c) la violazione manifesta seria e grave del divieto di pubblica provocazione a commettere i reati di terrorismo di cui all'art. 5 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017; d) il pregiudizio o rischio grave e serio di pregiudizio per la pubblica sicurezza, ivi compresa la salvaguardia della difesa e della sicurezza nazionali.

notificate dall'Autorità. La quarta è che si siano svolte, senza successo ossia senza il raggiungimento di una "soluzione amichevole" le consultazioni con lo Stato membro che ha la giurisdizione sul fornitore di servizi oggetto di contestazione e con la Commissione.
Questa previsione, al di là dell'utilizzo assai improprio dell'espressione soluzione amichevole utilizzata nel T.U., è assai interessante perché rinvia ad un meccanismo di soluzione di eventuali controversie che è disciplinato a livello europeo dall'art. 3 della direttiva (UE) 2018/1808 con lo scopo di superare i conflitti di giurisdizione tra gli Stati in un settore, quello della trasmissione radiotelevisiva, in cui come noto la frequenza e la relativa capacità trasmissiva non rispondono alle logiche dei confini nazionali quanto piuttosto alle regole della fisica.
Un meccanismo in cui l'ultima parola spetta alla Commissione europea sulla base del parere fornito dall'ERGA (*European Regulators Group for Audiovisual Media Services*, organismo in cui sono rappresentati i regolatori dei 27 Stati membri) anche alla luce del c. 5 dell'art. 7 che prevede che l'Autorità nazionale si conformi alle decisioni con le quali la Commissione europea accerti l'incompatibilità della sospensione rispetto al diritto dell'Unione.
Al potere ordinario di sospensione, il Testo Unico affianca un potere straordinario al quale l'Autorità può ricorrere in casi urgenti. Fermo restando che la norma non definisce la nozione di caso urgente, rinviando dunque anche per questo all'attuazione dell'AGCOM, la differenza rispetto al procedimento ordinario sta nella possibilità di derogare al presupposto della ripetitività delle violazioni e alla notifica previa. Rimane però fermo, l'obbligo di garantire un contradditorio e di svolgere quanto prima le consultazioni con lo Stato membro e con la Commissione. Del pari, la Commissione può sempre chiedere all'esito della sua analisi il ritiro della misura adottata.

3. La specifica attenzione garantita ai minori nell'ambito delle nuove norme poste "a tutela dei diritti fondamentali"

Nel Titolo IV del TUSMA recante la disciplina aggiornata dei servizi di media audiovisivi e radiofonici, il Capo I è significativamente intitolato "Disposizioni applicabili a tutti i servizi di media audiovisivi e radiofonici – Norme a tutela dei diritti fondamentali della persona e dei minori".
La prima parte della rubrica segnala il tentativo di offrire una disciplina comune dei servizi di media audiovisivi e radiofonici superando, quindi, per quanto possibile la dicotomia tra servizi lineari e servizi a catalogo. La seconda parte della rubrica dà conto della particolare attenzione che le nuove norme pongono nei confronti dei minori, destinatari di norme specifiche a loro tutela, unitamente a quelle dettate per tutelare i diritti fondamentali di tutte le persone (minori ovviamente inclusi). Il tutto secondo una progressione per cui il minore, in quanto soggetto vulnerabile, riceva una tutela rafforzata[10].

[10] Sui soggetti vulnerabili P. Scarlatti, *I diritti delle persone vulnerabili*, Napoli, 2022.

Nell'ambito di questo Capo, merita particolare attenzione l'art. 37.
Tale articolo è specificamente dedicato alla tutela dei minori nella programmazione audiovisiva.
Il primo comma si apre con alcuni specifici divieti.
Il primo divieto riguarda la trasmissione di programmi televisivi gravemente nocivi per lo «sviluppo fisico, psichico o morale dei minori» ed in particolare tra di essi quelli «che presentano scene di violenza gratuita o insistita o efferata ovvero scene pornografiche». Il secondo divieto, più specifico, riguarda la trasmissione di film «la cui proiezione o rappresentazione in pubblico ai minori di anni diciotto sia stata vietata dalle Autorità a ciò competenti».
I divieti in questione sono da intendersi come assoluti per i servizi lineari.
Per i servizi a richiesta, invece, tali programmazioni sono trasmissibili solo se soddisfatti i criteri forniti al c. 3 ossia nel caso in cui il fornitore adotti un sistema capace di escludere che i minori vedano o ascoltino normalmente tali programmi come, ad esempio, attraverso un meccanismo di controllo specifico e selettivo che vincoli la visione nonché attraverso apposita segnaletica.
Il secondo comma dell'art. 37 introduce limiti in relazione alle fasce orarie di programmazione. Fermi restando i divieti del comma precedente, la norma qui prevede che i programmi che possano nuocere «allo sviluppo fisico, psichico o morale dei minori o film vietati ai minori di anni quattordici» debbano essere preferibilmente trasmessi, fra le ore 23 e le ore 7. Laddove la programmazione avvenga in orari diversi, essa è lecita solo se siano previsti accorgimenti che rendano difficile vedere o ascoltare normalmente tali programmi da parte dei minori.
Il compito di dare attuazione a quanto previsto sia nel primo che nel secondo comma è affidato all'AGCOM che è chiamata a definire, attraverso procedure di co-regolazione, sia i criteri per individuare i programmi vietati sia eventuali altri accorgimenti utili per escludere la visione da parte di minori[11].
In questo l'AGCOM procede d'intesa con il Ministero dello Sviluppo Economico, sentiti l'Autorità garante per l'infanzia e l'adolescenza e il Comitato di applicazione del Codice di autoregolamentazione media e minori. La norma provvede, in modo non esaustivo né tassativo, a fare menzione del possibile uso di numeri di identificazione personale, di sistemi di filtraggio, di verifica dell'età o di identificazione.
La scelta rimessa alla co-regolazione è quindi piuttosto ampia e trova due soli limitazioni generali ai sensi delle lett. a) e b). La prima sta nel fatto che il contenuto classificabile «a visione non libera» deve essere offerto con una funzione di controllo parentale che sia in grado di inibire l'accesso in mancanza dello specifico codice segreto che ne rende la visione possibile. La seconda limitazione è che il codice segreto deve essere comunicato con modalità riservate, corredato dalle avvertenze in merito alla responsabilità nell'utilizzo e alla custodia, al contraente maggiorenne che stipula il contratto relativo alla fornitura del contenuto o del servizio.

[11] I fornitori di servizi di media audiovisivi e radiofonici e le emittenti radiofoniche si conformano ai menzionati criteri e alla disciplina di dettaglio entro trenta giorni dalla data di entrata in vigore dei regolamenti emessi dall'Autorità, garantendo il rispetto delle condizioni direttamente poste dal presente articolo, assicurando al contempo che i contenuti classificati ai sensi del c. 1 siano ricevibili e fruibili unicamente nel rispetto delle condizioni fissate ai sensi del c. 5.

In ogni caso, le trasmissioni sia radiofoniche sia radiotelevisive, tanto in chiaro che a pagamento, devono essere rispettivamente precedute da un'avvertenza acustica e identificate, per l'intera durata della trasmissione, da un simbolo visivo chiaramente percepibile e riconoscibile dall'utente[12].
Anche in questo caso è previsto l'intervento dell'AGCOM che, ricorrendo a procedure di co-regolamentazione, è chiamata ad individuare misure tecniche diverse e aggiuntive.

4. La realizzazione di iniziative scolastiche e programmi per un uso corretto e consapevole del mezzo televisivo e la riserva di programmazione a favore dei minori

I c. 10 ed 11 dell'art. 37 contengono due previsioni di grande importanza per i minori.
Il c. 10 prevede che il Ministro dello Sviluppo Economico, d'intesa con il Ministro dell'istruzione, con l'Autorità garante per l'infanzia e l'adolescenza e con il Presidente del Consiglio dei ministri[13], disponga la realizzazione di iniziative scolastiche per un uso corretto e consapevole del mezzo televisivo, nonché di programmi con le stesse finalità rivolti ai genitori, utilizzando a tale fine anche gli stessi mezzi radiotelevisivi, in orari caratterizzati da ascolti medi elevati e soprattutto nella fascia oraria compresa tra le ore 19 e le ore 23, e in particolare i mezzi della società concessionaria del pubblico servizio radiofonico, televisivo e multimediale.
Il tema dell'educazione dei minori all'uso corretto e consapevole del mezzo televisivo è oggi essenziale (quanto e più di ieri) alla luce della grande diffusione di fornitori di contenuti a catalogo così come è essenziale fornire alle famiglie le informazioni necessarie per implementare i blocchi o i sistemi di *parental control* che la tecnologia rende disponibili.
Con riferimento alla seconda previsione, il c. 11 specifica che le quote di riserva per la trasmissione di opere europee previste nella normativa europea e recepite nel Testo Unico all'art. 52 dovranno necessariamente annoverare anche opere cinematografiche o per la televisione, comprese quelle di animazione, specificamente rivolte ai minori, produzioni e programmi adatti ai minori ovvero idonei alla visione da parte dei minori oltre che degli adulti[14].
Il tempo minimo di trasmissione di tale programmazione, nell'ambito della quota complessiva, è ancora una volta rimessa alla determinazione dall'Autorità con proprio regolamento.
Per la concessionaria del servizio pubblico, l'art. 54, c. 8, prevede un'ulteriore sotto quota non inferiore al 7% della quota prevista per le opere europee, di cui almeno il

[12] A norma del c. 4 dell'art. 37 le limitazioni di cui sopra si applicano anche alle anteprime di opere cinematografiche destinate alla proiezione o distribuzione in pubblico nella misura in cui le limitazioni ed i vincoli si applicano alla trasmissione dell'opera cinematografica di cui costituiscono promozione.

[13] Nel caso in cui il Presidente del Consiglio abbia delegato ad un Ministro o ad un sottosegretario le relative competenze l'intesa di cui al c. 10 dell'art. 37 del TUSMA è da ricercarsi con l'autorità delegata.

[14] Art. 54 del TUSMA recante "Disposizioni applicative in materia di opere audiovisive di espressione originale italiana".

65% deve essere riservato ad opere di animazione.

5. Le norme a tutela dei minori applicabili ai servizi di piattaforma per la condivisione di video

Il Capo II, rubricato "Disposizioni applicabili ai servizi di piattaforma per la condivisione di video" è dedicato alla regolazione delle cd. piattaforme per la condivisione di video. Gli artt. 41 e 42 del TUSMA introducono specifici poteri di regolazione e di monitoraggio nei loro confronti e rappresentano il recepimento nazionale di uno degli aspetti più peculiari della normativa europee. Occorre segnalare come le norme qui in commento si trovino oggi nella difficile situazione di doversi legare sia con la direttiva 2000/31/CE, recepita in Italia con il d.lgs. 70/2003, sia con il regolamento (UE) 2022/2065 che, come detto, è già in vigore ma si applicherà, nella sua interezza, a decorrere dal 17 febbraio 2024[15].

Si trovano, cioè, in mezzo tra un regime della responsabilità dei fornitori ormai corroso dal passare del tempo ed uno nuovo ancora tutto da valutare alla prova dei fatti[16].

Allo stato dell'arte, l'art. 41 detta le "Disposizioni generali" ossia definisce l'ambito di applicazione materiale della legislazione italiana riprendendo le nozioni "europee" di stabilimento, impresa controllata ed i principi di libera circolazione infra europea, qui operando un rinvio proprio all'art. 5, c. 2, 3 e 4 del d.lgs. 70/2003 per la procedura di limitazione della libera circolazione di programmi, video generati dagli utenti e comunicazioni commerciali audiovisive veicolati da una piattaforma per la condivisione di video.

Con riferimento alle ipotesi che legittimano la limitazione, il TUSMA prevede, *ex* lett. a) del c. 7 dell'art. 41, specularmente a quanto sancito per le trasmissioni televisive, «la tutela dei minori da contenuti che possono nuocere al loro sviluppo fisico, psichico o morale».

L'art. 42 definisce le "Misure di tutela" ribadendo ai sensi del primo comma, che i fornitori di piattaforme per la condivisione di video devono adottare misure adeguate per tutelare i minori da programmi, video generati dagli utenti e comunicazioni commerciali che possano nuocere al loro sviluppo fisico mentale o morale.

Per quanto riguarda i video maggiormente nocivi, da intendersi in analogia con l'art. 37 T.U., quelli «che presentano scene di violenza gratuita o insistita o efferata ovvero scene pornografiche», i fornitori di servizi sono chiamati ad adottare le più rigorose tecniche di controllo dell'accesso[17].

La norma rinvia in proposito all'art. 38, c. 3 del T.U. che prevede, in caso di violazione, la sanzione della disattivazione dell'impianto di trasmissione. Nel caso di specie occor-

[15] Sul DSA, O. Pollicino – G. De Gregorio, *L'alba di nuove responsabilità sulle piattaforme digitali: il Digital Services Act*, in *Agenda Digitale*, 15 dicembre 2020; O. Pollicino – G. De Gregorio – M. Bassini., *Verso il Digital Services Act: problemi e prospettive. Presentazione del simposio*, in *medialaws.eu*, 23 novembre 2020.

[16] Sull'incapacità del vecchio regime della responsabilità di ordinare un mercato ormai esploso v. anche l'analisi di M. Bassini, *La Cassazione e il simulacro del provider attivo: mala tempora currunt*, in questa *Rivista*, 2, 2019, 248 ss.

[17] Così l'art. 42, c. 6, del TUSMA.

re dire che il rinvio non è chiaro perché il concetto di disattivazione non è trasferibile automaticamente sul web. Per cui la norma può essere letta come possibilità di oscuramento del contenuto o come possibilità di rendere inaccessibile la piattaforma. La seconda ipotesi deve, però, ritenersi poco praticabile per via del doveroso rispetto del principio di proporzionalità della sanzione rispetto all'illecito.

Il secondo comma dell'art. 42 pone il principio generale della necessaria conformazione, per i fornitori di piattaforme, alle disposizioni generali relative alle comunicazioni commerciali audiovisive sia quelle promosse commercialmente, vendute o organizzate sia quelle non promosse, vendute o organizzate dagli stessi assumendo su di esse il dovere di informare gli utenti nel caso in cui i programmi e i video generati contengano tali comunicazioni.

Il terzo comma dell'art. 42 estende il modello della co-regolazione e dell'autoregolazione ai fornitori di piattaforme per la condivisione, prevedendo a tal fine il necessario coinvolgimento del Comitato media-minori e dell'AGCOM. Quest'ultima in particolare deve, ricevutane comunicazione, verificare la conformità delle proposte alla legge ed ai propri regolamenti e, nel caso in cui la verifica dia esito positivo, adottarle con propria delibera. La delibera dell'AGCOM conferisce al Codice efficacia ed è la base legale del successivo controllo sulla loro attuazione che l'AGCOM è chiamata a svolgere.

I Codici adottati devono individuare misure finalizzate a ridurre l'esposizione dei minori di anni dodici alle comunicazioni commerciali relative a prodotti alimentari (incluse bevande) che contengano sostanze (zuccheri, sale, sodio, acidi grassi, grassi) la cui assunzione eccessiva rispetto alla quantità raccomandata non è raccomandata nell'ambito di una corretta dieta[18].

L'attività di autoregolazione, sanzionata a valle dall'approvazione tramite delibera dell'AGCOM, è destinata ad incontrare un limite anche a monte nelle Linee Guida che l'Autorità stessa può adottare, sempre in stretta cooperazione con il Comitato media minori e con il Garante per l'infanzia e per l'adolescenza.

Tali Linee guida, a norma del c. 5 dell'art. 42, devono indicare i criteri specifici informatori dei codici di condotta alla luce della natura e del contenuto del servizio offerto, prendendo in specifica considerazione le categorie da tutelare, tra cui evidentemente vi sono i minori[19].

Per quanto, infine, riguarda gli obblighi che i fornitori di piattaforme per la condivisione sono tenuti a rispettare, è di particolare interesse il c. 7 dell'art. 42 che definisce un vero e proprio decalogo in cui la tutela dei minori è assolutamente centrale.

Il primo obbligo consiste nella necessaria specificazione dei contenuti che non debbono essere condivisi – perché ritenuti idonei a nuocere allo sviluppo fisico, mentale o morale dei minori – nelle condizioni del servizio della piattaforma. L'accettazione da parte degli utenti deve costituire una condizione di accesso al servizio.

[18] In ogni caso i Codici devono garantire che le comunicazioni commerciali non accentuino la qualità positiva degli aspetti nutrizionali di tali prodotti e bevande.

[19] Con la delibera n. 16/22/CONS del 4 febbraio, l'Autorità per le garanzie nelle comunicazioni (AGCOM) ha indetto una consultazione pubblica finalizzata all'adozione di Linee guida per l'attuazione dell'art. 7-*bis* del d.l. 28/2020 dedicato ai «sistemi di protezione dei minori dai rischi del cyberspazio».

Il secondo obbligo riguarda l'inclusione, nei termini e nelle condizioni dei servizi di piattaforme per la condivisione di video, dei requisiti per le comunicazioni commerciali audiovisive non promosse commercialmente, vendute o organizzate dai fornitori di piattaforme per la condivisione di video.
Il terzo obbligo consiste nell'implementazione di funzionalità che consentano agli utenti che caricano video generati dagli utenti di dichiarare se tali video contengono comunicazioni commerciali audiovisive di cui sono a conoscenza anche presumibilmente.
Il quarto obbligo è la predisposizione di meccanismi trasparenti e facilmente utilizzabili per consentire agli utenti di segnalare o indicare al fornitore di piattaforme interessato, i contenuti che non dovrebbero essere caricati sulla piattaforma.
Il quinto obbligo riguarda l'implementazione di sistemi mediante i quali i fornitori di piattaforme per la condivisione di video possono spiegare agli utenti di tali piattaforme quale sia il seguito che le loro segnalazioni ricevono.
Il sesto obbligo consiste nell'utilizzo di sistemi per verificare, nel rispetto della normativa in materia di protezione dei dati personali, l'età degli utenti delle piattaforme di condivisione di video per quanto attiene ai contenuti che possono nuocere allo sviluppo fisico, mentale o morale dei minori.
Il settimo obbligo è la predisposizione di sistemi di facile uso che consentano agli utenti delle piattaforme per la condivisone di video di valutare i contenuti in esse presenti
L'ottavo obbligo è la previsione di sistemi di controllo parentale sotto la vigilanza dell'utente finale per quanto attiene ai contenuti che possano nuocere allo sviluppo fisico, mentale o morale dei minori.
Il nono, e penultimo obbligo, è la predisposizione di procedure trasparenti, di facile uso ed efficaci per la gestione e la risoluzione dei reclami degli utenti nei confronti dei fornitori di piattaforme per la condivisione di video
Il decimo obbligo è l'adozione di misure e strumenti efficaci di alfabetizzazione mediatica al fine di sensibilizzare gli utenti in merito a tali misure e strumenti. Questi strumenti devono necessariamente prendere in specifica considerazione i minori e le loro famiglie e rappresentano attuazione di quel necessario progetto di educazione digitale di cui l'UE è promotrice.

6. Norme a tutela dei minori in ambito pubblicitario

Forse meno innovative, giacché si muovono su un terreno nel quale l'intervento europeo è più consolidato, ma non per questo meno importanti per la ricostruzione del quadro complessivo, sono le norme, contenute nel Capo III del Testo Unico, e poste a tutela dei minori in materia di pubblicità, sponsorizzazione e inserimento di prodotti.
I minori sono espressamente presi in considerazione nell'art. 43 recante "Principi generali in materia di comunicazione commerciali audiovisive e radiofoniche" e nell'art. 47 rubricato "Disposizioni sulle televendite".
Per quanto riguarda l'art. 43, la norma prevede una serie di obblighi che riguardano i

fornitori di servizi di media soggetti alla giurisdizione italiana. Tra di essi, la lett. e) vieta le comunicazioni commerciali audiovisive per le bevande alcoliche che si rivolgono specificamente ai minori o né incoraggiano un uso smodato e la lett. g) che vieta, più in generale, le comunicazioni commerciali che possano arrecare un pregiudizio fisico o morale ai minori. Più nel dettaglio, le comunicazioni commerciali non possono esortare i minori all'acquisto di un prodotto o di un servizio sfruttando la loro inesperienza, non possono incoraggiarli a persuadere i loro genitori all'acquisto di prodotti, non devono sfruttare la fiducia che i minori ripongono nei genitori o negli insegnanti ovvero in altre persone, e, infine, non possono mostrare minori che si trovano in situazioni pericolose.
Nonostante il tentativo di specificare alcuni divieti la formulazione della lett. g) permane assai ampia. Il compito di individuare cosa debba ritenersi «poter arrecare un pregiudizio fisico o morale ai minori» è affidato ancora una volta alla co-regolamentazione e all'auto-regolamentazione.
In questo senso il riferimento è al c. 4 dell'art. 43 che è dedicato ai codici di condotta che i fornitori di servizi di media possono adottare d'intesa con l'AGCOM e sentiti i Ministeri dello Sviluppo economico e, in questo caso, anche della Salute.
La norma in questione pone particolare attenzione ai prodotti alimentari con l'obiettivo di promuovere una dieta sana e varia per le più giovani generazioni. Per questa ragione rimette ai codici di condotta anche il compito di prevedere come limitare l'esposizione dei minori a contenuti pubblicitari che riguardano prodotti ricchi di grasso, sale e zuccheri.
Per quanto riguarda l'art. 47, ossia le televendite, il c. 2 specifica che esse non debbano né esortare i minori a stipulare contratti di compravendita o di locazione di prodotti e di servizi né arrecare loro un pregiudizio morale o fisico.
Inoltre, a loro ulteriore tutela, la norma prevede che la televendita non debba: a) esortare direttamente i minori ad acquistare un prodotto o un servizio, sfruttandone l'inesperienza o la credulità; b) esortare direttamente i minori a persuadere genitori o altri ad acquistare tali prodotti o servizi; c) sfruttare la particolare fiducia che i minori ripongono nei genitori, negli insegnanti o in altri; d) mostrare, senza motivo, minori in situazioni pericolose.

7. Il divieto di trattamento dei dati personali a fini commerciali dei dati dei minori raccolti nell'esercizio delle misure e degli strumenti previsti a loro tutela

Due norme che meritano specifica attenzione, rispettivamente poste nell'ambito delle misure dettate a protezione dei diritti fondamentali e dei minori e delle misure destinate ai fornitori di piattaforme di condivisione, sono quelle che vietano il trattamento dei dati personali relativi a minori raccolti in applicazione delle misure tecniche previste per limitare l'accesso a contenuti non idonei alla loro visione. Si tratta specificamente dell'art. 37, c. 9, e dell'art. 42, c. 7, lett. e).
Le norme in questione intervengono ad integrare quanto disposto dal regolamento

(UE) 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, comunemente noto con l'acronimo GDPR.
Il punto è interessante perché il GDPR detta una pluralità di norme immediatamente applicabili al trattamento di dati personali di minori, ma non contiene uno specifico divieto, come nel caso qui oggetto di analisi. In generale, infatti, il GDPR preferisce responsabilizzare i titolari piuttosto che imporre divieti, anche in conseguenza del fatto che esso persegue contemporaneamente l'obiettivo della protezione dei diritti e del favorire la circolazione dei dati[20].
Questa valorizzazione passa anche attraverso la previsione del consenso dei minori per il trattamento dei loro dati nell'ambito della fornitura di servizi della società dell'informazione[21]. Questo perché così facendo impone ai titolari un *surplus* di attenzione nell'esercizio dei compiti loro propri.
Tornando però al caso qui in esame, occorre sottolineare come non si tratta di un divieto generale per i fornitori di servizi media audiovisivi e di piattaforme per la condivisione di contenuti.
Questo per due ragioni. In primo luogo perché riguarda solo il trattamento di quei dati necessari per le attività che i fornitori devono svolgere a tutela dei minori stessi. In secondo luogo perché il divieto di trattamento riguarda solo tre specifiche finalità: commerciali, di profilazione e di pubblicità mirata.
In ogni caso, al fine di superare qualsiasi dubbio sulla compatibilità della norma interna rispetto al quadro normativo europeo in materia di protezione dei dati personali, occorre precisare che la previsione del Testo Unico è diretto recepimento (la formulazione è identica) di un obbligo che la direttiva europea poneva in capo agli Stati membri.

8. Il ruolo dell'AGCOM nel nuovo quadro normativo con specifica attenzione all'attuazione delle norme poste a tutela dei minori

Come emerge in modo assai evidente dalla mera descrizione delle norme che mirano a tutelare i minori, il TUSMA affida all'AGCOM un ruolo di primo piano nella regolazione, certamente accresciuto rispetto al precedente quadro normativo. Più chiaramente, occorre dire, che l'apparato di attuazione della normativa in esame è quasi integralmente rimesso a regolamenti dell'AGCOM[22].

[20] Su questo punto le osservazioni di F. Pizzetti (a cura di) *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 12, che fin da subito ha evidenziato come una lettura del GDPR solo come normativa a presidio delle libertà e dei diritti delle persone fosse non solo insufficiente, ma pure sbagliata perché dimenticava l'obiettivo strategico della circolazione dei dati per la costruzione della società digitale.

[21] Sul tema del consenso del minore, in termini assai critici, M. Bianca, *La tutela del minore nell'età digitale. Riflessioni a margine della lettura del libro bianco AGCOM 2.0. su media e minori*, in *Comunicazione.doc.,* 2018, 59 ss.

[22] Su questo specifico tema il parere del Consiglio di Stato, sez. Consultiva per gli Atti Normativi,

Molto si è detto negli anni sulla questione se l'Autorità indipendente potesse o meno intervenire con proprie regole in materia di diritti fondamentali, in particolar modo laddove fosse possibile scorgere nella Costituzione italiana una riserva di legge assoluta. La questione fu oggetto di un confronto acceso in dottrina allorché l'AGCOM, ai sensi del d.lgs. 70/2003, adottò il regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative che prevedeva una procedura di *notice and take down* all'esito della quale l'Autorità poteva disporre la cancellazione del contenuto[23]

Nel caso qui in esame la questione è però diversa.

Innanzitutto, l'intervento dell'Autorità di regolazione è previsto dalla normativa europea. Senza voler aprire il vaso di pandora della prevalenza del diritto europeo sul diritto nazionale (anche costituzionale) e dei contro-limiti a questa prevalenza, occorre dire che la legittimazione europea è assai importante. Ciò soprattutto perché avviene in un settore che per sua natura è parte integrante di quella società digitale di cui l'Unione europea sta progressivamente scrivendo le regole anche attraverso un lavorio giurisprudenziale che conduce una continua reinterpretazione in senso evolutivo della Carta dei diritti fondamentali e delle tradizioni costituzionali comuni.

In secondo luogo, nel disegno europeo, il coinvolgimento delle Autorità di regolazione si inserisce in una strategia normativa che mira alla valorizzazione dell'auto-regolazione e della co-regolazione non tanto nel senso che si lascia meramente ai privati il compito di darsi le proprie regole quanto piuttosto secondo una strategia in cui i fornitori di servizi media audiovisivi e i fornitori di piattaforme per la condivisione di video sono chiamati a compartecipare nella definizione di regole perché sono loro ad essere responsabili (e passibili di sanzione) nel caso in cui non garantiscano ai minori una tutela adeguata[24].

Un modello che l'Unione europea ha già sperimentato con buon successo nel settore della protezione dei dati e che sembra riproporre, almeno in parte, anche nella normativa sui servizi media audiovisivi e nel recentemente approvato Regolamento DSA. Per cui, può dirsi che l'AGCOM nelle norme del T.U. che si sono analizzate non ha solo un ruolo di garanzia per i minori, nel senso che compartecipando con i fornitori di servizi media audiovisivi alla scrittura delle regole attuative degli obblighi di legge li guida verso un sistema di massima tutela, ma pure un ruolo di garanzia per i fornitori stessi perché offre loro una sponda laddove altrimenti essi sarebbero chiamati a farsi carico dell'attuazione, rischiando di esserne responsabili nel caso in cui non raggiun-

Adunanza di Sezione del 21 settembre 2021.

[23] Delibera n. 680/13/CONS. Su di essa sia consentito rinviare a M. Orofino*, L'intervento regolamentare dell'AGCOM in materia di diritto d'autore: profili di criticità formale e sostanziale*, in F. Pizzetti (a cura di), *Il caso del diritto d'autore*, Torino, 2013, 123 ss. La vicenda è stata oggetto di un ampio contenzioso giurisprudenziale giungendo tanto davanti alla Corte costituzionale quanto al Consiglio di Stato. La questione è, infine, stata sanata con l'irrobustimento della normativa che attribuisce all'AGCOM il potere regolamentare e sanzionatorio con riferimento al diritto d'autore online. l'accurata ricostruzione di S. Lavagnini, *Riforma del diritto d'autore e nuovi poteri di Agcom: cosa cambia e prossimi step*, in *Agendadigitale.eu*, 26 gennaio 2022.

[24] Queste forme di auto regolazione "controllata" e di co regolazione sono anche la risposta europea al problema della diffusione di poteri privati incidenti sui diritti fondamentali. Su questa questione F. Paruzzo*, I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Torino, 2022.

gessero gli obiettivi previsti dal Testo Unico e dalla direttiva.

9. L'ampliamento delle competenze del Comitato Media-Minori

Un ruolo piuttosto rilevante nella *governance* complessiva del sistema lo ha il cd. Comitato media e minori. Tale organo ha una storia ormai lunga alle spalle. Istituito, infatti, originariamente come organo di autodisciplina tra le imprese radiotelevisive, fu istituzionalizzato dalla legge n. 112 del 2004[25].

La sua positivizzazione già rispondeva ad un approccio, che all'epoca era assai innovativo, volto ad integrare nel dato normativo il principio dell'autoregolazione[26]. Dalla l. 112/2004 il Comitato era poi trasmigrato con il d.lgs. 177/2005 nel Testo Unico della radiotelevisione, poi divenuto Testo Unico dei servizi di media audiovisivi e radiofonici.

L'art. 8 del nuovo T.U., rubricato "Funzioni del Ministero dello Sviluppo Economico", specifica al c. 2 che presso il suddetto ministero opera il Comitato di applicazione del Codice di autoregolamentazione media e minori[27].

Il nome odierno del Comitato riflette l'estensione progressiva delle sue competenze. Dall'originario Comitato di applicazione del codice di autoregolamentazione TV e minori si è passati al Comitato di applicazione del Codice di autoregolamentazione media e minori[28], mantenuto anche nell'attuale Testo Unico con la specificazione che esso opera nei settori dei servizi media audiovisivi e della radiofonia.

Una specificazione da leggersi oggi ai sensi delle definizioni contenute nell'art. 3 che al c. 1, lett. a), chiarisce come per servizio di media audiovisivo debba intendersi «un servizio […] che abbia come obiettivo principale del servizio stesso o di una sua sezione distinguibile, la fornitura di programmi al grande pubblico, sotto la responsabilità editoriale di un fornitore di servizi di media, al fine di informare, intrattenere o istruire […]» ossia, come ulteriormente specificato alla lett. b) una trasmissione televisiva attraverso un servizio media audiovisivo lineare oppure un servizio di media audiovisivo a richiesta sulla base di un catalogo oppure una comunicazione commerciale audiovisiva.

Per cui il Comitato acquisisce oggi competenze piene rispetto a tutti i servizi media audiovisivi.

Di conseguenza, in un contesto in cui auto-regolamentazione e co-regolamentazione divengono capisaldi del nuovo impianto normativo è lecito attendersi che si giunga

[25] Il Comitato media minori è "inglobato" dalla l. 112/2004 secondo la felice espressione utilizzata da M. Cuniberti, *La legge n. 112 del 2004: aspetti generali*, in *La riforma del sistema radiotelevisivo*, aggiornamento ad Aa.Vv., *Percorsi di diritto dell'informazione*, Torino, 2014, 17.

[26] Così, assai acutamente, mette in luce L. Musselli, *Televisione e minori: tutela pubblicistica*, Milano, 2009, 85.

[27] Il nuovo Testo Unico, qui oggetto di analisi, conferma la collocazione ministeriale del Comitato presso il Ministero dello Sviluppo Economico, che a far data dal 30 ottobre 2010, aveva assunto le competenze del Ministero delle Comunicazioni.

[28] Ciò è avvenuto ai sensi dell'art. 6, c. 1, d.P.R. 172/2007.

anche ad un ampliamento del Codice di autoregolamentazione[29].
D'altra parte le disposizioni di cui ai c. 6 e 7 dell'art. 37 del T.U. sembrano dirlo esplicitamente[30].
Il c. 6 prevede, infatti, che i fornitori di servizi di media diffusi tramite qualsiasi canale o piattaforma siano già oggi obbligati ad osservare le disposizioni oggi esistenti. Inoltre, la norma aggiunge che essi saranno tenuti anche a rispettare quelle che fossero in futuro adottate, facendo quindi presagire la necessità di un'integrazione.
A questo si aggiunge il c. 7 che stabilisce che i fornitori di servizi di media siano altresì obbligati a garantire, anche secondo quanto stabilito nel Codice, l'applicazione di specifiche misure a tutela dei minori nella fascia oraria di programmazione compresa tra le ore 16 e le ore 19 e all'interno dei programmi direttamente rivolti ai minori, con particolare riguardo ai messaggi pubblicitari, alle promozioni e ogni altra forma di comunicazione commerciale audiovisiva. In questo modo prevedendo la necessità di una specifica modifica del Codice, alla luce delle innovazioni apportate.

10. Osservazioni conclusive e sulla compatibilità del quadro giuridico rispetto alle nuove norme del regolamento

In conclusione di questo breve contributo occorre formulare alcune osservazioni sia di carattere generale relative all'analisi svolta sia specificamente riguardanti i rapporti tra il quadro giuridico analizzato e alcune nuove disposizioni introdotte dal regolamento europeo sui servizi digitali (Regolamento DSA).
La prima osservazione riguarda evidentemente il salto di qualità della disciplina europea, e di quella nazionale di recepimento, nella protezione dei minori rispetto a contenuti potenzialmente pericolosi. Questo innalzamento delle tutele passa in particolar modo dagli obblighi introdotti a carico dei fornitori di piattaforme per la condivisione di contenuti nonché dai nuovi poteri assegnati all'AGCOM. In altri termini si allarga il novero dei soggetti coinvolti (e pertanto delle fattispecie vincolate) e si rafforzano i poteri interdettivi e sanzionatori. Inoltre, si punta attraverso l'ampio ricorso alla co-regolazione al coinvolgimento dei fornitori stessi.
Tanto la responsabilizzazione dei fornitori di contenuti quanto l'approccio *risk-based* della normativa in esame ricordano molto da vicino la strategia seguita dal "Legislatore" europeo fin dall'approvazione del GDPR. Una strategia che pare oggi essere divenuta comune in molti atti normativi, già in vigore oppure ancora *in itinere* facenti parte del pacchetto digitale con cui l'UE mira a disciplinare la società digitale[31].

[29] V. in proposito, D. Pacelli – C. Rumi, *La tutela del minore nell'ambito del Codice di autoregolamentazione*, in M. Bianca (a cura di), *The best interest of the child*, Roma, 2021, 231 ss.

[30] Eventuali nuovi atti di autoregolamentazione sono recepiti con decreto del Ministro dello Sviluppo Economico, previo parere della Commissione parlamentare di cui alla l. 451/1997.

[31] A. Simoncini, *L'intervento regolamentare dell'AGCOM in materia di diritto d'autore: profili di criticità formale e sostanziale*, in *BioLaw Journal-Rivista di BioDiritto*, 2021, 411 ss., il quale avverte come tale strategia è possibile solo se si individua chiaramente il comportamento vietato e contemporaneamente quello consentito a determinate condizioni.

La seconda osservazione riguarda specificamente il tentativo di attuare l'obiettivo europeo di promuovere l'auto-regolazione e la co-regolazione.

Il tema è stato trattato recentemente da molti autori che hanno sottolineato, con diversità di accenti, quanto l'emersione di questa opzione dipenda dai fenomeni di globalizzazione tipici della società digitale, dalla sfiducia verso l'idoneità della legge a disciplinare la società digitale, dalla maggiore flessibilità che co-regolazione ed auto-regolazione garantiscono in un contesto in cui le tecnologie disponibili cambiano con estrema rapidità, dalla superiore differenziazione che co-regolazione ed auto-regolazione garantiscono rispetto alla necessaria generalità ed astrattezza della norme di legge.

Ognuna di queste letture apporta ovviamente un tassello alla comprensione di fenomeni in corso che appaiono assai complessi e mutevoli. Rispetto ad essi, si possono offrire due contributi relativi a quanto osservato in questo scritto. Il primo riguarda il fatto che il ricorso alla co-regolazione e all'auto-regolazione nel TUSMA oscilli tra due ipotesi: quella del regolamento dell'AGCOM adottato secondo procedure che prevedono la compartecipazione dei regolati e quella del Codice di condotta che l'Autorità è chiamata ad approvare al fine di renderlo vincolante anche da un punto di vista normativo. Il successo della prima ipotesi è legato alla capacità dell'AGCOM di sollecitare a monte e cogliere a valle le argomentazioni dei regolati e più in generale di tutti i soggetti interessati o comunque attivi nel settore. Il successo della seconda è, invece, strettamente dipendente dalla rappresentatività dei partecipanti al processo di elaborazione del codice di condotta[32].

La terza osservazione generale riguarda il ruolo dell'AGCOM.

L'attribuzione di poteri regolamentari è assai significativa. I regolamenti dell'AGCOM sono destinati tra l'altro a disciplinare fattispecie che incidono direttamente su posizioni soggettive dando consistenza normativa a proposizioni che nel decreto legislativo riservano margini cospicui di adattamento e d'interpretazione. È evidente che ciò risponda anche ad un disegno europeo volto a valorizzare le autorità di regolazione. Pur tuttavia non può evitarsi di segnalare come le consultazioni preventive sugli schemi di regolamento siano uno strumento debole se inteso a colmare quel deficit democratico che è inevitabile in scelte rimesse alla discrezionalità di Autorità che debbono essere e restare indipendenti. Il tema di come bilanciare l'espansione del ruolo delle autorità indipendenti preservando i circuiti di decisione politica deve tornare ad essere al centro della riflessione della dottrina. Questo perché le norme del cd. Pacchetto digitale vanno tutte nella direzione qui osservata e richiedono evidentemente dei correttivi per evitare che i Parlamenti ed i Governi nazionali risultino completamente esclusi dalla loro attuazione.

Altrettanto significativa sempre con riferimento ad AGCOM è l'attribuzione di poteri interdittivi, conformativi e sanzionatori nei confronti dei fornitori di servizi media audiovisivi e di piattaforme per la condivisione di contenuti. Se da un punto di vista teorico può dirsi che l'AGCOM assuma un ruolo di garanzia anche in materia di diritti fondamentali, testimoniando il proseguimento di una traiettoria che affianca alle

[32] Forse può dirsi che l'unica pecca sta nel fatto che l'obbligo legale di osservare tali atti non è adeguatamente esplicitato.

funzioni di regolazione quelle di controllo; da un punto di vista sostanziale occorre segnalare che tale trasformazione deve essere necessariamente accompagnata da un rafforzamento dell'Autorità stessa in termini di risorse finanziarie e di personale.
Per quanto attiene, infine, ai rapporti tra le norme del TUSMA ed il regolamento sui servizi digitali (Regolamento DSA) occorre specificare che la questione non coinvolge i fornitori di servizi media audiovisivi ma essenzialmente le piattaforme per la condivisione di contenuti[33].
In proposito il considerando 10 del DSA specifica come esso non «dovrebbe pregiudicare altri atti del diritto dell'Unione che disciplinano la prestazione di servizi della società dell'informazione, quali la direttiva 2010/13/UE così come modificata dalla direttiva (UE) 2018/1808"[34].
Questo però non è dirimente. Non solo perché, in altre parti del DSA, si specifica come esso integri l'applicazione della direttiva 2010/13/UE ma pure perché vi sono sovrapposizioni inevitabili; si pensi ad esempio alle regole che disciplinano l'ambito territoriale di applicazione delle norme.
Limitando l'esame alle norme che incidono sulla tutela dei minori si prenda ad esempio l'art. 28 del DSA. La norma contiene un obbligo ed un divieto a carico di tutti i fornitori di piattaforme che evidentemente si si sovrappongono in tutto o in parte a disposizioni presenti nel TUSMAR e qui oggetto di analisi
Nel dettaglio, l'art. 28, primo paragrafo, DSA prevede che i fornitori di piattaforme adottino le misure adeguate e proporzionate per garantire ai minori un elevato livello di tutela della vita privata, di sicurezza e di protezione sul loro servizio. La nozione di protezione elevata è certamente più ampia di quella riferita ai contenuti lesivi contenuta nel Testo Unico. Per ciò che attiene al divieto, di cui al secondo paragrafo dell'art. 28, esso impone ai fornitori di non proporre sull'interfaccia messaggi pubblicitari basati sulla profilazione del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è un minore[35]. Il divieto è molto più esteso di quelli definiti dal TUSMA e relativi solo a specifici contenuti pubblicitari.
In conclusione alcune piccole osservazioni sulla disciplina del DSA delle cd. grandi piattaforme ossia quelle che secondo la normativa hanno un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni[36]. Si tratta delle norme forse più interessanti dell'intero regolamento poiché pongono a carico di tali soggetti un *surplus* di obblighi in ragione della capacità pervasiva dei contenuti da loro veicolati. Tra di essi meritano attenzione l'obbligo di valutazione del rischio della loro attività e gli obblighi di attenuazione dei medesimi. In entrambi i casi, infatti, occorre segnalare che la tutela dei minori è parametro di valutazione così come obiettivo degli strumenti di attenuazione del rischio.

[33] Occorre ricordare che il DSA non si applica alle piattaforme che si qualifichino come micro imprese o piccole imprese. art. 19 del Regolamento DSA.

[34] La medesima previsione contenuta nel citato considerando è poi nell'art. 2 del Regolamento DSA relativo all'ambito di applicazione materiale della normativa europea.

[35] Come specificato nella norma, questa previsione non obbliga il fornitore del servizio a trattare dati personali ulteriori per accertare se il destinatario sia o meno effettivamente un minore.

[36] Art. 33 del Regolamento DSA che prevede anche un obbligo di designazione di tali soggetti da parte della Commissione europea.

Su tali previsioni qui appena accennate sarà certamente necessario riflettere in modo analitico. Per ora può dirsi che esse vanno certamente a comporre un quadro di maggior tutela destinato ad integrare, rafforzandolo, quello definito, anche per le piattaforme, dalla direttiva sui servizi media audiovisivi e dal Testo Unico italiano.

Messaggistica WhatsApp ed e-mail nel contesto delle prerogative dei membri del Parlamento *ex* art. 68, terzo comma, Cost. Prospettive costituzionali di diritto della comunicazione*

Enrico Albanesi

Abstract

Oggetto del presente commento è la questione della qualificazione giuridica di messaggistica WhatsApp e di e-mail nel contesto delle prerogative dei membri del Parlamento *ex* art. 68, c. 3, Cost. ed *ex* legge 20 giugno 2003, n. 140. Le riflessioni traggono spunto dal c.d. caso Renzi e dalla sollevazione da parte del Senato di un conflitto di attribuzione tra poteri dello Stato di fronte alla Corte costituzionale il 22 febbraio 2022. Il saggio intende dimostrare che la prospettiva più opportuna per tentare una qualificazione giuridica di messaggistica WhatsApp e di e-mail nel contesto delle prerogative dei membri del Parlamento deve necessariamente essere individuata alla luce della *ratio* sottesa alle prerogative parlamentari, dell'evoluzione degli strumenti tecnologici e del loro inquadramento giuridico nonché degli altri valori costituzionali in rilievo.

This essay analyses the legal nature of WhatsApp messages and e-mails when covered by the immunities of the Members of Parliament under article 68, section 3, of the Italian Constitution and under Law 20 June 2003, No. 140. Some general reflections will be made here with regards to the case concerning Senator Matteo Renzi, that was brought by the Italian Senate before the Italian Constitutional Court on 22 February 2022. The main hypothesis of this essay is that the legal nature of WhatsApp messages and e-mails can be shaped, first, in the light of the rationale underpinning the different immunities of the Members of Parliament, secondly, in the light of the evolution of ICTs and their legal nature, thirdly, in the light of other relevant constitutional principles.

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Sommario

1. Ipotesi di ricerca. – 2. Il fatto (il c.d. caso Renzi) e le posizioni giuridiche in campo sulla sussunzione della messaggistica WhatsApp e delle e-mail, in quanto tali, *esclusivamente* ad una (o a nessuna) fattispecie astratta di cui all'art. 68, terzo comma, Cost. ed alla legge n. 140 del 2003. Osservazioni critiche. – 3. Argomentazioni a sostegno della prospettiva qui adottata: *a*) la giurisprudenza costituzionale: la *ratio* delle differenti prerogative dei membri del Parlamento *ex* art. 68, terzo comma, Cost. ed *ex* legge n. 140 del 2003; – 4. (*segue*): *b*) l'evoluzione degli strumenti tecnologici ed il loro inquadramento giuridico: la messaggistica WhatsApp e le e-mail come *documento* a carattere *comunicativo*; – 5. (*segue*): *c*) altri valori costituzionali in rilievo: la parità di trattamento dei soggetti terzi. – 6. Conclusioni: le modalità di acquisizione della messaggistica WhatsApp e delle e-mail «nei confronti di un membro del Parlamento» come elemento di *discrimen* ai fini della riconduzione delle stesse all'art. 4 o *de iure condendo* all'art. 6 della legge n. 140 del 2003.

Keywords

messaggistica WhatsApp – e-mail – prerogative dei membri del Parlamento – sequestro di corrispondenza – intercettazioni delle conversazioni e delle comunicazioni

1. Ipotesi di ricerca

Oggetto del presente commento è la questione della qualificazione giuridica di messaggistica WhatsApp e di e-mail nel contesto delle prerogative dei membri del Parlamento *ex* art. 68, c. 3, Cost. ed *ex* legge 20 giugno 2003, n. 140.

Le riflessioni traggono spunto dal c.d. caso Renzi, cioè le vicende sviluppatesi nell'ambito di un procedimento penale pendente dinanzi alla Procura della Repubblica presso il Tribunale di Firenze nei confronti del sen. Matteo Renzi. Vicende che hanno portato il Senato della Repubblica a deliberare il 22 febbraio 2022 la sollevazione di un conflitto di attribuzione tra poteri dello Stato nei confronti della stessa Procura[1], ritenuto ammissibile dalla Corte costituzionale il 20 dicembre 2022[2]. Il caso sarà descritto oltre nel dettaglio (cfr. paragrafo 2).

Ciò che si vuole qui ora preliminarmente esporre è l'ipotesi di ricerca che si tenterà di dimostrare: cioè che la prospettiva più opportuna per tentare una qualificazione giuridica di messaggistica WhatsApp e di e-mail nel contesto delle prerogative dei membri del Parlamento, alla luce della giurisprudenza costituzionale, dell'evoluzione degli strumenti tecnologici e del loro inquadramento giuridico nonché degli altri valori costituzionali in rilievo, deve necessariamente essere diversa rispetto a quella seguita nel dibattito sui profili giuridici svoltosi presso la Giunta delle elezioni e delle immunità parlamentari e presso l'Assemblea del Senato sulla sollevazione del conflitto di

[1] Cfr. XVIII legislatura, Senato della Repubblica, Assemblea, *Resoconto stenografico*, 406ª seduta pubblica 22 febbraio 2022, 24-46.

[2] Cfr. Corte costituzionale, ord. 20 dicembre 2022, n. 261.

attribuzione nel caso in esame.

Nel corso del dibattito sono emerse infatti due distinte ricostruzioni giuridiche della messaggistica WhatsApp e delle e-mail, entrambe caratterizzate però dallo stesso approccio: quello cioè di sussumere queste ultime, in quanto tali, *esclusivamente* ad una (o a nessuna) fattispecie astratta di cui all'art. 68, c. 3, Cost. ed alla legge n. 140 del 2003.

La prima ricostruzione, sostenuta dalla relatrice della Giunta sen. Modena[3] e fatta propria dalla stessa Giunta[4] e dall'Assemblea[5], configura la messaggistica WhatsApp e le e-mail, in quanto tali, come riconducibili alla nozione di «corrispondenza»: con la conseguenza di ritenersi necessaria un'autorizzazione *ex ante* al sequestro delle stesse eseguito nei confronti di un membro del Parlamento *ex* art. 68, c. 3, Cost. ed *ex* art. 4 della legge 20 giugno 2003, n. 140.

La seconda, patrocinata dal sen. Grasso, legge invece la messaggistica WhatsApp e le e-mail, in quanto tali, come non rientranti né nella nozione di «corrispondenza» né in quella di «comunicazioni»: con la conseguenza di non risultare necessaria un'autorizzazione *ex ante* al loro sequestro *ex* art. 68, c. 3, Cost. ed *ex* art. 4 della legge 20 giugno 2003, n. 140 nei confronti di un membro del Parlamento; né un'autorizzazione *ex post* all'utilizzo delle stesse in occasione di acquisizioni casuali (dove cioè il membro del Parlamento "compaia" fortuitamente) nel corso di procedimenti riguardanti terzi *ex* art. 6 della legge n. 140 del 2003. Alla luce di questa seconda ricostruzione, la messaggistica WhatsApp e le e-mail sarebbero invece riconducibili alla nozione di «documenti»: con la conseguenza che «la relativa acquisizione non soggiace alle regole stabilite per la corrispondenza né tantomeno alla disciplina delle intercettazioni»[6].

Come si cercherà di dimostrare, nessuna delle due prospettive risulta però appagante: né dal punto di vista della giurisprudenza costituzionale e della *ratio* delle differenti prerogative dei membri del Parlamento *ex* art. 68, c. 3, Cost. ed *ex* legge n. 140 del 2003 (cfr. paragrafo 3); né dal punto di vista dell'evoluzione degli strumenti tecnologici e del loro inquadramento giuridico (cfr. paragrafo 4); neppure dal punto di vista della tutela di altri valori costituzionali, riconducibili alla posizione di soggetti terzi (cfr. paragrafo 5).

Si tenterà allora di prospettare qui una ricostruzione alternativa delle fattispecie (cfr. paragrafo 6).

---

[3] Cfr. XVIII legislatura, Senato della Repubblica, Doc. XVI n. 9, *Relazione della Giunta delle elezioni e delle immunità parlamentari.*

[4] Si veda il dibattito in Giunta, conclusosi poi con l'approvazione della proposta della relatrice nella seduta del 14 dicembre 2021. Cfr. XVIII legislatura, Senato della Repubblica, *Resoconto sommario n. 645 supplemento*, Giunta delle elezioni e delle immunità parlamentari, 16 novembre 2022, 11 ss.; *Resoconto sommario n. 651 supplemento*, Giunta delle elezioni e delle immunità parlamentari, 24 novembre 2022, 9 s.; *Resoconto sommario n. 660*, Giunta delle elezioni e delle immunità parlamentari, 9 dicembre 2022, 5 ss.; *Resoconto sommario n. 662*, Giunta delle elezioni e delle immunità parlamentari, 14 dicembre 2022, 6 ss.

[5] Cfr. XVIII legislatura, Senato della Repubblica, Assemblea, *Resoconto stenografico*, cit., 24 ss.

[6] Ivi, 37 ss.

2. Il fatto (il c.d. caso Renzi) e le posizioni giuridiche in campo sulla sussunzione della messaggistica WhatsApp e delle e-mail, in quanto tali, *esclusivamente* ad una (o a nessuna) fattispecie astratta di cui all'art. 68, terzo comma, Cost. ed alla legge n. 140 del 2003. Osservazioni critiche

Come si è accennato, le presenti riflessioni traggono spunto dalle vicende riguardanti un procedimento penale pendente dinanzi alla Procura della Repubblica presso il Tribunale di Firenze nei confronti del sen. Renzi.

Nel corso del procedimento, per quanto qui interessa, la Procura ha proceduto al sequestro di alcuni messaggi WhatsApp scambiati tra il sen. Renzi ed il sig. V.M. (acquisiti attraverso il sequestro del cellulare di quest'ultimo), quattro e-mail scambiate tra il sen. Renzi ed il dott. M.C. nonché l'estratto conto bancario del sen. Renzi. I difensori del senatore hanno quindi fatto istanza alla Procura il 21 settembre 2021 (avanzandosi formale intimazione di astenersi dallo svolgimento di qualsiasi attività investigativa preclusa ai sensi dell'art. 68 Cost. e della legge n. 140 del 2003). Su tale istanza la Procura ha dichiarato il non luogo a provvedere il 4 ottobre 2021, in quanto l'utilizzazione dei dati processuali è stata operata non nei confronti del sen. Renzi ma di altro indagato, non soggetto alle prerogative invocate dai difensori.

Ritenendo comunque lese le proprie prerogative per il solo fatto che l'acquisizione dei messaggi, delle e-mail e dell'estratto conto sia avvenuta senza previa autorizzazione della Camera di appartenenza, il sen. Renzi ha sottoposto la questione al Presidente del Senato il 7 ottobre 2021 che in data 12 ottobre 2021 ha deferito la questione alla Giunta delle elezioni ai sensi dell'art. 34, c. 1, e dell'art. 135 del regolamento del Senato, trattandosi di una materia di competenza della Giunta.

Come si è accennato, il Senato ha deliberato il 22 febbraio 2022 a favore della sollevazione di un conflitto di attribuzione tra poteri dello Stato nei confronti della Procura di Firenze, approvandosi dunque la proposta in tal senso della Giunta delle elezioni del 14 dicembre 2021. Il sequestro della messaggistica WhatsApp, delle quattro e-mail e dell'estratto conto, a prescindere dalla circostanza dell'utilizzo o meno di tali prove nei confronti del membro del Parlamento ed a prescindere dalla circostanza che il sequestro sia avvenuto presso terzi (come nel caso dell'acquisizione della messaggistica attraverso il sequestro di un cellulare di un terzo), non è infatti mai stato autorizzato dal Senato. Secondo il Senato, ciò costituirebbe dunque una violazione dell'art. 68, c. 3, Cost. poiché l'autorità giudiziaria avrebbe dovuto avanzare al Senato stesso la previa richiesta di autorizzazione a tale sequestro.

Le fattispecie che appaiono concettualmente più controverse e su cui si vuole qui svolgere alcune riflessioni, sono quella della messaggistica WhatsApp e delle e-mail. Non sembra invece porre particolari problemi dal punto di vista teorico la fattispecie del conto corrente bancario e presentare se mai quest'ultima solo qualche aspetto ricostruttivo controverso, che però sembra attenere piuttosto alla non chiara (stando agli

atti parlamentari che si è potuto consultare) configurazione della fattispecie concreta[7]. Entrambe le opposte ricostruzioni prospettate nel corso del dibattito al Senato sembrano presentare dei profili controversi.

Nella relazione della Giunta delle elezioni si è richiamato il fatto che il concetto di corrispondenza ha subito un'evoluzione "tecnologica" e che al tradizionale formato cartaceo si sono aggiunte forme di corrispondenza di tipo elettronico, quali e-mail, SMS, messaggi WhatsApp. Sarebbero dunque due caratteristiche proprie della corrispondenza (la forma scritta e la segretezza) a consentire di ricondurre tali fattispecie nell'ambito dell'art. 68, c. 3, Cost., sotto l'etichetta di (sequestro di) «corrispondenza» e non sotto l'etichetta di (intercettazioni di) «conversazioni o comunicazioni», che invece presupporrebbero conversazioni orali. La conseguenza di tale ricostruzione è la necessità che l'autorità giudiziaria richieda un'autorizzazione *ex ante* al sequestro di tale corrispondenza ai sensi dell'art. 68, c. 3, Cost. e dell'art. 4 della legge 20 giugno 2003, n. 140, «a prescindere dalla circostanza dell'utilizzo o meno di tali prove nei confronti del parlamentare stesso» e «a prescindere anche dalla circostanza che il sequestro avvenga "presso terzi"»[8].

Nel suo intervento il sen. Grasso ha sottolineato invece come la messaggistica WhatsApp e le e-mail non possano ricondursi né alla nozione di «corrispondenza», la quale «implica attività dinamiche di spedizione e di ricezione»; né a quella di (intercettazione di) comunicazioni, dato che quest'ultima richiede «la captazione di un flusso di comunicazioni in corso». Tali fattispecie costituirebbero invece documenti, cioè «un *tertium genus* non previsto dalla legge […] n. 140 del 2003». Il sen. Grasso ha richiamato a sostegno di tale tesi la giurisprudenza della Cassazione che configura appunto come documenti «sms, WhatsApp, posta elettronica scaricata o conservata nella memoria, rinvenuti in un cellulare sottoposto a sequestro»[9]. La conseguenza di tale ricostruzione è la non riconducibilità di tali fattispecie né all'art. 68, c. 3, Cost. ed all'art. 4 della legge n. 140 del 2003, né all'art. 6 della legge n. 140 del 2003.

Le due ricostruzioni, imperniate sulla sussunzione della messaggistica WhatsApp e delle e-mail, in quanto tali, esclusivamente ad una (o a nessuna) fattispecie astratta di cui all'art. 68, c. 3, Cost, ed alla legge n. 140 del 2003, non convincono.

Non convince la prima. In primo luogo, perché essa individua la caratteristica della corrispondenza nella natura scritta, senza tenersi quindi conto fino in fondo dell'evoluzione degli strumenti tecnologici: seguendosi tale linea, non dovrebbero rientrare nell'etichetta di corrispondenza, ad esempio, messaggi WhatsApp orali. In secondo luogo (come è d'altronde evidente dal fatto che nella relazione si ragioni «a prescin-

[7] Con riguardo al contro corrente bancario, il profilo controverso, nel caso concreto, è se si sia trattato di un sequestro di un «estratto conto inviato dalla banca al senatore» (come si legge a pagina 5 della relazione della relatrice, sopra citata in nota 3), in quanto tale riconducibile quindi alla nozione di «corrispondenza» *ex* art. 68, c. 3, Cost. ed *ex* art. 4 della legge n. 140 del 2003; oppure, «di un documento acquisito legittimamente dalla magistratura, tramite richiesta alla banca, a seguito di una segnalazione di operazione sospetta, come tale prevista dalla legge», estraneo dunque alla nozione di «corrispondenza» *ex* art. 68, c. 3, Cost. ed *ex* art. 4 della legge n. 140 del 2003 (come prospettato dal sen. Grasso a pagina 38 nell'intervento del 22 febbraio 2022, sopra citato in nota 6).

[8] Cfr. XVIII legislatura, Senato della Repubblica, Doc. XVI n. 9, cit., 4 s.

[9] Cfr. XVIII legislatura, Senato della Repubblica, Assemblea, *Resoconto stenografico*, cit., 37 s.

dere» dalle due circostanze sopra menzionate che, come si dirà, in realtà dovrebbero essere rilevanti), perché non consente di operare alcuna distinzione né alla luce della *ratio* sottesa alle differenti prerogative parlamentari, né delle caratteristiche degli strumenti tecnologici e del loro inquadramento giuridico, né di altri valori costituzionali che potrebbero venire in rilievo.
Non convince neppure la seconda ricostruzione. Per difetto: essa esclude dalla nozione di «corrispondenza» quelle fattispecie che, se pur attraverso modalità tecnologiche, implicano comunque attività dinamiche di spedizione e di ricezione, come quelle che si compiono quando si invia o si riceve un messaggio WhatsApp o una e-mail. Per eccesso: nel richiamarsi la giurisprudenza della Cassazione sulla messaggistica WhatsApp e sulle e-mail da intendersi quali documenti, sembra trascurarsi il fatto che quei casi non vedessero coinvolti (direttamente, indirettamente o casualmente) membri del Parlamento.
Si tornerà oltre su questi punti. Qui conta ora solo ribadire come in definitiva la prospettiva più corretta non sembra essere quella di sussumere tali fattispecie, in quanto tali, esclusivamente ad una (o a nessuna) fattispecie astratta di cui all'art. 68, c. 3, Cost. e della legge n. 140 del 2003. Quanto piuttosto quella di tentare una qualificazione giuridica della messaggistica WhatsApp e di e-mail nel contesto delle prerogative dei membri del Parlamento alla luce della giurisprudenza costituzionale, dell'evoluzione degli strumenti tecnologici e del loro inquadramento giuridico, nonché degli altri valori costituzionali in rilievo.

3. Argomentazioni a sostegno della prospettiva qui adottata: a) la giurisprudenza costituzionale: la *ratio* delle differenti prerogative dei membri del Parlamento *ex* art. 68, terzo comma, Cost. ed *ex* legge n. 140 del 2003;

Sono tre gli argomenti a sostegno della necessità di trovare una prospettiva alternativa a quelle elaborate nel corso del dibattito al Senato.
Il primo può trarsi dalla giurisprudenza costituzionale e riguarda la *ratio* delle differenti prerogative dei membri del Parlamento ai sensi dell'art. 68, c. 3, Cost. e della legge n. 140 del 2003.
Nella sent. n. 390 del 2007 la Corte costituzionale ha chiarito perfettamente la *ratio* sottesa a ciascuna delle prerogative di cui all'art. 68, c. 3, Cost. e di cui agli artt. 4 e 6 della legge n. 140 del 2003, facendo peraltro la Corte chiarezza anche a livello terminologico tra intercettazioni c.d. dirette, indirette e casuali (termini su cui, specie sul secondo, continuano tuttavia a registrarsi imprecisioni nell'uso corrente).
Scrive la Corte che l'art. 68, c. 3, Cost. (incentrato sul meccanismo dell'autorizzazione *ex ante*)[10], «mira a porre a riparo il parlamentare da illegittime interferenze giudi-

[10] L'art. 68, c. 3, Cost. dispone che: «Analoga autorizzazione [della Camera alla quale appartengono] è richiesta per sottoporre i membri del Parlamento ad intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni e a sequestro di corrispondenza».

ziarie sull'esercizio del suo mandato rappresentativo; a proteggerlo, cioè, dal rischio che strumenti investigativi di particolare invasività o atti coercitivi delle sue libertà fondamentali possano essere impiegati con scopi persecutori, di condizionamento, o comunque estranei alle effettive esigenze della giurisdizione». In tale prospettiva, precisa la Corte, il bene protetto si identifica con «l'esigenza di assicurare il corretto esercizio del potere giurisdizionale nei confronti dei membri del Parlamento, e non con gli interessi sostanziali di questi ultimi (riservatezza, onore, libertà personale), in ipotesi pregiudicati dall'atto». L'art. 68, c. 3, Cost. non mira dunque a salvaguardare la riservatezza delle comunicazioni del parlamentare in quanto tale ma è strumentale alla salvaguardia delle funzioni parlamentari: volendosi impedire, aggiunge la Corte, che «l'ascolto di colloqui riservati da parte dell'autorità giudiziaria possa essere indebitamente finalizzato ad incidere sullo svolgimento del mandato elettivo, divenendo fonte di condizionamenti e pressioni sulla libera esplicazione dell'attività». La Corte precisa peraltro (in un inciso che risulterà particolarmente rilevante nell'ottica del presente commento) che ciò avviene analogamente per l'autorizzazione preventiva alle perquisizioni ed ai sequestri di corrispondenza, il cui oggetto ben può consistere anche «in documenti di carattere comunicativo»[11].

In quest'ottica, l'art. 4 della legge n. 140 del 2003[12], costituisce sviluppo dell'art. 68, c. 3, Cost., disciplinando esso il meccanismo dell'autorizzazione *ex ante*, da parte della Camera di appartenenza, all'esecuzione delle intercettazioni c.d. dirette (cioè quelle, come si ricava *a contrario* dalle parole della Corte sulle intercettazioni c.d. indirette, effettuate ponendo sotto controllo le utenze dei membri del Parlamento) e delle intercettazioni c.d. indirette (intese, secondo le parole della Corte, come «captazioni delle conversazioni del membro del Parlamento effettuate ponendo sotto controllo le utenze dei suoi interlocutori abituali»[13]).

Dall'art. 68, c. 3, Cost. esulano invece le intercettazioni c.d. casuali o fortuite: quelle cioè caratterizzate dal «carattere imprevisto dell'interlocuzione del parlamentare»[14]. In questo caso la *ratio* di un'eventuale prerogativa avente ad oggetto siffatte intercetta-

---

[11] Cfr. Corte cost., sent. 23 novembre 2007, n. 390, § 5.2 *Considerato in diritto*. Tale *ratio* emerge anche dall'esame dei lavori preparatori dell'art. 68, c. 3, Cost., come modificato nel 1993. Cfr. in proposito M. Cerase, *Anatomia critica delle immunità parlamentari italiane*, Rubbettino, 2011, 161 ss. Dà un giudizio positivo sulla sentenza, definita come «importante ed equilibrata», N. Zanon, *Il regime delle intercettazioni "indirette" e "occasionali" fra principio di parità di trattamento davanti alla giurisdizione e tutela della funzione parlamentare,* in *federalismi.it,* 2007, n. 23. Sottolinea invece alcune incongruenze tra l'impianto argomentativo della Corte e l'assetto dato alle intercettazioni c.d. indirette T. Giupponi, *Le intercettazioni "indirette" nei confronti dei parlamentari e la legge n. 140/2003: cronaca di un'illegittimità costituzionale (pre)annunciata,* in *formucostituzionale.it*, 2007.

[12] L'art. 4, c. 1, dispone che «Quando occorre eseguire nei confronti di un membro del Parlamento perquisizioni personali o domiciliari, ispezioni personali, intercettazioni, in qualsiasi forma, di conversazioni o comunicazioni, sequestri di corrispondenza, o acquisire tabulati di comunicazioni, ovvero, quando occorre procedere al fermo, all'esecuzione di una misura cautelare personale coercitiva o interdittiva ovvero all'esecuzione dell'accompagnamento coattivo, nonché di misure di sicurezza o di prevenzione aventi natura personale e di ogni altro provvedimento privativo della libertà personale, l'autorità competente richiede direttamente l'autorizzazione della Camera alla quale il soggetto appartiene».

[13] Cfr. Corte cost., sent. 23 novembre 2007, n. 390, cit., § 5.3 *Considerato in diritto*.

[14] *Ibid.*

zioni, non può essere quella appena richiamata con riferimento all'art. 68, c. 3, Cost. perché «l'eventualità che l'esecuzione dell'atto sia espressione di un atteggiamento persecutorio – o, comunque, di un uso distorto del potere giurisdizionale nei confronti di un membro del Parlamento, volto ad interferire indebitamente sul libero esercizio delle sue funzioni – resta esclusa, di regola, proprio dalla accidentalità dell'ingresso del parlamentare nell'area di ascolto»[15]. La *ratio* qui è dunque quella di tutelare la riservatezza del parlamentare, rispetto ad un mezzo di ricerca della prova particolarmente invasivo, come le intercettazioni, specie alla luce di quel «fenomeno patologico che incide, di per sé, sulla generalità dei cittadini: quello, cioè, della disinvolta diffusione, anche a mezzo stampa, dei contenuti dei colloqui intercettati, spesso anche per parti irrilevanti ai fini del processo»[16].

La Corte chiarisce a tal proposito che, se un'eventuale prerogativa avente ad oggetto le intercettazioni c.d. casuali esula dall'art. 68, c. 3, Cost. e non deve considerarsi dunque «costituzionalmente imposta», ciò non vuol dire che non possa ritenersi «costituzionalmente consentita»[17]. Ecco dunque l'art. 6 della legge n. 140 del 2003 che dispone il meccanismo dell'autorizzazione *ex post*, da parte della Camera di appartenenza, all'utilizzo dei risultati delle intercettazioni[18]. Per il carattere imprevisto dell'interlocuzione del parlamentare, qui l'autorità giudiziaria non potrebbe infatti, «neanche volendo, munirsi preventivamente del *placet* della Camera di appartenenza»[19].

L'aver richiamato la prospettiva della Corte costituzionale sulla diversa *ratio* sottesa alle varie prerogative di cui all'art. 68, c. 3, Cost. e di cui agli artt. 4 e 6 della legge n. 140 del 2003, appare particolarmente fruttuoso in questa sede perché sembra aver dimostrato come la Corte costituzionale non ragioni in termini di riconduzione esclusiva dei mezzi di comunicazione a differenti fattispecie astratte riguardanti le prerogative dei membri del Parlamento (come è emerso invece nel dibatto al Senato sull'inquadramento della messaggistica WhatsApp e delle e-mail). La Corte ragiona piuttosto in termini di *ratio* sottesa alle differenti prerogative, tanto che lo stesso mezzo investigativo (l'intercettazione) riguardante lo stesso mezzo di comunicazione (le conversazioni e le comunicazioni) può benissimo essere ricondotto all'art. 4 oppure all'art. 6 della legge n. 140 del 2003 a seconda della differente modalità di acquisizione nei confronti del membro del Parlamento: se cioè l'intercettazione è avvenuta «nei confronti di un membro del Parlamento» (art. 4) oppure su «conversazioni o comunicazioni […] nel corso di procedimenti riguardanti terzi, alle quali hanno preso parte membri del Par-

15 *Ibid.*

16 *Ibid.*

17 Ivi, § 5.5 *Considerato in diritto.*

18 L'art. 6, c. 1, dispone che «Fuori dalle ipotesi previste dall'articolo 4, il giudice per le indagini preliminari, anche su istanza delle parti ovvero del parlamentare interessato, qualora ritenga irrilevanti, in tutto o in parte, ai fini del procedimento i verbali e le registrazioni delle conversazioni o comunicazioni intercettate in qualsiasi forma nel corso di procedimenti riguardanti terzi, alle quali hanno preso parte membri del Parlamento, ovvero i tabulati di comunicazioni acquisiti nel corso dei medesimi procedimenti, sentite le parti, a tutela della riservatezza, ne decide, in camera di consiglio, la distruzione integrale ovvero delle parti ritenute irrilevanti, a norma dell'articolo 269, commi 2 e 3, del codice di procedura penale».

19 Cfr. Corte cost., sent. 23 novembre 2007, n. 390, cit., § 5.3 *Considerato in diritto.*

lamento» (art. 6).

4. (*segue*): b) l'evoluzione degli strumenti tecnologici e del loro inquadramento giuridico: la messaggistica WhatsApp e le e-mail come *documento* a carattere *comunicativo*

Il secondo argomento può trarsi dall'evoluzione degli strumenti tecnologici e del loro inquadramento giuridico[20].

Come si è accennato, nella sent. 390 del 2007 la Corte costituzionale fa espresso riferimento al fatto che l'art. 68, c. 3, Cost. e l'art. 4 della legge n. 140 del 2003 si riferiscano anche alle perquisizioni ed ai sequestri di corrispondenza, «il cui oggetto ben può consistere anche in documenti di carattere comunicativo»[21]. A differenza di quanto sostenuto dal sen. Grasso[22], la messaggistica WhatsApp e le e-mail sembrano dunque riconducibili alla nozione di «corrispondenza» di cui all'art. 68, c. 3, Cost.[23], in quanto sono documenti che però in qualche modo "tengono traccia", su un supporto fisico, di una comunicazione. Peraltro, come si è già detto sopra in modo critico rispetto alla tesi della relatrice sen. Modena[24], anche messaggistica WhatsApp orale potrebbe benissimo quindi rientrare in tale nozione.

Come è stato acutamente notato da una più generale prospettiva costituzionalistica, «le norme a tutela delle varie forme di corrispondenza si riferiscono generalmente al supporto fisico sul quale viene graficamente fissato il pensiero o la comunicazione (rispettivamente, la lettera o la cartolina, il modulo su cui viene trascritto il messaggio telegrafico, i fonogrammi o i dispacci trascritti dal telefonista, il dischetto su cui è memorizzato il messaggio)»; mentre «il termine comunicazione (telegrafica, telefonica, informatica o telematica) intende riferirsi piuttosto al momento dinamico del processo comunicativo»[25].

Viene però a questo punto da chiedersi se la messaggistica WhatsApp e le e-mail possono essere viste anche nel loro momento dinamico del processo comunicativo e dunque quali «comunicazioni»; e possano essere dunque ricondotte anche all'art. 6 della legge n. 140 del 2003. Nella prospettiva costituzionalistica, per «comunicazione»

[20] Ad esempio, l'art. 616, c. 4, c.p. (come modificato nel 1993) oggi dispone che «per "corrispondenza" si intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza».

[21] Cfr. Corte cost., sent. 23 novembre 2007, n. 390, cit., § 5.2 *Considerato in diritto*.

[22] Cfr. *retro* paragrafo 2.

[23] É stato sottolineato, ad esempio, che l'art. 68, c. 3, Cost. si riferisce anche al sequestro di corrispondenza di cui all'art. 254 c.p.p. (il quale, in ogni caso, presuppone comunque nel mittente o nel destinatario della posta la qualità di imputato). Così M. Cerase, *Anatomia critica delle immunità,* cit., 184. Si ricorda che ai sensi dell'art. 254 c.p.p., presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni, è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica.

[24] Cfr. *retro* paragrafo 2.

[25] Cfr. A. Valastro, *Libertà di comunicazione e nuove tecnologie. Inquadramento costituzionale e prospettive di tutela delle nuove forme di comunicazione interpersonale,* Milano, 2001, 117.

si intende d'altronde un concetto generale cui sono riconducibili tutte le forme esplicative della libertà di cui all'art. 15 Cost.[26]: quest'ultimo «comprende tanto la "corrispondenza" quanto le "altre forme di comunicazione", incluse quelle telefoniche, elettroniche, informatiche, tra presenti o effettuate con gli altri mezzi resi disponibili dallo sviluppo della tecnologia»[27], come sottolineato dalla Corte costituzionale nel 2017[28]. Anche la normativa europea[29] e la disciplina nazionale di attuazione[30] riconducono oggi i messaggi di posta elettronica ed i servizi di messaggistica alla nozione di servizi di comunicazione interpersonale.

A tale notazione possono tuttavia essere opposte alcune obiezioni che, come notato dal sen. Grasso, escluderebbero la possibilità di considerare come «comunicazioni» la messaggistica WhatsApp e le e-mail e quindi di ricondurre queste ultime all'art. 6 della legge n. 140 del 2003[31].

La prima è che la giurisprudenza della Cassazione ha qualificato la messaggistica WhatsApp e le e-mail come documenti. La Cassazione ha infatti chiarito che «i dati informativi acquisiti dalla memoria del telefono dell'indagata (sms, messaggi WhatsApp, messaggi di posta elettronica "scaricati" e/o conservati nella memoria dell'apparecchio cellulare) hanno natura di documenti ai sensi dell'art. 234 cod. proc. pen., di tal che la relativa attività acquisitiva non soggiace né alle regole stabilite per la corrispondenza, né tantomeno alla disciplina delle intercettazioni telefoniche»[32].

Si tratta tuttavia di statuizioni che la Cassazione ha riferito, appunto, a dati informativi acquisiti dalla memoria del telefono di un privato cittadino, ai fini della loro valutazione circa la legittimità della loro acquisizione probatoria. La controversa fattispecie di cui si sta invece discutendo in questa sede, è invece completamente diversa, trattandosi di comunicazioni di un membro del Parlamento e venendo dunque in rilievo specifiche esigenze costituzionali meritevoli di tutela[33]. È dunque specificamente all'art. 68, c. 3, Cost. ed alla legge n. 140 del 2003, quali discipline speciali delle comunicazioni dei

---

[26] *Ibid.*

[27] Cfr. Corte cost., sent. 24 gennaio 2017, n. 20, § 3.3 *Considerato in diritto*. In questa prospettiva, cfr. ora R. Zaccaria - A. Valastro - E. Albanesi, *Diritto dell'informazione e della comunicazione,* Padova, 2021, 70 ss.

[28] Tali mezzi non sono tuttavia equivalenti, precisa la Corte, specie in ragione del loro differente «grado di materializzazione», tale da giustificare differenti modalità di ricerca della prova. Cfr. Corte cost., sent. 24 gennaio 2017, n. 20, cit., § 3.5 *Considerato in diritto*. Su quest'ultimo profilo, cfr. D. Coduti, *Libertà e segretezza della corrispondenza dei detenuti nella sentenza n. 20 del 2017 della Corte costituzionale,* in *federalismi.it,* 2017, Focus Human Rights n. 2, 6 ss.

[29] Cfr. l'art. 2, n. 4, della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche (rifusione) nonché, espressamente, il *Considerando 17* della stessa. Cfr. R. Zaccaria - A. Valastro - E. Albanesi, *Diritto dell'informazione e della comunicazione,* cit., 176 s.

[30] Cfr. l'art. 2, c. 1, lett. fff), n. 2) del d.lgs. 8 novembre 2021, n. 207, *Attuazione della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche (rifusione).*

[31] Cfr. *retro* paragrafo 2.

[32] Cfr. Cass. pen., sez. VI, 17 gennaio 2020, n. 1822 nonché, da ultimo, Cass. pen., sez. V, 6 maggio 2021, n. 17552.

[33] In definitiva, nel caso specifico non si tratta di stabilire «cosa sia corrispondenza per il semplice cittadino». Così S. Curreri, *La libertà di comunicazione del parlamentare. Riflessioni sul "caso Renzi",* in *lacostituzione.info*, 4 marzo 2022.

membri del Parlamento, che occorre fare qui riferimento.
La seconda obiezione è che proprio l'art. 68, c. 3, Cost. (e quindi l'art. 6 della legge n. 140 del 2003), quando menziona intercettazioni «in qualsiasi forma», intenderebbe riferirsi solamente alla distinzione tra intercettazioni telefoniche e quelle ambientali, ma non a forme di comunicazione diverse.
In realtà la Corte costituzionale, nella sent. n. 390 del 2007, nota come la formula «in qualsiasi forma» fu introdotta nel corso del procedimento di revisione costituzionale (al posto dell'originaria formula «intercettazioni telefoniche e ambientali») non solo a fronte della estraneità della formula «intercettazioni ambientali» dal codice di rito, ma anche per l'opportunità di adottare «una formula più generica, atta ad abbracciare ogni possibile mezzo comunicativo»[34].
La terza obiezione (in realtà "viziata" dalla giurisprudenza della Cassazione menzionata che però, come si è detto, non riguarda fattispecie che coinvolgono membri del Parlamento) è che le «intercettazioni» di cui all'art. 68, c. 3, Cost. (e quindi all'art. 6 della legge n. 140 del 2003) implicherebbero, quale oggetto, un flusso di comunicazioni in corso.
Anche qui si potrebbe però ribattere che la Corte costituzionale, come si è appena detto, nella sent. n. 390 del 2007 fa riferimento a «qualsiasi mezzo di comunicazione» che, dunque, potrebbe essere oggetto di un'intercettazione *lato sensu* intesa. Anche messaggistica WhatsApp o e-mail, alle quali hanno preso parte membri del Parlamento e trovate nel cellulare di un terzo, nel momento in cui venga acquisito il supporto fisico della comunicazione, potrebbero cioè essere intese come «comunicazioni intercettate»: dandosi dunque a quest'ultima formula un'interpretazione estensiva, se viste nell'ottica della tutela delle prerogative del membro del Parlamento. D'altronde, se si assume che la *ratio* dell'art. 6 della legge n. 140 del 2003 sia la tutela della riservatezza, tale esigenza sembra sussistere sia nel caso di un flusso di comunicazioni in corso sia nel caso in cui il flusso di comunicazioni si sia concluso.
Può però una simile interpretazione estensiva ritenersi conforme al «senso più aderente al testo normativo», criterio che la Corte costituzionale richiede ove siano in rilievo immunità e prerogative a tutela della funzione parlamentare[35]? Si deve riconoscere che con una tale interpretazione si andrebbe oltre il dato letterale: come si legge nel Dizionario della lingua Treccani, «intercettare» significa «ricevere, venire in possesso di messaggi, notizie, comunicazioni trasmesse ad altro destinatario sia per iscritto, sia per via telegrafica, telefonica, per via radio o mediante segnali ottici, senza impedirne la prosecuzione ma agendo in modo che né il mittente né il destinatario se ne accorgano».
La via di sussumere la messaggistica WhatsApp e delle e-mail all'art. 6 della legge n. 140 del 2003 sembra dunque preclusa dal lato letterale: da questo punto di vista, l'esito è dunque analogo al percorso interpretativo del sen. Grasso.
Tuttavia, non sembra che la chiave di lettura (sulla potenziale riconducibilità degli strumenti tecnologici in esame ad una pluralità di fattispecie) sia stata qui seguita infruttuosamente.

[34] Cfr. Corte cost., sent. 23 novembre 2007, n. 390, cit., § 5.1 *Considerato in diritto*.

[35] *Ibid.*

In primo luogo, perché ha consentito comunque di ricondurre gli strumenti tecnologici in esame quantomeno alla nozione di corrispondenza di cui all'art. 68, c. 3, Cost. ed all'art. 4 della legge n. 140 del 2003 (esito invece escluso dalla lettura del sen. Grasso).
In secondo luogo, perché ha consentito di mettere in evidenza il fatto che, se si assume che la *ratio* dell'art. 6 della legge n. 140 del 2003 sia la tutela della riservatezza, tale esigenza sembra sussistere sia nel caso di un flusso di comunicazioni in corso, sia nel caso in cui il flusso di comunicazioni si sia concluso e sia ormai fissato su supporto fisico. Differente discorso è se mai chiedersi se l'art. 6 della legge n. 140 del 2003 ricomprenda nel suo ambito la fattispecie dell'acquisizione di tale supporto fisico ma, come si è detto, il dato letterale sembra costituire un ostacolo insormontabile in tal senso.
In terzo luogo, perché (ove non intervenisse il legislatore) potrebbe essere la Corte costituzionale, in sede di conflitto di attribuzione attualmente pendente, a procedere ad un'auto-rimessione della questione di legittimità costituzionale della norma di cui all'art. 6 della legge n. 140 del 2003, nella parte in cui non prevede, tra le fattispecie in esame, anche quella della acquisizione di siffatto supporto fisico, *sub specie* di «sequestro della corrispondenza», in parallelismo con l'art. 4 della stessa legge.
Certo, è assai difficile che la Corte costituzionale riconosca una siffatta illegittimità costituzionale dell'art. 6 della legge n. 140 del 2003 per violazione dell'art. 68, c. 3, Cost.: non va dimenticato che la Corte costituzionale ha qualificato la prerogativa avente ad oggetto le intercettazioni c.d. casuali non come «costituzionalmente imposta» ma come «costituzionalmente consentita»[36].
Tuttavia, ciò non toglie che nei medesimi termini la Corte possa dichiarare l'illegittimità costituzionale dell'art. 6 della legge n. 140 del 2003 per violazione dell'art. 3 Cost., in quanto è esclusa dalla disciplina una fattispecie (l'acquisizione del supporto fisico su cui è fissata la comunicazione) per la quale sussiste un'esigenza, quella di tutelare la riservatezza dei membri del Parlamento, che è tuttavia analoga a quella sottesa alla fattispecie (l'intercettazione di comunicazioni) disciplinata legislativamente.

5. (*segue*): c) altri valori costituzionali in rilievo: la parità di trattamento dei soggetti terzi

Il terzo argomento può trarsi dalla necessità di offrire tutela ad altri valori costituzionali in rilievo che coinvolgono la posizione dei soggetti terzi. Quantomeno, alla luce di ciò che si è sottolineato nel paragrafo precedente: nella prospettiva cioè in cui sull'art. 6 della legge n. 140 del 2003 intervenga il legislatore o, nei termini che si sono appena detti, la Corte costituzionale.
La principale preoccupazione del sen. Grasso a fronte della ricostruzione prospettata dalla Giunta e fatta poi propria dall'Assemblea, deriva dal fatto che nella relazione della Giunta la messaggistica WhatsApp e le e-mail siano configurate come corrispondenza ai sensi dell'art. 68, c. 3, Cost. e dell'art. 4 della legge 20 giugno 2003, n. 140, «a prescindere dalla circostanza dell'utilizzo o meno di tali prove nei confronti del parlamentare stesso» ed «a prescindere anche dalla circostanza che il sequestro avven-

[36] Ivi, § 5.5 *Considerato in diritto*.

ga "presso terzi"»[37]. Questo, ha sottolineato il sen. Grasso, comporterebbe in particolare la conseguenza abnorme di rendere inutilizzabili nei confronti del terzo anche documenti legittimamente sequestrati a quest'ultimo, per il sol fatto che un membro del Parlamento casualmente "compaia" nella comunicazione. Proprio perché il membro del Parlamento "compare" nella messaggistica WhatsApp o nelle e-mail del tutto casualmente, sarebbe infatti impossibile ottenere un'autorizzazione preventiva della Camera di appartenenza: tali risultanze probatorie sarebbero quindi da ritenersi illegittime e non potrebbero essere utilizzate nei confronti del terzo. Con la conseguenza di una disparità di trattamento non solo tra il parlamentare ed i terzi ma tra gli stessi terzi, ove si pensi che alcuni di questi vedrebbero inutilizzabili nei propri confronti tali risultanze probatorie, per il sol fatto che un membro del Parlamento sia "comparso" nella messaggistica WhatsApp o nelle e-mail del tutto casualmente.

Non sarebbe in questo caso neppure disponibile il meccanismo di "salvataggio" introdotto dalla Corte costituzionale nella sentenza n. 390 del 2007 rispetto all'art. 6 della legge n. 140 del 2003 che con riguardo alle intercettazioni c.d. casuali consente oggi all'autorità giudiziaria: qualora intenda utilizzare le intercettazioni solo nei confronti dei terzi, di non munirsi dell'autorizzazione della Camera di appartenenza; qualora invece intenda utilizzarle sia nei confronti dei terzi che del parlamentare, di utilizzarle limitatamente ai terzi, ove la Camera di appartenenza neghi l'autorizzazione all'utilizzo nei confronti del parlamentare[38].

Ebbene, ove il legislatore o la Corte costituzionale "estendano" la disciplina dell'art. 6 della legge n. 140 del 2003 all'acquisizione del supporto fisico su cui è fissata la comunicazione, l'autorità giudiziaria si vedrebbe riconosciuta (alla luce della sent. n. 390 del 2007) la possibilità: qualora intenda utilizzare i risultati di tale acquisizione solo nei confronti dei terzi, di non munirsi dell'autorizzazione della Camera di appartenenza; qualora invece intenda utilizzarle sia nei confronti dei terzi che del parlamentare, di utilizzarle limitatamente ai terzi, ove la Camera di appartenenza neghi l'autorizzazione all'utilizzo nei confronti del parlamentare.

In definitiva, ove si adottasse una prospettiva alternativa a quelle emerse dal dibattito al Senato, un intervento del legislatore o della Corte costituzionale consentirebbero, tenuto conto di quanto già statuito dalla Corte nella sent. n. 390 del 2007, di assicurare la parità di trattamento dei terzi.

6. Conclusioni: le modalità di acquisizione della messaggistica WhatsApp e delle e-mail «nei confronti di un membro del Parlamento» come elemento di *discrimen* ai fini della riconduzione delle stesse all'art. 4 o *de iure condendo* all'art. 6 della legge n. 140 del 2003

L'ipotesi di ricerca che si è inizialmente avanzata appare ormai dimostrata: la prospettiva più opportuna per tentare una qualificazione giuridica della messaggistica

[37] Cfr. XVIII legislatura, Senato della Repubblica, Doc. XVI n. 9, cit., 4 s.

[38] Cfr. Corte cost., sent. 23 novembre 2007, n. 390, cit., § 6 *Considerato in diritto*.

WhatsApp e di e-mail nel contesto delle prerogative dei membri del Parlamento, non sembra essere quella di sussumerle, in quanto tali, esclusivamente ad una (o a nessuna) fattispecie astratta di cui all'art. 68, c. 3, Cost. ed alla legge n. 140 del 2003.
Alla luce della giurisprudenza della Corte costituzionale (che distingue la *ratio* sottesa alle prerogative di cui all'art. 68, c. 3, Cost. e dell'art. 4 della legge n. 140 del 2003, da un lato, ed alla prerogativa di cui all'art. 6 della legge n. 140 del 2003, dall'altro), della natura tecnologica della messaggistica WhatsApp e delle e-mail nonché dell'esigenza di tutelare la parità di trattamento dei terzi, la prospettiva più opportuna appare allora quella di guardare se la messaggistica WhatsApp e le e-mail siano state acquisite o meno «nei confronti di un membro del Parlamento» (per usare le parole dell'art. 4 della legge n. 140 del 2003).
Ove ricorra tale requisito, l'autorità giudiziaria dovrà chiedere un'autorizzazione *ex ante* alla Camera di appartenenza ai sensi dell'art. 4 della legge n. 140 del 2003, poiché, per le ragioni che si sono qui argomentate, l'acquisizione della messaggistica WhatsApp e le e-mail costituiscono «sequestro di corrispondenza».
Ove non ricorra tale requisito, allo stato attuale della legislazione, tale fattispecie non potrebbe ricondursi all'art. 6 della legge n. 140 del 2003, poiché il dato letterale (che fa riferimento a «comunicazioni intercettate») sembra impedirlo. Ciò non toglie, tuttavia, che il legislatore o la Corte costituzionale, nei termini che si sono detti, possa benissimo "estendere" l'art. 6 della legge n. 140 del 2003 alla fattispecie dell'acquisizione del supporto su cui è fissata la comunicazione.
Cosa vuol dire tuttavia l'espressione «nei confronti di un membro del Parlamento»?
Dalla sent. n. 390 del 2007 si ricava che a tal fine deve guardarsi alla «direzione dell'atto d'indagine»: il parlamentare deve essere «individuato in anticipo come destinatario dell'attività di captazione, ancorché questa abbia luogo monitorando utenze di diversi soggetti»[39] (è quest'ultimo il caso delle intercettazioni c.d. indirette). In altre parole, ciò che conta non è la titolarità o la disponibilità dell'utenza captata ma la «direzione dell'atto d'indagine»: se quest'ultimo «è volto, in concreto, ad accedere nella sfera delle comunicazioni del parlamentare, l'intercettazione non autorizzata è illegittima, a prescindere che il procedimento riguardi terzi o che le utenze sottoposte a controllo appartengano a terzi»[40]. Di ciò (cioè la direzione dell'atto di indagine) il Senato tenne conto, ad esempio, nell'esaminare il caso in cui l'autorità giudiziaria avanzò richiesta di autorizzazione *ex* art. 68, c. 3, Cost. al sequestro di due *computer* nella disponibilità del sen. Armando Siri, nell'ambito di un procedimento penale nei suoi confronti[41]. Così come fece la Camera a fronte della richiesta da parte dell'autorità giudiziaria, *ex* art. 6 della legge n. 140 del 2003, di autorizzazione all'utilizzo di intercettazioni casuali che avevano coinvolto l'on. Francesco Saverio Romano, sottolineandosi come in quel caso non fosse invece emerso mai dagli atti di indagine «un orientamento o una 'mira" dell'indagine volti alla captazione di conversazioni del parlamentare»[42].

[39] Ivi, § 5.3 *Considerato in diritto*.

[40] *Ibid.* Si veda sul punto, con un'analisi problematica dei successivi sviluppi, M. Cerase, *Anatomia critica delle immunità,* cit., 170 ss.

[41] Cfr. XVIII legislatura, Senato della Repubblica, Doc. IV n. 2-A.

[42] Cfr. XVI legislatura, Camera dei deputati, Doc. XVI n. 24-A, 2.

Ebbene, per concludere, *quid iuris* nel c.d. caso Renzi?

Alla luce della documentazione esaminata dal Senato, non si ritiene di avere qui sufficienti elementi per inquadrare il caso concreto. In altri termini, non risulta chiaro dalla documentazione esaminata dal Senato proprio la circostanza se gli atti di indagine (il sequestro del cellulare del sig. V.M. e l'acquisizione delle quattro e-mail) siano avvenuti «nei confronti» del sen. Renzi, nei termini appena precisati.

In caso affermativo, sarebbe dunque mancata l'autorizzazione *ex ante* del Senato *ex* art. 4 della legge n. 140 del 2003. In caso negativo, la fattispecie concreta non sarebbe riconducibile all'art. 6 della legge n. 140 del 2003, impedendolo il dato letterale. Tuttavia, si ripete, non si hanno qui elementi conoscitivi sufficienti per qualificare il caso concreto in un senso o nell'altro.

L'unico membro del Senato che nel corso del dibattito sembra aver colto questo profilo è stata la sen. Rossomando. Dopo aver richiesto un supplemento istruttorio (negato però dalla Giunta con un voto a maggioranza), la sen. Rossomando ha motivato il proprio voto di astensione sulla relazione della Giunta sul presupposto di una carenza di elementi conoscitivi proprio in ordine alla direzione degli atti di indagine. In particolare, nota la senatrice in sostanziale conformità con quanto si è andato dimostrando in questa sede, «è evidente che le operazioni di intercettazione hanno ad oggetto la captazione di contenuti nella loro dimensione dinamica [ma] per la corrispondenza occorre verificare come è avvenuta in concreto l'acquisizione di tali contenuti». Ad esempio, nel caso concreto, occorrerebbe comprendere «se essi sono stati versati integralmente su un supporto tecnico o invece sottoposti a chiave di ricerca»[43].

Valuterà ora la Corte costituzionale, in sede di giudizio sul conflitto di attribuzione tra poteri sollevato dal Senato, se gli elementi a sua disposizione sono sufficienti per decidere sul caso concreto. Ove così fosse ed ove la questione fosse ritenuta dalla Corte rilevante, sarebbe auspicabile un'auto-rimessione della Corte della questione di legittimità costituzionale dell'art. 6 della legge n. 140 del 2003, nei termini prospettati in questa sede.

[43] Cfr. XVIII legislatura, Senato della Repubblica, *Resoconto sommario n. 662*, Giunta delle elezioni e delle immunità parlamentari, 14 dicembre 2022, 17.

La disciplina delle piattaforme *online* fra giurisdizioni e legislatori nazionali e sovranazionali. Dai casi *Airbnb* al *Digital Services Package**

Maria Esmeralda Bucalo

Abstract

Partendo dalla definizione di *sharing economy,* il saggio analizza la giurisprudenza europea relativa alle società che rendono *online* servizi per l'informazione (le cosiddette piattaforme digitali). L'intervento giurisprudenziale a livello europeo si è rivelato fino ad oggi supplente della inesistenza di un quadro normativo unitario a fronte della eterogenea congerie di normative degli Stati membri, i quali si occupano del tema sotto diversi aspetti. A fronte delle molteplici questioni pregiudiziali sollevate dai giudici nazionali, l'affastellarsi delle pronunce della Corte di giustizia, volte a risolvere casi concreti nelle loro specificità, contribuisce oggi a renderne meno saldo il ruolo nomofilattico, evidenziando la natura eminentemente casistica delle regole attualmente vigenti. A risolvere questi problemi è stato recentemente approvato il *Digital Service Package,* che costituisce la risposta normativa dell'Unione Europea alla necessità di regolamentare in modo uniforme lo spazio digitale, definendo da un lato le misure per proteggere gli utenti *online* e sostenendo dall'altro le innovazioni tecnologiche.

Starting from the definition of sharing economy, the essay analyzes the European jurisprudence relating to companies that provide online information services (digital platforms). The jurisprudential intervention at the European level has proved up to now to replace the inexistence of a unitary regulatory framework in the face of the heterogeneous jumble of regulations of the Member States, which deal with the issue under various aspects. Faced with the multiple preliminary questions raised by national judges, the jumble of rulings by the Court of Justice, aimed at solving concrete cases in their specificity, today contributes to making their nomophylactic role less solid, highlighting the eminently casuistic nature of the rules currently in force. To solve these problems, the Digital Service Package was recently approved, which constitutes the regulatory response of the European Union to the need to regulate the digital

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

space in a uniform way, defining on the one hand the measures to protect online users and on the other supporting the technologic innovations.

Sommario

1. Una premessa necessaria: la *sharing economy* ed economia delle piattaforme - 2. Il *leading case*: la "versione francese" del caso *Airbnb* - 3. La "versione italiana" del caso *Airbnb Ireland:* la questione pregiudiziale sollevata dal Consiglio di Stato – 4. La "versione belga" del caso *Airbnb*: la questione pregiudiziale sollevata dalla *Cour constitutionnelle* belga e decisione della Corte di giustizia – 5. La decisione della Corte di giustizia sulla questione pregiudiziale sollevata dal Consiglio di Stato: la "modulazione" della nozione di regola tecnica al fine dell'interesse (generale) fiscale - 6. Questioni pregiudiziali ancora pendenti (italiane e non solo) - 7. La via della regolazione unitaria delle piattaforme: *Digital Services Package*

Keywords

sharing economy - piattaforme *online* – legislazione nazionale – questioni pregiudiziali – normativa europea

1. Una premessa necessaria: la *sharing economy* ed economia delle piattaforme

Le riflessioni oggetto del presente lavoro originano dallo studio, oramai protrattosi da qualche anno, delle pronunce della giurisprudenza eurounionale in tema di servizi resi dagli intermediari *online*. Appare però necessario, in via preliminare qualche cenno sulla *sharing economy,* che è il modello economico nel quale si innesta l'attività di queste società, e sui relativi problemi definitori[1].

In generale può dirsi che *sharing economy* si basa sulla idea per la quale ciascuno ha a disposizione tutto ciò di cui ha bisogno e dunque la condivisione di beni e servizi propri con altri individui consente di sopperire a tutti i bisogni della vita individuale e sociale, ammortizzando i costi.

Tale modello economico, che ha evidenti refluenze sociali, si basa dunque più che sulla proprietà o sul possesso esclusivo di beni e servizi, sulla possibilità di accedere al loro uso, il quale viene condiviso per mezzo delle nuove tecnologie.

Il problema definitorio però resta rilevante se solo si pone mente al fatto che questo nuovo modello di mercato, divenuto un fenomeno globale, ha determinato notevoli mutamenti di natura sia economica sia sociale (si pensi per esempio a quanto, in pochi anni si siano modificate le modalità di produzione, consumo e scambio di beni e servizi).

Tali mutamenti, agevolati dal progresso tecnologico e dal *World Wide Web* in grado di collegare persone che si trovano nei più disparati angoli del pianeta, oltre che com-

[1] I. Scott - E. Brown, *Redefining and regulating the new sharing economy,* in *University of Pennsylvania Journal of Business Law,* 16 (9), 2017, 559-560, parlano infatti di *shifting definition.*

portare una notevole riduzione dei costi e la accelerazione delle transazioni, hanno fatto emergere un nuovo e diverso sistema economico fondato sullo scambio e la condivisione di beni e servizi. In altre parole, l'economia lineare espressa dal mercato tradizionale, nel quale domanda e offerta si incontravano grazie anche alla netta distinzione dei ruoli fra venditore e consumatore, è oggi superata da una economia di tipo circolare, che determina il venir meno della distinzione citata[2] e della necessità di consumare solo beni e servizi nuovi, privilegiando il riuso.

Per comprendere l'estensione del fenomeno, pur mantenendoci in ambito lessicale, basta rendersi conto di quanto sia precocemente invecchiata l'originaria definizione di *sharing economy*, dovuta alla dottrina anglosassone, che la intendeva come «*An economy built on distributed networks of connected individuals and communities versus centralized institutions, transforming how we can produce, consume, finance, and learn*»[3].

Oggi, infatti, accade sovente che con la stessa locuzione si faccia riferimento a fenomeni del tutto diversi usati in modo intercambiabile ("*peer economy*", "*collaborative economy*", "*on-demand economy*", *"collaborative consumption"*) o anche a modelli efficienti di incontro fra domanda e offerta, che però di condiviso non hanno nulla[4].

Il problema definitorio dunque appare, con ogni probabilità conseguenza della confusione fra *sharing economy* e *e-commerce*. Se infatti quest'ultimo ha contribuito alla estensione progressiva del mercato dovuta all'espandersi della tecnologia informatica, il *quid pluris* della prima è determinato invece in primo luogo dall'aver consentito «la creazione di un'offerta e di una domanda di beni che prima non erano in circolazione, o che erano oggetto di scambio solo in misura molto limitata»[5], in secondo luogo dalla modalità attraverso la quale questo commercio ha luogo, cioè mettendo in contatto le persone coinvolte nello scambio di beni e servizi, le quali scambiano dati e informazioni per via digitale[6]. Tutto ciò comporta evidentemente un notevole

---

[2] Per definire questa nuova categoria di soggetti che assumono la veste di produttori o di consumatori a seconda delle circostanze i sociologi usano appunto il termine *"prosumer"*. Il termine fu usato per la prima volta da A. Toffler, *La terza ondata*, Milano, 1987. Si veda anche B. Lang - R.J. Kemper - G. Northey, *Prosumers in times of crisis: definition, archetypes and implications*, in *Journal of Service Management*, *ahead-of-print*, 1° gennaio 2020, i quali identificano il *prosumer* in un «individuo che consuma e produce valore per il consumo sia proprio che altrui, e può ricevere incentivi impliciti o espliciti dalle organizzazioni coinvolte nello scambio».

[3] R. Botsman, *The Sharing Economy Lacks a Shared Definition,* in *Fast Company*, 21 novembre 2013. Sebbene, già allora, le difficoltà definitorie del fenomeno fossero manifeste, tanto che J. Orsi, *Practicing Law in the Sharing Economy: Helping People Build Cooperatives, Social Enterprise, and Local Sustainable Economies,* Chicago, 2012, 2 affermava che «*Although it is hard to encapsulate the qualities of this new economy, it generally facilitates community ownership, localized production, sharing, cooperation, [and] small-scale enterprise*».

[4] R. Botsman, *Defining The Sharing Economy: What Is Collaborative Consumption–And What Isn't?,* in *Fast Company*, 27 maggio 2015, la quale sottolinea l'errore commune di inserire nella categoria di *"sharing economy"* piattaforme ad accesso mobile (con semplice *app* da telefono), che invece sono la versione moderna della consegna porta a porta, perché *«They're thrown under the same umbrella as part of the sea change in consumer behavior that uses the smartphone as a remote control to efficiently access things in the real world»*.

[5] C. Nicolini, *The sharing economy is growing as a form of trade in different spheres. What factors have contributed to its growth and what part can it play in development?,* in *conexionintal.iadb.org*.

[6] Secondo R. Belk, *You are what you can access: sharing: and collaborative consumption online,* in *Journal of Business Research,* 67(8), 2014, 1595: «*There are two commonalities in these sharing and collaborative consumption practices: 1) their use of temporary access non-ownership models of utilizing consumer goods and services and 2) their*

risparmio di risorse ed un nuovo modo di fare commercio più economico, sostenibile ed efficiente.

Così anche il modo attraverso il quale i produttori di beni e servizi e i consumatori si approcciano a questo nuovo mercato è diverso da quanto non accada nel "mercato tradizionale". Uno degli ultimi esempi cui si può fare riferimento è *Vinted*, una piattaforma *peer-to-peer* di economia della condivisione recentemente approdata in Italia, che consente agli utenti registrati di barattare o vendere e acquistare, fissando autonomamente il relativo corrispettivo in denaro, determinate categorie di beni di seconda mano in loro possesso. Si crea così una *virtual community* nella quale, attraverso la chat, ci si "incontra", ci si "segue", ci si scambiano opinioni; attraverso la consultazione dei *feedback* rilasciati alla fine di ogni transazione il futuro consumatore o il futuro veditore possono venire a conoscenza della attendibilità di un altro utente, al quale decideranno o meno di approcciarsi; attraverso una semplice ricerca si trova il bene di cui si ha bisogno e si può scegliere quale acquistare a seconda delle sue condizioni e/o del prezzo[7].

La piattaforma inoltre non possiede i beni che tratta, ma funge da mero "connettore" tra utenti e fornitori, non essendo neppure intermediario di pagamenti posto che l'utente può scegliere se pagare con la propria carta di credito o attraverso il credito che ha salvato su proprio *account* con la vendita di suoi beni, laddove non abbia chiesto l'accredito con bonifico direttamente sul suo conto corrente[8].

Dalla struttura appena accennata può dirsi, utilizzando le parole di Van Dijk, Thomas Poell e De Waal[9], che *Vinted* come *Airbnb* siano una *platform society,* locuzione che enfatizza l'inestricabile relazione tra le piattaforme *online* e le strutture sociali che esse creano. Esse, infatti, non posso più essere considerate dei meri fenomeni economici avulsi dalla società, piuttosto stanno contribuendo a modificare la società stessa[10], infiltrandosi in essa, «convergendo con le istituzioni tradizionali, […] forzando i governi ad adeguare le loro strutture legali e democratiche»[11].

---

reliance on the Internet».

[7] Per realizzare gli scambi la piattaforma ha stipulato degli accordi con i maggiori operatori logistici, che si occupano del trasporto dei pacchi a spese dell'acquirente, il quale può anche scegliere a quale operatore affidarsi, lasciando al venditore solo il compito di portare il bene confezionato a sua cura presso il punto di raccolta che preferisce.

[8] Si legge infatti sulla pagina della piattaforma dedicata alle "informazioni e buone prassi" che «*Vinted* è un servizio di hosting online che consente agli utenti di scambiare, vendere e acquistare oggetti sulla sua piattaforma (il "Sito").

Vinted facilita queste transazioni e permette agli utenti di comunicare tramite messaggi privati o messaggi sul forum. […] *Vinted* non vende, acquista o scambia articoli e non è parte di alcuna transazione tra gli utenti».

Si noti fin d'ora che la piattaforma non è intermediario di pagamenti, ciò oltre a qualificarne la natura, è anche determinante ai fini fiscali, tenendo conto che la questione di pregiudizialità che fra poco si tratterà sorge proprio dall'essere *Airbnb* anche intermediario di pagamenti, attraverso la collegata società *Airbnb Payment.*

[9] J. Van Dijck - T. Poell - M. De Waal, *The Platform Society: Public Values in a Connective World*, New York, 2018.

[10] Concorda G. Smorto, *Sharing economy as a means tu Urbano Commoning,* in *Comparative law Review,* 7(1), 2016, 2-3.

[11] J. Van Dijck, Nuovi mondi online, in Il Foglio, 25 febbraio 2019, sottolinea che la locuzione indica anche che è vero che «le piattaforme potenziano i benefici personali e il guadagno economico di ciascuno, ma nel contempo simultaneamente esercitano pressione sui mezzi collettivi e sui servizi

Ciò inevitabilmente crea conflitti fra questi nuovi attori e le istituzioni pubbliche tradizionali di ogni livello[12]. La molteplicità degli strumenti, delle piattaforme e delle *app* infatti ha come diretta conseguenza, a livello giuridico, la molteplicità di regole che questi operatori autonomamente si danno, obbligando all'osservanza gli utenti, e che creano una confusione giuridico-normativa difficile da seguire e da ridurre ad unità.
Vieppiù la autoregolazione, sulla base delle quali le piattaforme operano, non è avulsa dai principi generali dettati dagli ecosistemi giuridici nei quali esse sono venute ad esistenza, ma la loro estensione a livello globale comporta il più delle volte che essa confligga con le regole giuridiche che invece insistono presso le istituzioni nazionali e/o locali. Ne è un esempio il caso *Airbnb*, che progressivamente sta assumendo di estensione europea, coinvolgendo sotto diversi aspetti ordinamenti di diversi Stati membri.
Alla problematicità determinata dall'estrema frammentazione del quadro normativo si somma quella determinata dalla sopracitata commistione fra produttori e consumatori, professionisti e non professionisti, che rende non più attuali e adeguate le regole tradizionali del mercato e comporta anch'essa necessariamente delle nuove sfide per i legislatori di tutti i livelli di governo, i quali si trovano oggi a dover dare delle nuove regole ad un mercato in continua evoluzione[13].
In questo l'assenza di un unico sostrato giuridico e normativo che costituisca il fondamento sul quale innestare le regole di derivazione privata poste dalle piatteforme, determina il sorgere delle controversie delle quali si tratterà nell'immediato prosieguo.
Ne consegue in supplenza l'attivismo degli organi di controllo, non solo giurisdizionali[14], i quali sono chiamati, a dirimere caso per caso le questioni che via via vengono loro sottoposte. Poiché la pluralità e, sovente, la diversità delle decisioni non aiuta la necessaria univocità della regolazione, lo studio vuole soffermarsi sul ruolo di giudice della nomofilachia, che, in questo campo, sta progressivamente assumendo la Corte di giustizia dell'Unione Europea e esaminare infine il *Digital Services Package,* recentemen-

pubblici, […] forzando i governi a ad adeguare le loro strutture legali e democratiche».

[12] L'Avvocato Generale Szpunar nelle conclusioni a C-83/21 del 7 luglio 2022, §§ 2-4 (delle quali più ampiamente si tratterà nel § 5), ha osservato che oltre agli indiscussi vantaggi determinati dal loro sviluppo (estensione del mercato, del numero degli utenti, dei servizi offerti, aumento della domanda e dell'offerta), le piattaforme «hanno contribuito ad aggravare molti problemi sociali, politici, amministrativi e giuridici associati allo sviluppo massiccio dei servizi in discussione».

[13] G. Smorto, *Critical Assessment of European Agenda for the Collaborative Economy, on behalf of European Parliament. In-Depth Analysis for the IMCO Committee*, Bruxelles, 2017, 12 il quale afferma che *«Facing the rise of peer-to-peer economy, the bipartisan appeal is to "level the playing field"- review the regulatory framework by establishing fair rules for each category and leave the market forces ruling on winners and losers, in accordance with the well-known adagio "the State should not be picking winners". But, if this premise can be easily endorsed, the problematic part concerns the actual identification of such rules».*

[14] Che le piattaforme e le loro attività siano soggette al controllo attento non solo della giurisdizione ma anche di altri organi come *in primis* le Autorità Indipendenti è stato recentemente messo in luce dalla multa irrogata nei confronti di *Vinted* da AGCM per pratiche pubblicitarie scorrette. Si legge nel comunicato della Autorità del 10 novembre 2022 (disponibile in *agcm.it*) che a finire sotto la lente erano stati «in particolare i costi delle operazioni di compravendita e il prezzo effettivo dei prodotti commercializzati *online.* […] La società ha però omesso di indicare in modo chiaro e trasparente, fin dal momento dell'iniziale "aggancio pubblicitario", l'esistenza a carico dei consumatori di costi ulteriori rispetto al prezzo di acquisto del prodotto, legati all'applicazione della commissione per la "Protezione Acquisti" e alle spese di spedizione». Avverso il provvedimento (disponibile in *agcm.it*), la piattaforma ritiene di dover promuovere ricorso, non condividendone le motivazioni.

te approvato, costituito dal *Digital Market Act* e dal *Digital Service Act,* che costituirà le fondamenta di una disciplina condivisa a livello eurounionale.

2. Il *leading case*: la "versione francese" del caso *Airbnb*

Come appena più sopra si è avuto modo di affermare, l'inesistenza di un quadro normativo unitario che disciplini il fenomeno ha determinato, come sovente accade in casi di vuoto normativo, l'intervento in supplenza degli organi giurisdizionali, prima nazionali e poi sovranazionali, volto però a risolvere casi concreti nelle loro specificità e, dunque, per sua natura carente di univocità.

Il *leading case* della Corte di giustizia in materia di piattaforme di *peer-to-peer accommodation* è costituito dalla pronuncia *Airbnb Ireland* (C-390/18) del 19 dicembre 2019, la quale può essere considerata un ulteriore tassello giurisprudenziale del complicato regime giuridico degli intermediari digitali di beni e servizi a livello europeo[15].

Il rinvio pregiudiziale dal quale è scaturita la decisione citata nasce da una denuncia con costituzione di parte civile presentata dalla *AHTOP (Association pour un hébergement et un tourisme professionnels*) nel gennaio 2017, la quale lamentava l'abusività dell'esercizio da parte di *Airbnb* di un'attività di mediazione e gestione di immobili ed esercizi commerciali, in quanto senza licenza per l'esercizio della professione richiesta nell'ordinamento francese dall'art. 3 della legge n. 70-9 del 1970 (cd. *loi Hoguet*), il che comportava l'integrazione di fattispecie di diritto penale.

Davanti alla difesa di *Airbnb,* la quale sosteneva che la sua attività dovesse ascriversi a quella dei servizi di intermediazione tramite piattaforma digitale e che dunque alla fattispecie andasse applicata la direttiva 2000/31/CE, che garantisce la libertà di prestazione di servizi, il *juge d'instruction* del *Tribunal de Grande Instance de Paris* decideva di sospendere il giudizio, rinviando alla Corte di giustizia, alla quale chiedeva in primo luogo «se le prestazioni fornite in Francia dalla (…) *Airbnb Ireland* mediante una piattaforma elettronica gestita dall'Irlanda godessero della libertà di prestazione di servizi prevista dall'articolo 3 della direttiva 2000/31(…)» e in seguito «se le norme restrittive relative all'esercizio della professione di agente immobiliare in Francia, previste dalla [legge *Hoguet*], siano opponibili alla (…) *Airbnb Ireland*».

Per comprendere la portata delle questioni sollevate dal giudice del rinvio è necessario ricordare che la citata direttiva all'art. 2 definisce "servizio" qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

Il successivo art. 3, par. 2, della medesima direttiva dispone poi che «Gli Stati membri non possono, per motivi che rientrano nell'ambito regolamentato, limitare la libera circolazione dei servizi delle società dell'informazione provenienti da un altro Stato membro», indicando poi ai successivi par. 4 e 5 i limiti entro i quali «gli Stati membri possano adottare provvedimenti in deroga al paragrafo 2».

Si tratta di limiti di natura sostanziale e formale. Quanto ai primi, tali provvedimenti

[15] Più in generale in tema di piattaforme le prime pronunce della Corte di giustizia sono le notissime CGUE, C-434/15, *Uber Spain* (2016) e CGUE, C-320/16, *Uber France* (2018).

in deroga possano essere adottati, nel rispetto del principio di proporzionalità, solo a tutela dell' "ordine pubblico, in particolare per l'opera di prevenzione, investigazione, individuazione e perseguimento in materie penali, quali la tutela dei minori e la lotta contro l'incitamento all'odio razziale, sessuale, religioso o etnico, nonché violazioni della dignità umana della persona; della sanità pubblica; della pubblica sicurezza, compresa la salvaguardia della sicurezza, e della difesa nazionale e dei consumatori, ivi compresi gli investitori".

Quanto ai secondi, lo Stato dovrà preventivamente notificare i summenzionati provvedimenti in deroga alla Commissione, alla quale spetta il sindacato sulla effettiva giustificabilità del provvedimento adottato alla luce del diritto europeo.

Le limitazioni imposte dalla *loi Hoguet* (entrata in vigore precedentemente alla direttiva CE 2000/31) all'esercizio della attività di intermediazione immobiliare, ponevano dunque degli evidenti problemi di compatibilità con il citato quadro normativo europeo, quanto meno quanto alla definizione dei servizi prestati da *AirBnB*: se immobiliari e dunque ascrivibili alla disciplina francese o se resi da società di informazione e conseguentemente da attrarre sotto l'egida della disciplina eurounionale.

Nel caso che qui ci occupa la Corte sosteneva che il servizio reso da *Airbnb* integrasse tutte le condizioni richieste per essere qualificato servizio reso da società di informazione, procedendo conseguentemente al cd. *Uber test,* valutare cioè se il servizio di mediazione svolto dalla società non costituisca anche «parte integrante di un servizio globale, il cui elemento principale è un servizio al quale va riconosciuta una diversa qualificazione giuridica»[16]. Tale valutazione avviene sulla scorta di due criteri fondamentali, la presenza dei quali determina la non ascrivibilità della società fra quelle che erogano servizi di informazione: il grado d'influenza della piattaforma sull'erogazione del servizio sottostante e l'indispensabilità della piattaforma per il servizio intermediato[17].

Per la Corte di Lussemburgo la posizione e la natura di *Airbnb* è ben diversa da quella di *Uber,* perché la prima, pur determinando termini e condizioni di servizio per quanto concerne le politiche di cancellazione, non gestisce gli aspetti della fissazione delle tariffe e della remunerazione di coloro che mettono a disposizione le proprietà e dunque il servizio da essa fornito è ben distinto dall'offerta immobiliare, poiché la piattaforma mirerebbe semplicemente a creare un elenco strutturato di alloggi disponibili sulla piattaforma a vantaggio di locatori e locatari[18].

---

[16] Sulla scorta della sua precedente giurisprudenza sui cd. casi *Uber*. CGUE, C-434/15, *Uber Spain,* cit. e C-320/16, *Uber France,* cit.

[17] CGUE, C-434/15, *Uber Spain,* cit., § 40. È bene ricordare, anche per comprendere la differenza con la decisine in commento, che nel caso di *Uber* la Corte aveva concluso che entrambi i citati criteri risultavano soddisfatti e, dunque, aveva valutato l'intermediazione svolta come parte integrante di un servizio complessivo il cui elemento principale era il trasporto (CGUE, C-434/15, *Uber Spain* cit., § 38). Secondo parte della dottrina ciò salvaguardava lo spazio istituzionale riservato alla regolazione pubblica dei trasporti ed in particolare a quella degli Stati membri. In tal senso M. Midiri, *Nuove tecnologie e regolazione. Il "caso Uber",* in *Riv. trim. dir. pubb.*, 3, 2018, 1026-1028.

[18] In tema si vedano le riflessioni di C. Bush, *The Sharing Economy at the CJEU: does Airbnb pass the 'Uber test'? Some observations on the pending case C-390/18 – Airbnb Ireland,* in *Journal of European Consumer and Market Law,* 4, 2018, 173., che avevano anticipato la decisione della Corte di giustizia, pur mostrandone alcune criticità. Fra queste il non aver considerato *Airbnb* un *market-maker,* che ha oggettivamente

È bene fin d'ora avere cura di notare che nella sentenza cui qui si accenna è presente anche un interessante argomento, utile anche ai fini dell'analisi delle più recenti pronunce su *Airbnb*[19], che serve alla Corte a corroborare la identificata natura della piattaforma. Secondo i Giudici di Lussemburgo, infatti, i servizi aggiuntivi e accessori resi dalla piattaforma (come il servizio di fotografia, di comparazione prezzi, ma anche quello di riscossione) «non possono rimettere in discussione la natura distinta del servizio di mediazione fornito da questa società e pertanto la sua qualificazione come 'servizio della società dell'informazione', a meno di non voler modificare sostanzialmente le specifiche caratteristiche di questo servizio»[20].

Quanto alla legge francese più restrittiva, che impone agli intermediari immobiliari di agire solo se dotati di licenza professionale, la Corte ne rilevava la incompatibilità rispetto all'art. 3, par. 4, della direttiva 2000/31/CE, perché esso impone un obbligo preciso e categorico allo Stato di notificarla preliminarmente alla Commissione e allo Stato fornitore del servizio, al fine di consentire alla prima di svolgere il suo sindacato sulla legittimità del provvedimento ed eventualmente chiedere allo Stato membro di astenersi dalla adozione.

Conseguentemente poiché la violazione francese dell'obbligo di notifica si inserisce nella procedura prescritta per la limitazione della prestazione dei servizi delle società di informazione, rendendola insanabilmente viziata[21], *Airbnb* non poteva essere perseguita penalmente ai sensi di disposizioni di legge ritenute maggiormente restrittive rispetto alla direttiva 2000/31/CE.

La "sentenza pilota" ora brevemente analizzata ci informa intanto della attenzione rivolta dalla Corte di giustizia al tema delle società di informazione e, oltre a coinvolgere i profili relativi alla prestazione di servizi per via digitale, alla loro consistente rilevanza economica e alla difficile distinzione fra servizi delle società di informazione e servizi tradizionali, prova a definire i confini della normazione nazionale, sovente caratterizzata da regole restrittive sull'accesso ai servizi, non conformi ai principi europei della libera circolazione dei servizi.

In secondo luogo, i giudici di Lussemburgo, anche in ragione della pluralità delle discipline nazionali in materia, fondano un nuovo *case law* sulla scorta di quegli stessi criteri indice individuati nella pronuncia *Uber,* decidendo di svolgere di una valutazione ap-

esteso il mercato degli alloggi residenziali, creando una nuova offerta di affitti a breve termine che non esisterebbe altrimenti e secondo G. Smorto, *Armi spuntate alle autorità locali contro le piattaforme,* in *ilSole24ore.com,* 21 dicembre 2019, non aver tenuto conto dell'influenza esercitata sul servizio reso dalla società, attraverso il complesso sistema di incentivi e strategie, che governano i *marketplace* delle piattaforme.

[19] Ci si riferisce a CGUE, C-674/20, *Airbnb Ireland* (2022) e a CGUE, C-83/21, *Airbnb Ireland* (2022).

[20] CGUE, C-390/18, *Airbnb Ireland* (2019), § 64, che in questo punto riprende il punto 46 delle conclusioni dell'Avvocato generale, il quale riteneva che siffatte prestazioni accessorie a valore aggiunto, fornite da una piattaforma elettronica ai propri clienti al fine, segnatamente, di distinguersi dai propri concorrenti, possano condurre, in mancanza di elementi aggiuntivi, a modificare la natura e pertanto la qualificazione giuridica dell'attività di quest'ultima

[21] F. Monceri, *Il caso Airbnb. Autonoma rilevanza dell'omessa notifica delle norme restrittive dei servizi di informazione e questioni ancora aperte,* in *DPCE online,* 1, 2020, 952. Sulla procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione dettata dalla direttiva (UE) 1535/2015 si veda A. Iannuzzi, *Il diritto capovolto. Regole a contenuto tecnico scientifico e Costituzione,* Napoli, 2018, 99 ss

profondita dei fatti e delle attività e riservandosi di analizzare piattaforma per piattaforma, società per società, se possa essere applicata la disciplina dell'Unione sui servizi delle società di informazione e dunque la tutela rafforzata assicurata dalla riconosciuta libertà di circolazione dei servizi[22].

3. La "versione italiana" del caso *Airbnb Ireland*: la questione pregiudiziale sollevata dal Consiglio di Stato

La molteplicità degli aspetti giuridici coinvolti dal tema oggetto di questo studio e la disomogeneità delle soluzioni apprestate dalle discipline degli Stati membri è palesato da quella che potremmo chiamare la versione italiana del caso *Airbnb Ireland*.
In via preliminare però è importante tenere in considerazione due aspetti che danno il La alla riflessione che ci sia appresta a svolgere. Il primo è relativo alla identificazione della società irlandese in "società che svolge servizi dell'informazione" da parte della giurisprudenza eurounionale. Tale riconoscimento le attribuisce un importante, atteso che la esonera da tutti quei vincoli, che le discipline nazionali possono legittimamente imporre a quelle società che invece di tale riconoscimento non godono[23].
Il secondo luogo non si può non tenere a mente che il tema comporta necessariamente delle sovrapposizioni fra i servizi resi dalle piattaforme e quelli resi dalle "società tradizionali" nei diversi settori del mercato coinvolti, con le conseguenziali difficoltà dei Legislatori nazionali, laddove decidano di disciplinare una materia, come quella che ci occupa, soggetta peraltro alla primazia del diritto dell'Unione.
L'attività di *Airbnb* è la manifestazione in concreto di quanto appena rappresentato: essa evidentemente incide su molteplici aeree disciplinari, dalla tutela della *privacy* e alla protezione dei dati personali, dalla pubblica sicurezza e alle norme tributarie relative al pagamento delle tasse sugli affitti e di soggiorno.
Il giudizio avanti al Consiglio di Stato, dal quale la questione di pregiudizialità è stata sollevata, aveva ad oggetto la richiesta di annullamento della sentenza del T.A.R. Lazio – Roma n. 2207 del 18 febbraio 2019, che aveva rigettato il ricorso proposto da *Airbnb Ireland* e *Airbnb Payment UK* contro l'Agenzia delle Entrate per l'annullamento del provvedimento del direttore della Agenzia delle Entrate di attuazione delle disposizioni di cui all'art. 4, c. 4-5 *bis,* del decreto legge n. 50 del 2017, convertito in legge n. 96 del 2017 (cd. Legge *Airbnb*).
A riprova di quanto siano rilevanti dal punto di vista economico i settori del mercato amministrati dalle piattaforme informatiche ed, in questo caso, quello degli affitti di breve periodo, l'art. 4, c. 4-6, del d.l. 24 aprile 2017, n. 50, convertito in l., 21 giugno 2017, n. 96 (cd. legge *Airbnb*) ha imposto una serie di obblighi agli intermediari del settore sia tradizionali sia *online*.

[22] In senso analogo P. Van Cleynenbreugel, *Le droit de l'Union européenne face à l'économie collaborative,* in *Revue trimestrelle de droit européenne,* 4, 2017, 705 e 721 e A. Canepa, *Il dilemma della regolazione delle piattaforme,* in L. Ammaniti - R. Cafari Panico (a cura di), *I servizi pubblici: vecchi problemi e nuove regole,* Torino, 2018, 153.

[23] Tranne le limitate eccezioni che a breve si avrà modo di esaminare.

Specificatamente, oltre alla trasmissione dei dati relativi ai contratti conclusi loro tramite (c. 4), il c. 5 ha disposto che «i soggetti residenti nel territorio dello Stato che esercitano attività di intermediazione immobiliare, nonché quelli che gestiscono portali telematici […], qualora incassino i canoni o i corrispettivi relativi ai contratti […], ovvero qualora intervengano nel pagamento dei predetti canoni o corrispettivi, operano, in qualità di sostituti d'imposta, una ritenuta del 21 per cento sull'ammontare dei canoni e corrispettivi all'atto del pagamento al beneficiario […]».
Inoltre, per i soggetti non residenti privi di stabile organizzazione in Italia il c. 5-bis del medesimo articolo, introdotto con la legge di conversione, ha disposto che «ai fini dell'adempimento degli obblighi derivanti dal presente articolo, in qualità di responsabili d'imposta, nominano un rappresentante fiscale […]», rinviando (c. 6) ad un provvedimento del direttore dell'Agenzia delle entrate che disponesse le relative norme di attuazione[24].
Le contestazioni mosse da *Airbnb* al provvedimento impugnato e poste a fondamento dei ricorsi avanti i giudici amministrativi di primo e di secondo grado muovevano intanto dalla constatazione della necessaria disapplicazione della disciplina di cui all'art. 4 del d.l. 50/2017, in quanto in contrasto con la disciplina di cui alla direttiva (UE) 1535/2015, che impone il citato obbligo di comunicazione delle regole tecniche, nonché con disciplina di cui alla direttiva 2000/31/CE volta a garantire l'effettività della concorrenza attraverso il divieto di normative nazionali che abbiano l'effetto di impedirla o ostacolino lo sviluppo di modelli innovativi nell'ambito della *sharing economy*.
Quanto a quest'ultimo aspetto, la normativa italiana avrebbe istituito una disparità di trattamento fra gli operatori soggetti alla ritenuta in quanto intervenienti nel pagamento della locazione e quelli che, pur svolgendo un servizio analogo nell'ambito della stessa intermediazione immobiliare, a tale obbligo non sono soggetti perché non intervengono nel pagamento. Ciò potrebbe indurre i proprietari degli immoli a migrare verso questi ultimi, creando un rilevante danno economico all'intero modello di *business* di *Airbnb*[25].

---

[24] Provvedimento appunto impugnato dalla società irlandese.

[25] Nel dichiarare non fondati tutti i motivi di ricorso e conseguentemente nel decidere non solo di non disapplicare, ma anche di non sollevare la questione pregiudiziale la sentenza del T.A.R. Lazio – Roma, sez. II *ter*, 18 febbraio 2017, n. 2207, motiva sulla scorta di alcune considerazioni, alcune delle quali verranno riprese da CGUE, C-674/20, *Airbnb UC c. Region de Bruxelles-Capitale* (vedi *infra* § 4). Il giudice di prima istanza muoveva intanto dal non ritenere applicabile alla fattispecie la disciplina di cui alla direttiva (UE) 2015/1535 e dunque l'obbligo di comunicazione delle regole tecniche. Essa infatti si riferisce ai servizi resi da società di informazione, mentre le previsioni contestate sarebbero riferite non al servizio di intermediazione in sé, ma al servizio accessorio esercitato implicante il pagamento (p.to 7.1).
Non considerava fondata neppure la contestazione relativa alla violazione della direttiva 2000/31/CE e del principio della concorrenza e libera prestazione dei servizi, perché «la normativa contestata impone identici obblighi sia a carico dei soggetti intermediari che hanno residenza in Italia sia di quelli non residenti né stabiliti in Italia che gestiscono portali telematici mettendo in contatto persone in ricerca di un immobile con persone che dispongono di unità immobiliari da locare (art. 4, c. 5, d.l. 50/2017), qualora essi incassino i canoni o i corrispettivi relativi ai contratti di cui ai commi 1 e 3, ovvero qualora intervengano nel pagamento dei predetti canoni o corrispettivi» (p.to 7.2) e perché l'obbligo di individuazione da parte dei soggetti non residenti in Italia (ai sensi del c. 5 *bis* dell'art. 4) di un rappresentante fiscale non era da ritenersi un ulteriore onere che disincentivasse l'accesso ai servizi resi da *Airbnb,* bensì una misura proporzionata a garantire la riscossione delle imposte sulle locazioni

Avverso la pronuncia di primo grado che rigettava il ricorso la società irlandese proponeva appello al Consiglio di Stato, il quale sollevava la questione pregiudiziale avanti la Corte di giustizia.

La questione, ancora in corso di definizione, ha subito un *iter* invero travagliato. Infatti, essendo stata inaspettatamente dichiarata manifestamente irricevibile la prima ordinanza di rinvio n. 6219 del 18 settembre 2019[26], perché non soddisfava i requisiti richiesti dall'art. 94 del Regolamento di Procedura avanti la Corte di giustizia[27], la questione è stata successivamente riproposta con ordinanza n. 777 del 26 gennaio 2021.

Dopo aver riportato per intero le disposizioni dell'ordinamento italiano, della cui interpretazione conforme al diritto dell'Unione Europea si dubita, e le tesi delle parti in modo esteso, senza peraltro tralasciare le precisazioni metodologiche finalizzate ad evitare una nuova dichiarazione di irricevibilità, col nuovo rinvio pregiudiziale il supremo collegio amministrativo solleva tre questioni pregiudiziali, delle quali una, in specie la terza, di natura meramente processuale.

Quanto alla prima questione la Corte espressamente richiede che il Giudice sovranazionale si esprima sulla corretta «esegesi delle espressioni "regola tecnica" dei servizi della società dell'informazione e "regola relativa ai servizi" della società dell'informazione, di cui alla direttiva 2015/1535/UE e in particolare […] se tali espressioni debbano interpretarsi come comprensive anche di misure di carattere
tributario non direttamente volte a regolamentare lo specifico servizio della società

brevi a fronte della inidoneità di altre misure (p.to 7).

Inoltre, non potevano essere equiparate, secondo il Tribunale, la posizione dell'intermediario che intervenga nel pagamento delle locazioni (come appunto *Airbnb*) e il locatore che invece non si vuole servire di tale servizio accessorio alla intermediazione mobiliare, perché «l'obbligo della ritenuta alla fonte e il conseguente versamento della cedolare secca sui proventi delle locazioni brevi non poteva che essere posto a carico unicamente di quei soggetti i quali si trovano ad avere la disponibilità di dette somme per la circostanza che essi, liberamente, hanno deciso di intervenire nei pagamenti» (p.to 7.3).

Quanto, infine, ai possibili rischi di distorsione della concorrenza, il T.A.R. non li considera sussistenti, poiché la scelta legislativa aveva come obiettivo la lotta contro l'evasione fiscale nel settore delle locazioni e che, dunque, poneva misure volte a tutelare l'interesse generale (p.to 7.4).

[26] CGUE, C-723/19, *Airbnb Ireland e Airbnb Payments c. Agenzia delle Entrate* (2020).

[27] Il quale dispone «Oltre al testo delle questioni sottoposte alla Corte in via pregiudiziale, la domanda di pronuncia pregiudiziale contiene:

a) un'illustrazione sommaria dell'oggetto della controversia nonché dei fatti rilevanti, quali accertati dal giudice del rinvio o, quanto meno, un'illustrazione delle circostanze di fatto sulle quali si basano le questioni;

b) il contenuto delle norme nazionali applicabili alla fattispecie e, se del caso, la giurisprudenza nazionale in materia;

c) l'illustrazione dei motivi che hanno indotto il giudice del rinvio a interrogarsi sull'interpretazione o sulla validità di determinate disposizioni del diritto dell'Unione, nonché il collegamento che esso stabilisce tra dette disposizioni e la normativa nazionale applicabile alla causa principale».

Secondo la Corte di giustizia l'ordinanza del Consiglio di Stato «menziona solamente una disposizione di diritto nazionale, segnatamente l'articolo 4, commi 4, 5 e 5-bis del decreto legge del 24 aprile 2017, n. 50, convertito dalla legge del 21 giugno 2017, n. 96, senza fornirne – contrariamente ai requisiti stabiliti all'articolo 94, lettera b), del regolamento di procedura – né il contenuto esatto né i riferimenti e i titoli precisi, e senza indicare gli elementi necessari alla comprensione dell'intera normativa nazionale rilevante che può trovare applicazione nel procedimento principale», potendosi desumere gli obblighi di qualunque natura posti a carico di operatori come l'*Airbnb Ireland* solamente dalla sintesi, fatta dal giudice del rinvio. «In secondo luogo, il giudice del rinvio non illustra con sufficiente precisione gli elementi di fatto rilevanti, contrariamente a quanto prescritto dall'articolo 94, lettera a), del regolamento di procedura» (p.ti 23-25 dell'ordinanza).

dell'informazione, ma comunque tali da conformarne il concreto esercizio all'interno dello Stato membro, in particolare gravando tutti i prestatori di servizi di intermediazione immobiliare - ivi inclusi, dunque, gli operatori non stabiliti che prestino i propri servizi *online* - di obblighi ancillari e strumentali all'efficace riscossione delle imposte dovute dai locatori»[28].

In questo il Supremo Collegio dimostra palesemente di non condividere le tesi delle società appellanti e dunque ritiene che «le misure nazionali in esame non siano sussumibili nella nozione euro-unitaria di "regola tecnica" dei servizi della società dell'informazione». A giustificare tale ragionamento l'esegesi testuale e logico-sistematica delle disposizioni, che evidenzia che esse non attengono «ad un servizio della società di informazione specificatamente considerato, ma al servizio di intermediazione immobiliare, sia esso svolto *online* od *offline*, sia esso curato da soggetti residenti, stabiliti ovvero privi di stabile organizzazione […] (dunque) indipendentemente dalle modalità con cui siffatta attività è in concreto svolta»[29]

Tale constatazione deriva vieppiù dall'individuazione della *ratio legis* del provvedimento normativo, volto al «recupero a tassazione dei redditi di locazione breve, mediante, tra l'altro, l'estensione a tali fattispecie di locazione del regime fiscale sostitutivo (la cosiddetta "*cedolare secca*") fino ad allora previsto per le sole locazioni di durata superiore»[30].

Pur non di meno, il Consiglio di Stato ha deciso di sollevare la questione interpretativa in ragione delle specificità della fattispecie, inerente disposizioni di natura fiscale. Fino ad ora infatti il concetto di regola tecnica è stato escluso solo in relazione a «disposizioni nazionali che si limitano a fissare le condizioni per lo stabilimento delle imprese o la prestazione di servizi da parte di queste ultime, come le disposizioni che assoggettino l'esercizio di un'attività professionale ad un previo atto autorizzativo», non essendosi mai la Corte espressa sulla sua riconducibilità anche a «disposizioni nazionali che, in funzione dell'esazione delle imposte ed in relazione ai connessi procedimenti di accertamento e riscossione, impongano specifici obblighi agli intermediari immobiliari, anche qualora questi operino *online* senza una stabile organizzazione nello Stato membro interessato»[31].

La seconda questione, anch'essa di natura interpretativa, ha ad oggetto invece gli obblighi accessori derivanti dalla applicazione della normativa italiana ed in particolare quelli relativi alla «raccolta dei dati inerenti ai contratti di locazione breve e la loro successiva comunicazione all'Amministrazione finanziaria», alla «ritenuta su tali pa-

[28] Cons. St., sez. IV, ord. 19 gennaio 2021, n. 777 (p.to 57), nel quale si specifica anche che tali obblighi ancillari sono:
«a) la raccolta e la successiva comunicazione alle Autorità fiscali dello Stato membro dei dati relativi ai contratti di locazione breve stipulati a seguito dell'attività dell'intermediario;
b) la ritenuta della quota-parte dovuta al Fisco delle somme versate dai conduttori ai locatori ed il conseguente versamento all'Erario di tali somme».

[29] Cons. St., sez. IV, ord. 777/2021, (p.ti 45-46). Difetterebbe dunque «il requisito della specificità, espressamente richiesto dal diritto unionale perché si possa configurare una "*regola tecnica*", […] (che) pertiene al settore dei servizi della società dell'informazione e (che), come nozione appunto settoriale, non è strutturalmente suscettibile di interpretazione estensiva oltre i confini della materia» (p.ti 51-52). Analogamente si era espresso in primo grado T.A.R. Lazio – Roma, sez. II *ter*, n. 2207/2017, p.to 7.1.

[30] Cons. St., sez. IV, ord. 777/2021 (p.to 47).

[31] Ivi (p.to 55).

gamenti con successivo versamento all'Erario» imposti agli intermediari immobiliari attivi in Italia anche *online* che intervengano nella fase del pagamento dei contratti di locazione breve stipulati loro tramite» e alla nomina di «un rappresentante fiscale tenuto ad adempiere in nome e per conto dell'intermediario non stabilito, alle misure nazionali»[32].

Anche in questo caso il Consiglio di Stato decide di sollevare la questione a causa della assenza di precedenti specifici in tema, sebbene non concordi con le conclusioni di *Airbnb*. Infatti, nella valutazione della mancata violazione del principio della libera prestazione dei servizi di cui all'art. 56 TFUE, appare *tranchant* il rilievo che le direttive relative ai servizi resi dalle società di informazione non trovano applicazione per i settori tributari e fiscali[33], nonché quello relativo alla mancata alterazione ad opera della normativa in esame del «*level playing field* fra soggetti nazionali (in quanto residenti o stabiliti) e soggetti operanti da un altro Stato membro in regime di libera prestazione di servizi»[34], poiché la normativa si applica indiscriminatamente a tutti gli operatori che comunque svolgono attività di intermediazione volta alla stipulazione di contratti di locazione breve di immobili ubicati nel territorio nazionale.

In più, anche a voler prescindere da queste considerazioni, il remittente si rifà alla più stabile giurisprudenza della Corte di giustizia, che afferma che una normativa nazionale di carattere generale, che si applica indistintamente a qualsiasi soggetto o impresa che operi nel territorio di uno Stato membro, determinando effetti restrittivi sulla libera prestazione di servizi, può essere giustificata se «risponde a esigenze imperative di interesse generale»[35] e sia volta a garantire il perseguimento di tale scopo in modo proporzionato[36].

Secondo il Supremo Collegio, tale è la disciplina oggetto della controversia negli obblighi che impone alle società appellanti, compreso anche quello relativo alla individuazione di un "rappresentate fiscale" che «semplifica notevolmente tutta la procedura di accertamento e riscossione, altrimenti destinata a disperdersi in plurime pratiche di informazione e collaborazione inter-statale, oltretutto attivabili solo in relazione agli specifici rapporti già previamente individuati dall'Autorità italiana»[37].

---

[32] Ivi (p.to 111).

[33] Il Consiglio dimostra di adeguarsi ad una interpretazione estesa di tali espressioni intese sia in senso sostanziale sia in senso procedurale «comunque afferenti alla materia dell'accertamento e della riscossione delle imposte dovute dai soggetti coinvolti dal servizio prestato» (p.to 76).

[34] Cons. St., sez. IV, ord. 777/2021 (p.to 83).

[35] Cons. St., sez. IV, ord. 777/2021 (p.to 84), che cita fra l'altro la ampia giurisprudenza eurounionale, che al concetto di interesse generale riconduce necessità di garantire l'efficacia della riscossione delle imposte, nonché quella di garantire l'efficacia dei controlli fiscali e la lotta contro l'elusione degli obblighi tributari (p.to 88).

[36] Quanto alla proporzionalità, il Supremo Collegio si premura di far pervenire alla Corte di giustizia anche le sue valutazioni sulla congruità della disciplina oggetto di contestazione in ragione di evidenze di fatto della situazione fiscale nazionale relativa al mercato *online* degli affitti di breve periodo. Esso è caratterizzato da una estesa offerta a prezzi molto modici che non consente all'Ente impositore di controllare il versamento dei tributi dovuti, favorendo una evasione di notevoli dimensioni (Cons. St., sez. IV, ord. 777/2021, p.to 94-96).

[37] Cons. St., sez. IV, ord. 777/2021, p.to 106. Analogamente CGUE, C-1/08, *Athesia Druck Srl contro Ministero dell'economia e delle finanze e Agenzia delle entrate* (2009), § 34, nella quale si afferma che « il meccanismo della rappresentanza [fiscale] ha unicamente lo scopo di consentire al fisco di avere un

Dall'esame dell'ordinanza di rinvio del Consiglio di Stato derivano due considerazioni fra loro conseguenziali. La prima è la constatazione che in materia di piattaforme e società che offrono servizi per l'informazione, in assenza di quadro normativo unitario, il progredire della disciplina è affidato esclusivamente alla giurisprudenza in via eminentemente casistica.
La seconda, immediatamente conseguenziale al primo, è che la natura casistica del diritto giurisprudenziale sul tema varia oramai non solo da caso a caso, dunque da società a società, ma anche nel coinvolgimento di una piattaforma, già precedentemente oggetto di valutazione, a seconda del servizio da essa reso, laddove tali servizi siano molteplici. Ciò evidentemente contribuisce a rendere il quadro normativo massimamente eterogeneo, in una molteplicità di nodi problematici difficilmente districabili.
A queste considerazioni di fatto si sommano le riflessioni che derivano dalla lettura combinata del rinvio pregiudiziale del Consiglio di Stato e della sentenza della Corte di giustizia sulla "versione francese" del caso *Airbnb*[38], le quali inducono intanto a ritenere che quest'ultima sia solo parzialmente risolutiva, poiché formalmente chiarisce soltanto che *Airbnb* sia una società ascrivibile a quelle che svolgono servizi di informazione. L'ordinanza in commento invece evoca ulteriori aspetti, quali l'ammissibilità di obblighi derivanti da misure fiscali di nuova introduzione e non comunicati alla Commissione, che i giudici amministrativi non solo non ritengono "regole tecniche", ma anche legittimano in forza dell'interesse generale alla lotta all'evasione fiscale, sebbene sostanzialmente restrittivi e incidenti sulla libera circolazione dei servizi resi dalla società medesima.

4. La "versione belga" del caso *Airbnb*: la questione pregiudiziale sollevata dalla *Cour constitutionnelle* belga e decisione della Corte di giustizia

Le norme fiscali costituiscono oggi il principale campo di gioco sul quale in questo momento si svolge la partita della regolazione delle società di servizi di informazione, poiché evidentemente la loro natura impone sovente a queste ultime misure restrittive per le attività che svolgono.
Questo fenomeno, infatti, non si è limitato al panorama italiano, se solo si tiene conto del fatto che quasi contemporaneamente alla approvazione del d.l. 50/2017, veniva approvata la legge della Regione di Bruxelles-Capitale del 23 dicembre 2016 relativa alla imposta regionale sui servizi recettivi turistici[39].
La legge in prima battuta definisce cosa si intende per intermediario, ossia «qualsiasi persona fisica o giuridica che, a titolo oneroso interviene per mettere a disposizione un'unità abitativa sul mercato turistico, per assicurare la promozione turistica di un esercizio recettivo turistico o per proporre servizi attraverso i quali i gestori o i turisti

interlocutore nazionale quando il soggetto passivo è stabilito all'estero»

[38] Vedi *supra* § precedente.

[39] *Ordonnance relative a la taxe régionale sur les établissements d'hebergement,* 23 dicembre 2016, pubblicata sul *Moniteur Belge* del 6 gennaio 2017.

possono entrare direttamente in contatto» (art. 2, n. 8).
Essa istituisce una imposta turistica forfettaria (art. 3), che è calcolata sulla base di un importo fisso per unità abitativa, moltiplicato per il numero di notti in cui l'immobile viene occupato, e la impone al gestore dell'esercizio recettivo turistico o, laddove questo sia insolvente o sconosciuto, al proprietario dell'immobile (art. 4).
Al fine di controllare il sorgere di nuove strutture recettive, la legge impone loro una *notification* preliminare di inizio attività da rendersi al Governo regionale entro un mese dalla apertura, comprensiva di tutte le informazioni sulla struttura medesima, pena un'ammenda amministrativa di 6.000 € (art. 6), e una *declaration* mensile sulla attività stessa, da rendersi all'amministrazione fiscale regionale (art. 7).
Infine l'art. 12 dell'*ordonnance* si occupa specificatamente del tema che ci occupa, imponendo precisi doveri di informazione agli intermediari, per gli esercizi recettivi turistici per i quali svolgono la loro attività o quella di promozione, sono tenuti «a comunicare a funzionari designati dal Governo, su richiesta scritta, i dati del gestore e i recapiti degli esercizi recettivi turistici, oltre al numero di pernottamenti e di unità abitative gestite nell'anno precedente», pena una ammenda amministrativa pari a 10.000 €.
La *ratio* della legge era evidentemente l'armonizzazione della tassazione delle strutture recettive turistiche, coinvolgendole tutte nella tassazione, sostituendo la tassa comunale sulle strutture alberghiere e esercenti attività alberghiera con una tassa unica. L'inclusione anche delle cosiddette "strutture recettive a domicilio" nella tassazione aveva dunque lo scopo di aumentare le entrate tributarie, ma anche e soprattutto quello di assicurare una concorrenza leale e un trattamento identico fra tutti gli esercenti del settore turistico[40].
Entrata in vigore la legge, l'amministrazione di aveva inviato a *Airbnb* la richiesta scritta di cui sopra, relativamente alla quale la società irlandese aveva espresso riserve dimostrandosi però disponibile a trattare con le autorità locali, le quali però facevano pervenire una seconda richiesta. Alla espressa dichiarazione della intimata di non voler rispondere, la *Regione Bruxelles Capitale* faceva immediatamente seguire l'imposizione della ammenda prevista.
Nelle more della trattiva, però, la società aveva adito la *Cour constitutionnelle* chiedendo l'annullamento dell'art. 12 della legge regionale brussellese[41]. In particolare e limitatamente a ciò che concerne il presente lavoro, la ricorrente contestava alla Regione di Bruxelles Capitale la violazione degli art. 10 e 11 Cost. belga (i.e. i principi di eguaglianza e non discriminazione) in combinato disposto con l'art 5.1 della direttiva (UE) 2015/1535 che impone agli Stati membri l'obbligo di comunicazione delle regole tecniche alla Commissione, con l'art. 3.5 della direttiva 2000/31/CE che fissa le condi-

[40] Così, peraltro, si legge nei lavori preparatori *Parliament de la Region de Bruxelles-Capitale,* 2016-2017, n. A-445/1 e A-445/2, dai quale emergeva peraltro che le piattaforme incise dai menzionati doveri di informazione fossero principalmente *Airbnb* e *Booking.com.*
Va anche ricordato, che le disposizioni legislative delle Regioni Fiandre e Vallonia realizzano un regime del tutto diverso rispetto a quello di Bruxelles, poiché lì è disposto per gli intermediari l'obbligo di comunicare alle autorità locali solo i dati del gestore e i recapiti delle strutture recettive, i quali vengono raccolti a fini di indagine o laddove vi siano dubbi sul fatto che le strutture soddisfino le condizioni richieste o in caso di reclamo nei confronti delle stesse.

[41] Il ricorso era presentato il 10 luglio 2017 recava numero di ruolo 6708/17.

zioni entro le quali gli Stati membri diversi da quello in cui ha sede la società di servizi di informazione possano imporre misure restrittive delle loro attività e con l'art. 56 TFUE relativo alla libera prestazione dei servizi

In particolare, veniva contestato che la libertà di circolazione dei servizi, assicurata dal combinato disposto delle menzionate disposizioni, sarebbe stata violata dal legislatore regionale, imponendo alle piattaforme obblighi di informazione tali da rendere impossibile o tutt'al più davvero difficile l'esercizio delle loro attività[42] e si sosteneva che tali obblighi non riguardassero la materia tributaria, esclusa dalle direttive citate, ma che si trattasse di regole tecniche[43].

Nel decidere di sollevare il rinvio pregiudiziale, la *Cour constitutionnelle* riprende la giurisprudenza della Corte Giustizia sul caso *Airbnb* del 2019, ma ritiene di non poter prescindere in questo caso dalla questione interpretativa posto che la Corte non si è ancora espressa su casi analoghi e sul concetto di *"domaine de la fiscalité"* , atteso che disposizione impugnata non si riferisce alle società di informazione, ma al servizio di locazione alberghiera turistica e dunque non è una tassa riferita alle piattaforme in generale e alle loro attività, e vuole facilitare la tassazione regionale relativa ai soggiorni turistici[44].

La decisione della Corte di giustizia[45] assume, dunque, una particolare importanza perché è la prima sul tema delle norme fiscali che incidono di fatto sulla attività delle

---

[42] La ricorrente contestava inoltre la violazione della competenza legislativa in materia di servizi delle società di informazione che in Belgio è federale. Tale contestazione è ritenuta non fondata dalla *Cour,* la quale rileva che la disposizione contestata si riferisce esclusivamente alle piattaforme che svolgono servizi relativi agli alloggi turistici (dunque non a tutte le piattaforme), imponendo doveri di natura fiscale (di competenza regionale). *Cour constitutionnelle,* arret 155/2020 del 26 novembre 2020, B.29 e B.30.

[43] Come è evidente le difese svolte da *Airbnb* davanti il Consiglio di Stato e davanti la *Cour constitutionnnele* sono le medesime. Cfr. sul punto § precedente.

[44] *Cour constitutionnelle,* arret 155/2022, cit., B.37.2 e B.37.3.

Le questioni pregiudiziali sollevate erano tre e tutte di natura interpretativa:

«1. Se l'articolo 1, paragrafo 5, lettera a), della direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno [1] , debba essere interpretato nel senso che una normativa nazionale che obbliga i prestatori di un servizio di intermediazione consistente nel mettere in contatto, tramite una piattaforma elettronica e dietro remunerazione, potenziali conduttori con locatori, professionisti o meno, che offrono servizi di alloggio di breve durata, a comunicare, su richiesta scritta dell'amministrazione finanziaria e a pena di ammenda amministrativa, «i dati del gestore e i recapiti degli esercizi ricettivi turistici, oltre al numero di pernottamenti e unità abitative gestite nell'anno precedente» al fine di identificare i soggetti debitori di un'imposta regionale sugli esercizi ricettivi turistici e i loro redditi imponibili, ricade nel «settore tributario» e deve di conseguenza essere considerata esclusa dall'ambito di applicazione della suddetta direttiva.

2. In caso di risposta affermativa alla prima questione, se gli articoli da 1 a 3 della direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno [2] , debbano essere interpretati nel senso che la direttiva in parola si applica a una normativa nazionale come quella descritta nella prima questione pregiudiziale. Se del caso, se l'articolo 56 del Trattato sul funzionamento dell'Unione europea debba essere interpretato nel senso che trova applicazione a una siffatta normativa.

3. Se l'articolo 15, paragrafo 2, della direttiva 2000/31/CE debba essere interpretato nel senso che si applica a una normativa nazionale come quella descritta nella prima questione pregiudiziale e nel senso che autorizza una siffatta normativa».

[45] CGUE, C-674/20, *Airbnb* (2022).

società che svolgono servizi dell'informazione e costituisce una nuova tessera che compone il variegato mosaico della materia, utile anche ai fini della analisi della possibile risoluzione della "versione italiana" del caso *Airbnb*.
Nella stessa, inoltre, la Corte fornisce anche brevi, ma importanti spunti di riflessione sia in generale sul tema delle attività svolte dalle piattaforme, sia su quello connesso della raccolta dei dati da loro operata.
La decisione dei Giudici di Lussemburgo è quella di dichiarare che la normativa della Regione di Bruxelles Capitale non osta con i parametri eurounitari rilevati.
Quanto alla questione del *"domaine de la fiscalité",* la Corte di giustizia ricorda che la direttiva 2000/31/CE fu adottata sulla scorta dell'allora art. 95 TCE (oggi 114 TFUE) sul riavvicinamento delle legislazioni, il quale al par. 2 espressamente esclude le disposizioni fiscali. Inoltre, sulla scorta della sua giurisprudenza[46], ribadisce che l'interpretazione di tali termini deve essere necessariamente estensiva ricomprendendovi «non solo tutti i settori tributari, […] ma anche tutti gli aspetti di tale materia, che si tratti di norme sostanziali o procedurali […] (e) che le modalità di recupero dei tributi di qualsiasi natura non possono essere distinte dal sistema di tassazione o di imposizione al quale si riferiscono»[47]. Tale giurisprudenza peraltro risulta infine positivizzata nella direttiva 2000/31/CE, che utilizza i più ampi termini "settore fiscale", per i quali evidentemente rimandano ad una l'interpretazione letterale estensiva e che anche ai considerando 12 e 13 affermano che essa non è volta a definire norme in materia di obblighi fiscali.
Dunque, sebbene sia pacifico che *Airbnb* sia una società che fornisce servizi per l'informazione[48], tuttavia la direttiva 2000/31/CE non è applicabile, in quanto la disciplina belga risponde ai canoni della normativa fiscale. Infatti, l'amministrazione destinataria delle informazioni è quella tributaria e tali informazioni sono inscindibili dalla sostanza tributaria della disciplina «essendo le sole in grado di identificare il soggetto effettivamente debitore della imposta, la base imponibile della medesima […] e di conseguenza il suo importo»[49].
Quanto al contrasto della disciplina brussellese con l'art. 56 TFUE relativo alla libertà di circolazione dei servizi all'interno dell'Unione, la Corte rileva che l'obbligo di dare seguito alla richiesta di informazioni è imposto a tutti gli intermediari a prescindere dal luogo di stabilimento e a prescindere dalle modalità attraverso le quali svolgono i loro servizi, sia *online* sia con altre "modalità di contatto", senza operare dunque alcuna discriminazione.
I giudici di Lussemburgo si dimostrano ben consci del fatto che l'evoluzione tecnologica e l'attuale configurazione del mercato delle prestazioni di servizi di intermediazione immobiliare determina che coloro che svolgono tali servizi svolgono attraverso una piattaforma *online* saranno certo maggiormente onerati dagli obblighi di trasmissione di dati, rispetto agli intermediari che rendono lo stesso servizio in altro modo. Ciò però per la Corte non è dirimente, anzi al contrario tale obbligo più gravoso è la pro-

[46] CGUE, C-338/01, *Commissione c/ Consiglio* (2004), §§ 63 e 66.

[47] CGUE, C-674/20, *Airbnb* (2022), § 27.

[48] Qui la corte riprende i punti 49 e 60 di CGUE, C-390/18, *Airbnb,* cit.

[49] CGUE, C-674/20, *Airbnb,* cit., § 33.

va del «maggior numero di transazioni alle quali detti intermediari procedono e della rispettiva quota di mercato. Di conseguenza non ne risulta alcuna discriminazione»[50].
Né tanto meno può addursi come discriminazione i maggiori oneri o i maggiori costi che la società dovrebbe trattenere ai fini della raccolta e della archiviazione dei dati necessari per rispondere alle richieste di informazioni della amministrazione belga: è infatti lo stesso intermediario *online* a memorizzare i dati con costi del tutto ridotti, così come peraltro provato dall'esistenza del servizio di *feedback* (sistema di valutazione) dei locatori e dei locatari consultabile dai futuri locatori e locatari[51].

5. La decisione della Corte di giustizia sulla questione pregiudiziale sollevata dal Consiglio di Stato: la "modulazione" della nozione di regola tecnica finalizzata all'interesse (generale) fiscale

La sostanziale rapidità con la quale è stato risolto il caso *Airbnb* nella sua versione belga è dovuta al fatto che la Corte in questa occasione ha deciso, udito previamente l'Avvocato Generale, senza conclusioni, poiché essa non è stata ritenuta sollevare alcuna novità in diritto.
Ed in effetti la normativa regionale belga palesa delle sostanziali differenze rispetto a quella italiana, che fanno comprendere le ragioni della lunga pendenza della questione sollevata dal Consiglio di Stato, per altro quasi contemporaneamente a quella sollevata dalla *Cour constitutionnelle*[52].
La disciplina italiana infatti richiede agli intermediari immobiliari *online* degli obblighi e delle prestazioni, che appaiono ontologicamente diversi da quelli previsti dalla Regione di Bruxelles Capitale: la ritenuta di imposta, la individuazione di un rappresentante fiscale e la sistematicità non solo nella conservazione dei dati, ma anche nella loro comunicazione alla Agenzia delle Entrate (non dunque "a richiesta" come in Belgio)[53].
Dall'insieme di questi dati può dedursi che la fattispecie italiana costituiva un ulteriore approfondimento della questione delle norme fiscali restrittive delle attività delle società di informazione. Così come, peraltro, analogamente poteva dirsi che le questioni sollevate dai giudici italiano e belga, rispetto al caso francese, abbiano comportato un'estensione dell'oggetto, riguardante sempre i servizi resi dalle piattaforme *online*, ma coinvolgenti aspetti diversi e non necessariamente ad essi connessi[54].

[50] Ivi, § 44.

[51] Tale sistema implica dunque che l'intermediario raccolga da sé i dati e dunque che evidentemente non ci siano oneri aggiuntivi. L'esistenza del menzionato sistema di valutazione era stata peraltro indicata dalla stessa *Airbnb* nel precedente che lo aveva coinvolto sempre alla Corte del Lussemburgo (CGUE, C-390/18, *Airbnb,* cit.).

[52] Si ricordi che la questione pregiudiziale è stata dapprima sollevata dal Consiglio di Stato con ordinanza n. 6219 del 18 settembre 2019 e dichiarata manifestamente irricevibile dalla Corte di giustizia, e poi nuovamente con ordinanza n. 777 del 26 gennaio 2021. Fra le due ordinanze italiane si colloca il rinvio pregiudiziale belga sollevato nel novembre 2020. Vedi *infra* § 3 e 4.

[53] Vedi *infra* §

[54] F. Monceri, *Il caso Airbnb,* cit., p. 953, il quale sostiene che le prescrizioni imposte dalla legge italiana

A sostegno di questa tesi anche alcune argomentazioni che si traevano dalle conclusioni dell'Avvocato Generale Szupnar, presentate il 7 luglio 2022.
Infatti, sebbene considerasse oramai "pacifico" che i servizi resi da *Airbnb* siano propri di una società dell'informazione e concordasse con la tesi della società per la quale «il regime fiscale controverso è stato concepito specificamente per le locazioni immobiliari concluse attraverso piattaforme *online*» nonostante «la formulazione delle disposizioni nazionali in discussione sia neutra da un punto di vista tecnologico»[55], l'Avvocato Generale riteneva che in questo caso specifico la definizione di "regola tecnica relativa ai servizi", utile al fine di definire la prima questione pregiudiziale, dovesse essere interpretata in modo "più modulato", al fine di stabilire se le disposizioni in esame abbiano come obiettivo quello di disciplinare "l'accesso o l'esercizio" del servizio medesimo[56].
Conseguentemente a questa "interpretazione modulata", tutte le norme contestate non rientrano nella nozione di "regola tecnica": la trasmissione delle informazioni alla amministrazione finanziaria ha lo scopo di controllare l'attività dei locatori e sorge *ex post* come conseguenza dell'esercizio dell'attività di intermediazione, non riguardando i rapporti intermediario/clienti, ma solo quelli con l'amministrazione finanziaria; l'obbligo di ritenuta fiscale quello di riscuotere le imposte sulla attività di locazione immobiliare, di cui l'obbligo di nominare un rappresentante fiscale semplicemente una conseguenza amministrativa[57]. Gli obblighi imposti dalla normativa italiana sarebbero dunque esclusi dall'ambito di applicazione della direttiva 2000/31/CE in quanto rientrano nel settore tributario, poiché il destinatario di tali informazioni è l'amministrazione finanziaria ed essi sono inscindibilmente legati a tale normativa[58].
La Corte di giustizia nella sentenza depositata il 22 dicembre 2022 conferma la "lettura

siano «difficili da contestare in quanto riferite tanto agli operatori che offrono il servizio di locazione breve attraverso piattaforme *online*, quanto a coloro che svolgono il servizio in modo tradizionale». Sul punto si permetta di rinviare a M.E. Bucalo, *I servizi delle piattaforme* online *fra giurisprudenza sovranazionale e interna e necessità di una regolazione flessibile. Riflessioni a partire dal caso* Airbnb, in *federalismi.it,* 22, 2020, p. 78.

[55] Conclusioni dell'Avvocato Generale, in C-83/21, *Airbnb,* (2022), §§ 33-35. È infatti attraverso i loro servizi che il settore delle locazioni brevi fra privati ha conosciuto uno sviluppo così rilevante, tanto da necessitare l'intervento del legislatore per contrastare l'evasione fiscale.

[56] Conclusioni dell'Avvocato Generale, in C-83/21, cit., § 37. Si tratta in realtà di una interpretazione quasi creativa (più che modulata) del combinato disposto dell'art. 1, par. 1, lett. e), primo comma e secondo comma, p.to i), della direttiva (UE) 2015/1535, ai sensi della quale «una regola si considera riguardante specificamente i servizi della società dell'informazione quando (...) essa si pone come finalità e obiettivo specifici (...) di disciplinare in modo esplicito e mirato tali servizi», dal quale viene tratto il significato (almeno parzialmente) diverso di «regola che abbia come finalità e obiettivo specifici quelli di disciplinare in modo esplicito e mirato l'accesso e l'esercizio di tali servizi».

[57] Conclusioni dell'Avvocato Generale, in C-83/21, cit., §§ 39-43. Sebbene si debba rilevare quanto sia davvero complicato sostenere che tale obbligo non condizioni l'attività in parola e riguardi solo «in modo incidentale» l'attività dell'intermediario.
Neppure si possono fare rientrare tali norme nella nozione di "regole tecniche *de facto*", ai sensi dell'art. 1, par. 1, lett. f), secondo comma, p.to iii), della direttiva (UE) 2015/1535, in quanto norme relative ai servizi connesse a misure di carattere fiscale, perché in CGUE, C-98/14 (2015), §§ 96-97, la Corte ha sostenuto che tali norme accompagnano misure fiscali che hanno lo scopo di influenzare il consumo di determinati prodotti o servizi, cosa che non accade nel caso specifico dove le disposizioni hanno come scopo la lotta all'evasione fiscale.

[58] CGUE, C-674/20, *Airbnb,* cit., §§ 32-33. Vedi *supra* § precedente

modulata" proposta dall'Avvocato Generale[59]e, riprendendo le argomentazioni della pronuncia brussellese, ritiene che tutti e tre i sopracitati obblighi imposti dal legislatore italiano rientrino nel settore tributario. Conseguentemente le risposte alle questioni pregiudiziali sollevate dal Consiglio di Stato presuppongono unicamente «l'esame della legittimità di (tali) misure […] rispetto al divieto di cui all'articolo 56 TFUE», perché, «sebbene la materia delle imposte dirette rientri nella competenza degli Stati membri, questi ultimi devono tuttavia esercitarla nel rispetto del diritto dell'Unione»[60].
Quanto al primo obbligo relativo alla trasmissione dei dati alla amministrazione fiscale da parte degli intermediari *online,* la Corte non ne ravvisa la lesività rispetto alla libertà di circolazione dei servizi per una molteplicità di ragioni: tale obbligo infatti è richiesto a tutti gli intermediari a prescindere dalle modalità delle loro prestazioni[61] e sebbene sia vero che per gli intermediari *online* esso sarebbe più gravoso e impegnativo, ciò sarebbe «solo il riflesso di un maggior numero di transazioni alle quali detti intermediari procedono e della loro rispettiva quota di mercato» derivante dalla evoluzione dei mezzi tecnologici[62]. Inoltre, poiché tali soggetti agiscono attraverso strumenti digitali e procedono alla archiviazione e memorizzazione dei dati, tale obbligo non sarebbe neppure così gravoso dal punto di vista dei costi[63].
Passando alla analisi della conformità rispetto all'art. 56 TFUE dell'obbligo di ritenuta fiscale introdotto dalla normativa italiana, la Corte, preliminarmente rilevando che anch'esso è imposto a tutti gli intermediari, concorda con le conclusioni dell'Avvocato Generale, laddove riteneva che esso costituisca un onere ben più importante rispetto a un semplice obbligo di informazione, se non altro a causa della responsabilità finanziaria che esso genera nei confronti dello Stato d'imposizione[64].
Pur non di meno esso non può essere considerato discriminatorio in quanto applicato alle sole piattaforme che gestiscono i pagamenti *online,* perché essi agevolano l'incontro di un gran numero di domande e offerte di locazioni brevi di immobili e dunque di un gran numero di persone fisiche, non soggette ad obblighi fiscali, che altrimenti sarebbero difficili da controllare ai fini tributari[65].
Sul punto le riflessioni dell'Avvocato Generale rilevavano come «La ritenuta fiscale (o la ritenuta d'acconto) è una tecnica fiscale universalmente utilizzata, che non solo consente di garantire l'efficace riscossione delle imposte, ma costituisce parimenti una

[59] CGUE, C-83/21, *Airbnb* (2022), §§ 32-38.

[60] Ivi, § 41, sulla scorta di stabile giurisprudenza fra cui CGUE, C-296/12 (2014).

[61] Ivi, § 45.

[62] Ivi, § 47 riprendendo CGUE, C-674/20, *Airbnb,* cit., § 44.

[63] CGUE, C-83/21, *Airbnb,* § 50.

[64] Conclusioni dell'Avvocato Generale, in C-83/21, cit., § 56.

[65] Così CGUE, C-83/21, *Airbnb,* cit., § 54. Più diffusamente l'Avvocato Generale nelle sue conclusioni (spec. §§ 61-63), riteneva anche che non risultassero valide neppure le argomentazioni di *Airbnb* relative alla discriminazione delle società che forniscono servizi *online* non stabilizzate, per il semplice fatto che tale attività non richiede lo stabilimento in un determinato luogo e costituisce un elemento caratterizzante l'economia delle piattaforme. Né era discriminatorio per le società non residenti l'imposizione di obblighi di ritenuta identici a quelli imposti ai residenti, perché il regime fiscale ha ad oggetto non una tassa sui servizi di *Airbnb*, ma sulle attività di locazione di beni immobili situati nel territorio italiano, che stanno alla base di tali servizi, di competenza esclusiva dello Stato italiano (§§ 64-66).

misura di semplificazione e di maggiore certezza giuridica per i contribuenti. Inoltre, per l'operatore che, in ogni caso, è in possesso dei fondi che costituiscono la base imponibile, come nel caso di un intermediario immobiliare che interviene nel pagamento dei canoni di locazione, l'obbligo di trasferire parte di tale somma alle autorità finanziarie non rappresenta un onere eccessivo. […] È del pari evidente che una misura di questo tipo consente di combattere efficacemente l'evasione fiscale, imponendo ad un operatore che non è personalmente interessato a sottrarsi all'imposta la responsabilità del versamento della stessa all'amministrazione finanziaria»[66].

Infine, quanto all'obbligo di nominare un rappresentante fiscale stabilito sul territorio dello Stato[67], la Corte rileva preliminarmente che esso grava solo su taluni prestatori di servizi immobiliari non residenti in Italia ed in particolare solo su quelli che intervengono nel pagamento incassando i canoni di affitto o comunque intervenendo nella riscossione degli stessi. Ciò evidentemente determina una «restrizione alla libera circolazione dei servizi, vietata, in linea di principio, dall'articolo 56 TFUE»[68].

Tale restrizione però, in ossequio alla sua costante giurisprudenza, viene valutata dalla Corte giustificata da motivi di interesse generale (quello di assicurare l'efficacia della riscossione fiscale) ed è idonea a garantire la realizzazione dell'obiettivo del contrasto all'evasione fiscale[69], soprattutto laddove si consideri che il ricorso a prestatori di servizi di intermediazione immobiliare che gestiscono un portale telematico, ha conosciuto uno sviluppo esponenziale e che tali locazioni sono per lo più brevi e dunque numerose in un unico esercizio fiscale.

Dove però la normativa italiana sul rappresentante fiscale non supera il vaglio di conformità rispetto all'art. 56 TFUE è la valutazione della proporzionalità della misura rispetto all'obiettivo da raggiungere[70], in particolare sotto il profilo della residenzialità o dello stabilimento del rappresentante medesimo sul territorio nazionale, senza alcuna distinzione basata per esempio sul volume di entrate fiscali riscosse e senza valutare che esso avrebbe potuto comunque risiedere anche in uno Stato membro diverso[71].

Quanto a quest'ultimo punto la Corte rileva (spec. § 74) che è irrilevante che «la semplice affermazione che il requisito della residenza costituisce la migliore garanzia dell'efficace adempimento degli obblighi di natura tributaria incombenti sul rappresentante fiscale, (perché) se il controllo su un tale rappresentante da parte delle autorità fiscali di

[66] Conclusioni dell'Avvocato Generale, in C-83/21, cit., §§ 69-70.

[67] Bisogna rilevare che la normativa italiana non dispone espressamente che il rappresentante debba essere stabilito in Italia, ma ciò era stato espressamente affermato dal Governo in udienza, rilevando che se così non fosse stato sarebbe venuta meno l'utilità dell'istituto, volto a consentire alla amministrazione fiscale un collegamento più facile con società con sede fuori dai confini nazionali (si vedano le Conclusioni dell'Avvocato Generale, § 75).

[68] CGUE, C-83/21, *Airbnb,* cit., § 59.

[69] Ivi, §§ 62-69.

[70] Ivi, §§ 70-77.

[71] Analogamente nelle sue conclusioni l'Avvocato Generale (§§ 80-82) aveva ritenuto non proporzionato l'obbligo imposto di nominare un rappresentante fiscale, sulla scorta di un caso del tutto simile a quello *de quo* (CGUE, C-678/11, *Commissione c/ Spagna* (2014) nel quale la Corte aveva affermato che l'obbligo di nominare un rappresentante ai prestatori di servizi transfrontalieri ai fini della trasmissione di informazioni e della ritenuta fiscale, costituisce una restrizione sproporzionata alla libera prestazione dei servizi contraria all'art. 56 TFUE.

uno Stato membro può effettivamente risultare più difficile qualora questi sia stabilito in un altro Stato membro, […] tuttavia le difficoltà amministrative non costituiscono, di per sé, un motivo atto a giustificare un ostacolo a una libertà fondamentale garantita dal diritto dell'Unione».

6. Questioni pregiudiziali pendenti (italiane e non solo)

Nonostante la definizione della questione di pregiudizialità sollevata dal Consiglio di Stato nei termini appena esposti, il discorso più ampio sulla compatibilità di alcune norme legislative con i servizi resi dalle piattaforme *online* e con il principio della libera circolazione degli stessi, come sanciti nell'ordinamento comunitario sia dalle disposizioni di natura originaria (i.e. l'art. 56 TFUE) sia dalle disposizioni di natura derivata (i.e. le direttive 2000/31/CE e (UE) 1535/2015) non sembra affatto chiuso. Ce lo dice una rapida analisi del sito della Corte di giustizia, presso la quale risultano pendenti diverse questioni pregiudiziali sul tema, segno che la supplenza giurisprudenziale in tema non riesce più a fare da argine e servono ulteriori e diversi rimedi.
Come sintomo del malessere diffuso avverso la non coerenza e la non univocità dell'ordinamento eurounitario in tema di economia delle piattaforme, va rilevato che le questioni, alle quali si accenna, sono sollevate da Stati membri diversi[72] e da ultimo e nuovamente anche dall'Italia.
L'immaginifico "giro per l'Europa" attraverso lo studio delle fattispecie che coinvolgono le società che forniscono servizi per l'informazione, infatti, si ferma ancora in Italia, per l'analisi dei recentissimi rinvii pregiudiziali sollevati dal TAR Lazio – Roma, coinvolgenti alcune importanti piattaforme operanti in diversi settori del mercato, ma alle quali la legislazione italiana ha imposto determinati oneri comunicativi[73], riportandoci alle problematiche sollevate nel *leading case* francese coinvolgente *Airbnb,* ma originariamente esplorate nei casi *Uber* e *Google Spain.*
Tutte le società ricorrenti hanno impugnato i provvedimenti dell'Autorità Garante per le Comunicazioni, che a vario titolo, hanno disposto l'obbligo di iscrizione al Registro degli Operatori di Comunicazione (ROC), nonché quello di comunicazione dell'Informativa Economica di Sistema (IES) a carico dei fornitori di servizi di intermediazione *online* e dei fornitori di motori di ricerca, che erano stati emessi a seguito della modifica della legge dell'art. 1 della legge n. 249/1997 (istitutiva dell'Agcom), operata dall'art. 1, c. 515, della legge di bilancio 2021 a seguito dell'emanazione del regolamento (UE) 2019/1150. A questi fini è prevista la compilazione di diversi moduli concernenti sia l'attività svolta sia l'organizzazione del soggetto obbligato, il loro annuale aggiorna-

[72] Fra le questioni di maggiore rilevanza che oggi coinvolgono le piattaforme vanno almeno menzionate quelle relative alla protezione dei dati personali che esse trattano. *Ex multis* fra quelle pendenti appare di particolare importanza *Meta c/Bundeskartellamt*, C-252/21, sollevata dal Tribunale Superiore del Land di Dusseldorf, e relativa anche alle condizioni generali di contratto sottoscritte dagli utenti.

[73] Si tratta di TAR Lazio – Roma, sez. IV bis, ordd. 12834, 12835, 12836, 12839, 12840 e 12841/2022. Le questioni sollevate risultano depositate in Corte di giustizia e recano rispettivamente i numeri C-662/22 *Airbnb,* C-665/22 e C-666/22 *Amazon,* C-666/22 *Eg Vacation Rentals Ireland,* C-663/22 *Expedia* e C-664/22 *Google Ireland.*

mento e in caso di violazione l'applicazione di sanzioni amministrative.
Inoltre, il c. 517 dell'art. 1 della stessa legge di bilancio 2021 prevede anche il pagamento di un contributo a carico dei fornitori di servizi di intermediazione e dei motori di ricerca *on line*, al fine di assicurare la copertura dei costi amministrativi complessivamente sostenuti per l'esercizio delle funzioni di regolazione, di vigilanza, di composizione delle controversie e sanzionatorie attribuite all'Autorità.
Secondo il remittente le misure introdotte dal legislatore istituirebbero un controllo relativo ai profili soggettivi dei fornitori e sarebbero del tutto diverse rispetto a quelle richieste dal regolamento e inadeguate a perseguirne il fine, volto ad assicurare la trasparenza e l'equità dei rapporti contrattuali fra utenti e piattaforme[74].
Il TAR, dunque, si riporta alla giurisprudenza eurounitaria in tema di regole tecniche delle società che svolgono servizi per l'informazione e dei relativi obblighi di notifica[75], ricordando che la direttiva (UE) 2015/1535 ne prevede la comunicazione alla Commissione al fine di garantirne il controllo a tutela del principio della libera circolazione delle merci e dei servizi.
Guardando aldilà della Manica e tronando al tema delle imposte che per le loro attività devono versare le società che svolgono servizi per l'informazione, è importante anche solo menzionare il caso che coinvolge la *Fenix International Limited,* la quale gestisce un *social media* conosciuto come *Only Fans*[76].
Attraverso tale piattaforma, gli utenti *creators* creano e pubblicano contenuti che pubblicano sul loro profilo, fissando un canone mensile di abbonamento (sebbene la piattaforma imponga un importo minimo annuo); gli utenti *fans* possono accedere ai contenuti caricati effettuando pagamenti *ad hoc* o pagando un abbonamento mensile per ogni *creator* che desiderano seguire o col quale desiderano interagire.
La *Fenix* fornisce anche la piattaforma attraverso la quale vengono effettuati i pagamenti, che poi vengono girati, sotto la sua responsabilità, ai *creators* attraverso un terzo prestatore di servizi di pagamento, con un addebito del 20%. Tanto i pagamenti dei *fans* quanto quelli dei *creator* appaiono come pagamenti fatti alla società.
Dal 2017 al 2020, periodo contestato dalla amministrazione tributaria britannica, la *Fenix* ha applicato e contabilizzato l'IVA a un'aliquota del 20% sugli addebiti operati sui *creators*. Per questo l'Amministrazione tributaria britannica aveva inviato alla società nell'aprile 2020 avvisi di accertamento per l'IVA dovuta, in quanto ai sensi dell'art. 9 bis, par. 1, ultimo comma, del regolamento di esecuzione (UE) n. 282/2011 del Consiglio recante disposizioni di attuazione della direttiva 2006/112/CE, «a un soggetto passivo che, in relazione ad una prestazione di servizi prestati tramite mezzi elettro-

[74] L'art. 16 del regolamento (UE) 2019/1150 prevede poi che «La Commissione, in stretta cooperazione con gli Stati membri, monitora attentamente l'impatto del presente regolamento sulle relazioni tra i servizi di intermediazione online e i loro utenti commerciali e tra i motori di ricerca online e titolari di siti web aziendali. A tale fine la Commissione raccoglie informazioni pertinenti per monitorare l'evoluzione di tali relazioni, anche mediante la realizzazione di studi adeguati. Gli Stati membri assistono la Commissione fornendo, su richiesta, tutte le informazioni pertinenti raccolte, anche riguardo a casi specifici».

[75] CGUE, C-674/20, cit. Vedi *supra* § 2.

[76] *Fenix International Limited c/ Commissioners for Her Majesty's Revenue and Customs,* C-695/20, per il quale sono state depositate le conclusioni dell'Avvocato Generale lo scorso 15 settembre 2022.

nici, autorizzi l'addebito al destinatario o la prestazione dei servizi ovvero stabilisca i termini e le condizioni generali della prestazione non è consentito designare esplicitamente un'altra persona quale prestatore di tali servizi».

Impugnato l'accertamento, la *Tax Chamber of the First-tier Tribunal del Regno Unito* (Sezione tributaria del Tribunale di primo grado) ha sollevato la questione di pregiudizialità avanti la Corte di giustizia, poiché ancora il Regno Unito era membro dell'U.E. e dunque poiché il regolamento direttamente applicabile.

Si tratta di un rinvio di validità sollevato dal giudice britannico, che invero sorprende quanto a data di presentazione (22 dicembre 2021), posto che il periodo di transizione relativo al recesso del Regno Unito dall'Unione Europea sarebbe terminato il 31 dicembre 2021, ma che la Corte di giustizia resta competente ai sensi dell'art. 86, par. 2, dell'accordo di recesso[77].

Il giudice tributario, infatti, nutre dubbi circa la validità dell'articolo 9 bis regolamento di esecuzione (UE) n. 282/2011, ritenendo che, essendo un mero regolamento di attuazione dell'art. 28 della cd. Direttiva IVA, ecceda i limiti a tal fine fissati, sostanzialmente modificando e integrando la normativa che meramente avrebbe dovuto eseguire.

Tale eccesso sarebbe ravvisabile nel mutamento radicale della disciplina determinato dalla presunzione, secondo la quale: «Ai fini dell'applicazione dell'articolo 28 della direttiva [IVA], se i servizi prestati tramite mezzi elettronici sono resi attraverso una rete di telecomunicazione, un'interfaccia o un portale […], si presume che un soggetto passivo che interviene in detta prestazione agisca in nome proprio ma per conto del prestatore di tali servizi».

A prescindere dalle conclusioni rese dall'Avvocato Generale, secondo il quale «Dall'esame della questione pregiudiziale non è emerso alcun elemento idoneo ad inficiare la validità dell'articolo 9 bis del regolamento di esecuzione (UE) n. 282/2011 del Consiglio», la questione assume una primaria importanza, per almeno due considerazioni.

La prima di ordine istituzionale, inerisce al rapporto fra i poteri e dunque ai gangli fondamentali profondi della forma di governo dell'Unione dal punto di vista pubblicistico (e non soltanto del diritto tributario), perché sollevando questo tipo di rinvio il giudice britannico, oramai sull'uscio dell'Unione Europea, senza mezzi termini taccia di scorrettezza l'operato delle istituzioni europee, affermando che il Consiglio nell'approvare il regolamento di attuazione della direttiva IVA avrebbe ecceduto le sue competenze oltrepassando il potere di esecuzione che gli è conferito dal TFUE.

La seconda considerazione, in realtà connessa alla prima, è che la crescente influenza esercitata dalle piattaforme *online* nell'economia, coinvolge oramai diversi settori del mercato e dell'ordinamento (sovente anche questioni tributarie) incidendo anche sui rapporti istituzionali fra gli organi sovranazionali e interni.

[77] Ai sensi dell'art. 86, par. 2, dell'accordo sul recesso del Regno Unito, la Corte resta competente a pronunciarsi in via pregiudiziale sulle domande presentate dai giudici del Regno Unito prima della fine del periodo di transizione.

7. La via della regolazione unitaria delle piattaforme: *Digital Services Package*

Dai casi sopra analizzati emerge in modo netto che la questione fondamentale determinata dallo sviluppo della economia delle piattaforme è quella di disciplinare in modo univoco e nel rispetto del diritto sovranazionale i problemi sorti connessi al suo funzionamento.

Infatti, l'elemento che più accentua questi problemi è costituito dallo strettissimo legame fra i servizi resi da queste società, per loro natura transfrontalieri, perché forniti tramite Internet, e quelli forniti agli utenti, che invece sono "reali", "concreti" e localizzati ordinariamente in un luogo fisico ben individuabile[78]. Ciò impatta con alcuni principi del diritto pubblico e dell'Unione Europea, *in primis* il principio di libera prestazione dei servizi, che oggi necessitano di un ripensamento necessario a far fronte alle nuove sfide determinate dal funzionamento delle piattaforme *online*.

Volendo trovare il filo conduttore delle riflessioni indotte dall'esame della giurisprudenza sopra analizzata, un primo elemento di fatto risulta immediatamente evidente: l'"andamento casistico" della positivizzazione delle "regole del gioco" in materia di economia digitale. Il risultato attuale è che alla Corte di giustizia viene affidato il compito di determinare i criteri in base ai quali riconoscere agli intermediari la natura di società che svolgono servizi per l'informazione (il cosiddetto *Uber test*) e conseguentemente se ad esse si applicano o meno le direttive servizi (direttiva 2000/31/CE e direttiva (UE) 2006/123[79].

D'altro canto, come si è tentato di dimostrare, la giurisprudenza eurounitaria in tema si fa sempre meno univoca, soprattutto laddove vengano contestati e fatti valere i limiti di applicabilità delle menzionate discipline[80]. In questi casi, laddove evidentemente l'interesse generale degli Stati e dell'Unione (in specie quello alla corretta riscossione fiscale) diviene predominante, la Corte "modula" il concetto di "regole tecniche", restringendone l'"ambito di applicazione"[81] e trovando "in modo creativo" la quadratura del cerchio nel rispetto delle legislazioni nazionali.

In questo intricato scenario, per Autorità locali, Governi e Legislatori la posizione da assumere è sempre meno chiara: da un lato, l'individuazione dei criteri identificativi delle piattaforme ad opera della giurisprudenza sovranazionale lega loro le mani, spesso a discapito della posizione e dei diritti degli utenti[82]; dall'altro, in assenza di regole univoche e di una giurisprudenza omogenea, la loro discrezionalità si amplia, soprattutto in materie nelle quali è possibili derogare alla normativa europea.

La confusione che domina il quadro attuale ha influito anche sulla attività dei giudici

[78] L'Avvocato Generale Szpunar nelle conclusioni a C-83/21 del 7 luglio 2022, § 3, ha affermato che le piattaforme hanno oramai «cambiato il profondamente il carattere dei servizi transfrontalieri […] conferendo loro un carattere misto, nel senso che detti servizi sono fortemente connessi a prestazioni successive che non hanno siffatta qualità».

[79] G. Smorto, *Armi spuntate,* cit., che rileva la illogicità di tale sistema che sovente non tiene conto dell'impatto sull'economia e sul territorio delle singole società.

[80] In specie gli art. 1, par. 5, e 3, par. 4, della direttiva 2000/31/CE e art. 2 direttiva 2006/131/CE.

[81] Si veda CGUE, C-83/21, *Airbnb,* cit. e spec. § 5.

[82] G. Smorto, *Armi spuntate,* cit.

che, sempre più frequentemente, in fattispecie aventi ad oggetto l'economia della piattaforme ritengono di dover sollevare questioni pregiudiziali avanti la Corte di giustizia, per la maggior parte delle quali di natura interpretativa, sebbene non manchino quelle di validità volte ad incidere in modo diverso e più penetrante nella attività normativa delle istituzioni europee, nonché nei rapporti fra queste ultime e gli Stati membri[83].

La necessità di una regolazione univoca dei principi dell'economia digitale è quindi una esigenza pressante che la Commissione aveva fatto propria già nel 2016 con la Comunicazione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale, e al Comitato delle Regioni intitolata "Un'agenda per l'economia collaborativa"[84]. In quel documento essa si era dimostrata ben consapevole dell'impatto che l'economia delle piattaforme avrebbe avuto con l'ordinamento europeo e aveva individuato fra le possibili soluzioni lo «sviluppo di *standard* comuni fra gli Stati per affrontare tali questioni in modo coerente»[85] e l'istituzione di «un quadro di monitoraggio che includa sia l'ambiente normativo in evoluzione che gli sviluppi economici e delle imprese […] teso a seguire le tendenze dei prezzi e della qualità dei servizi e a individuare eventuali ostacoli e problemi riscontrati, in particolare se derivano da regolamentazioni nazionali divergenti o lacune normative»[86], invitando peraltro gli Stati membri a chiarire e armonizzare la situazione normativa nazionale.

La nuova coscienza europea sulla necessità della regolazione del fenomeno dell'economia delle piattaforme oggi prende forma e si sostanzia nel *Digital Market Act*[87] e nel *Digital Service Act*[88]*,* che insieme formano un pacchetto completo di disposizioni sull'economia e i servizi digitali (*Digital Services Package*).

Essi sembrano delineare un modello di intervento regolativo che mira a contemperare, da un lato, le esigenze dello sviluppo economico del settore digitale e la capacità di innovazione del tessuto imprenditoriale europeo, e, dall'altro, gli interessi economici e politici dell'Unione

Il DSA, ad esempio, introduce una nuova serie di obblighi di trasparenza per quelle che definisce "*very large platform*", con l'obiettivo dichiarato di sottoporre queste ultime

[83] Si vedano per quelle di natura interpretativa quelle da ultimo sollevate dal TAR Lazio e per quelle di validità quella sollevata dal giudice tributario britannico, tutte esaminate nel § 6. Sul punto si veda anche P. Van Cleynenbreugel, *Le droit de l'Union européenne face à l'économie collaborative,* cit., 71, il quale, in assenza precise disposizioni, riteneva che fosse compito delle Corti valutare caso per caso la corretta applicazione del diritto eurounitario e vedeva nell'intervento regolativo sovranazionale la via per consentire anche agli Stati membri di esercitare i loro poteri normativi in modo ad esso conforme.

[84] COM (2016) 356 final, 2 giugno 2016.

[85] Ivi, 15-16. Analogamente quanto ai regimi fiscali, in quella sede la Commissione invitava gli Stati a imporre «obblighi proporzionati e a condizioni di parità, e applicare obblighi fiscali funzionalmente analoghi alle imprese che forniscono servizi comparabili».

[86] Ivi, 16.

[87] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 *(Digital Market Act)*

[88] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (*Digital Service Act).* Entrambi i regolamenti produrranno effetti da maggio 2023.

a un "maggiore controllo democratico"[89], riducendo l'ambito di applicazione delle esenzioni di responsabilità di cui alla direttiva 2000/31, ridefinendo le piattaforme come soggetti con precise responsabilità verso ole autorità pubbliche e verso i cittadini e non più semplice intermediario.

Il DMA invece riconosce le piattaforme come veri e propri *gatekeepers,* conferendo loro «il potere di agire come *rule-makers* privati» che si collocano nel mezzo del rapporto tra aziende e consumatori[90], cui consegue una serie di obblighi e relative sanzioni, il cui controllo è affidato alla Commissione[91].

Più specificatamente, la normativa nel suo complesso nel modificare la direttiva europea sull'*e-commerce* del 2000, mantiene le regole di natura sostanziale relative alla responsabilità degli intermediari *online,* ma ne potenzia il livello di trasparenza e *accountabilty,* attraverso *misure di carattere procedurale,* limitatamente però alle società di intermediazione considerate maggiormente rilevanti, secondo una soglia stimata in oltre 45 milioni di destinatari del servizio, ed escludendo così le micro e piccole imprese.

L'obiettivo della disciplina voluta dalla Commissione è allora quello di fornire un nuovo quadro giuridico dei servizi digitali, che, partendo dalle regole sostanziali già esistenti, sia in grado di rafforzare il mercato unico digitale e garantire il rispetto dei diritti e dei valori dell'Unione.

Inoltre, la normativa appare di primaria importanza anche al fine di evitare la estrema frammentazione normativa a livello dei singoli Stati membri, che comporterebbe ostacoli allo sviluppo delle imprese europee, rafforzando il potere dei *tech giants* e alla armonizzazione delle garanzie dei diritti dei cittadini.

La validità dell'intervento regolatore dei pubblici poteri si rivela, infatti, ancora preferibile, poiché è in grado di bilanciare, in modo equilibrato e finalmente univoco, le esigenze di tutelare i diritti dei singoli e quella di non ostacolare il fluire spedito dell'innovazione tecnologica, grazie alla sua "natura procedurale" (potremmo di flessibile o *in progress*) delle sue norme.

In tal senso può dirsi che il disegno del legislatore europeo sembra quindi intendere la nuova disciplina dei mercati e dei servizi digitali come uno strumento volto alla promozione dei diritti dei cittadini dell'Unione[92] e come forma di limitazione all'esercizio del potere delle grandi piattaforme, nel tentativo di democratizzare la rete attraverso un nuovo costituzionalismo digitale antropocentrico[93].

---

[89] Lo definisce così M. Santaniello, *Sovranità digitale e diritti fondamentali: un modello europeo di* Internet governance, in *Rivista italiana di informatica e diritto,* 2022, 1, 49.

[90] Così la Commissione europea nella pagina esplicativa del regolamento disponibile al link *ec.europa.eu.*

[91] Analogamente la proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final del 21 aprile 2021 si propone di affrontare i rischi sociali e individuali dello sviluppo delle intelligenze artificiali attraverso disposizioni legislative che ne assicurino la coerenza con «i valori, i diritti fondamentali e i principi dell'Unione». Sul punto D. Messina, *La proposta di regolamento europeo in materia di Intelligenza Artificiale: verso una "discutibile" tutela individuale di tipo* consumercentric *nella società dominata dal "pensiero artificiale",* in questa *Rivista*, 2, 2022, 204 ss.

[92] Così anche E. Celeste, *Digital Sovereignty in the EU: Challenges and Future Perspectives*, in F. Fabbrini - E. Celeste - J. Quinn (eds.), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford, 2021.

[93] In tema si veda M. Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*,

In questo nuovo contesto regolativo sovranazionale, si innesta il ruolo dei Governi nazionali, i quali al pari dell'Unione, non potranno più assumere solo il ruolo di arbitri delle dinamiche del mercato, ma dovranno necessariamente «essere attori decisivi per negoziare valori pubblici per conto e in favore dei cittadini» e degli utenti del mercato[94].

Cambridge, 2017 e C. Colapietro, *Le sfide del "costituzionalismo digitale": un approccio originale al rapporto fra diritto e tecnologia,* in *Rivista del Gruppo di Pisa,* fascicolo speciale, 3, 2021, 12.

[94] J. Van Dijck, Nuovi mondi online, in Il Foglio, 25 febbraio 2019.

Intelligenza urbana e tutela dei diritti fondamentali. Antinomia o complementarità nella nuova stagione algoritmica?

Federica Paolucci - Oreste Pollicino

Abstract

Parlare di città intelligente può sembrare un argomento di fantascienza. Eppure, dati, intelligenza artificiale e sensori sono strumenti che sempre di più fanno parte del panorama urbano. La presente analisi offre una panoramica dei principali interrogativi su cui può appuntarsi il contributo del diritto costituzionale. Difatti, è innegabile che la *smart city* pone delle sfide che concernono sicuramente il mercato, ma anche il nuovo assetto di poteri in ambito digitale.

Talking about a smart city may sound like science fiction. Yet, data, artificial intelligence, and sensors are tools that are increasingly part of the urban landscape. This analysis offers an overview of the main questions to which constitutional law can contribute. Undeniably, the smart city poses challenges that concern the market and the new order of powers in the digital sphere.

Sommario

1. Introduzione. - 2. Quale riservatezza nella città intelligente? Spunti di riflessione. - 2.1 (Segue) La fortezza europea della privacy alla prova della *smart city*. - 3. La città tra pubblico e privato. - 3.1 (Segue) Una sfida per il legislatore europeo. - 4. Conclusione.

Keywords

smart city - dati - protezione dati - privacy - digitalizzazione

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco". Il presente lavoro è frutto dell'attività di ricerca dei due autori. In particolare, i paragrafi 2 e 2.1 sono attribuibili interamente a Oreste Pollicino, mentre i paragrafi 3 e 3.1 a Federica Paolucci. I paragrafi 1 e 4 sono attribuibili a entrambi.

1. Introduzione

Le città sono sempre più popolate tanto da esseri umani[1], quanto da strumenti tecnologici. Dati, intelligenza artificiale e sensori stanno componendo un'inedita dimensione della *urbs* in cui i modelli tradizionali della città (e del vivere umano) sono chiamati a coesistere con la rete. Questa nuova sfera dello spazio urbano prende il nome di *smart city*: un termine ad ombrello con il quale si suole intendere la nuova integrazione tra spazio digitale e spazio reale. Al di là di ogni distopico scenario che tale contesto è in grado di generare e far immaginare, l'analisi di questo fenomeno deve concentrarsi sull'*humus* che sta consentendo l'intersecazione tra spazio urbano e rete: i dati. Difatti, gli incessanti flussi di informazione che dalla Siberia alla Terra del fuoco consentono al mondo contemporaneo di funzionare in ogni sua forma[2] sono il cuore della città del futuro, sicché il suo funzionamento si radica nella combinazione di *Internet of Things* (IoT)[3], *big data*[4], *ubiquitous computing*[5] e *cloud*[6]. Tutti questi elementi sono le vere e proprie architetture su cui poggia la città (ideale) intelligente, ed hanno il compito di rendere la macchina urbana ottimizzabile e, soprattutto, controllabile. Osservando singolarmente ogni componente della *smart city* si può notare come il comun denominatore non sono solo i dati, ma anche i rischi alla tutela dei diritti fondamentali degli individui.[7] Difatti, è nelle vulnerabilità di questi singole architetture che si sostanziano le questioni aperte sulla regolazione della *smart city*. In altre parole, si ritiene che il punto d'indagine non debba condannare la tecnologia per avere modificato gli spazi urbani

[1] Come evidenziano numerosi studi, tra il 2000 e il 2015, le città sono cresciute dell'1,5% all'anno in termini di superficie. La crescita della superficie coperta dalle città è stata maggiore nei Paesi a basso reddito (2,6%), che in quelli a reddito medio (2,6%), rispetto ai Paesi a medio reddito (1,9% nei Paesi medio-bassi e 1,5% nei Paesi medio-alti) o ai Paesi ad alto reddito (1%) (EC OECD, 2020). Si faccia riferimento al *Population data booklet* elaborato dallo UN Department of Economic and Social Affairs, UN Habitat.

[2] Il ruolo che il contesto digitale ha assunto negli ultimi anni è quanto mai evidente alla luce del cruciale supporto che l'intera rete è stata in grado di fornire nei momenti più bui della pandemia da COVID-19.

[3] Si veda, *ex multis,* L. Atzori - A. Iera - G. Morabito, *Understanding the Internet of Things: Definition, Potentials, and Societal Role of a Fast Evolving Paradigm*, in *Ad Hoc Networks*, 56, 2017, 122 ss.

[4] Come è noto, i *big data* sono identificabili attraverso le c.d. "tre v": volume, varietà, velocità. L'analisi dei *big data* consiste nell'elaborazione automatizzata in cui grandi insiemi di dati vengono analizzati da algoritmi in modi nuovi e imprevisti per trovare modelli e correlazioni tra gli insiemi di dati, producendo così nuove conoscenze e informazioni su individui, gruppi o società in generale e informazioni su individui, gruppi o sulla società in generale. Si veda in particolare R. Kitchin - G. McArdle, *What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets*, in *Big Data & Society*, 3(1), 2016.

[5] Concetto utilizzato dalla letteratura per indicare la capacità assertiva e osservativa degli oggetti interconnessi con e nella vita degli individui. Tale struttura può essere identificata con il nome di «*everyware*», come descritto *ante litteram* in W. J. Mitchell, *E-Topia: «Urban Life, Jim—But Not As We Know It»*, Cambridge (MA), 1999.

[6] Definito dal National Institute of Standards and Technology (NIST) in *Final Version of NIST Cloud Computing Definition Published*, 25 ottobre 2021 *«a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction»*.

[7] A tal riguardo, si rimanda anche alla puntuale analisi di Lilian Edwards, che muove, appunto, da una considerazione dei singoli rischi associati agli IoTs e al *cloud* per profilare gli aspetti di maggiore criticità per la privacy degli individui. L. Edwards, *Privacy, Security and Data Protection in Smart Cities,* in *European Data Protection Law Review,* 2 (1), 2016, 28 ss.

e aver esposto i cittadini a ulteriori rischi. Questi ultimi sono ben radicati nelle singole tecnologie, tutt'oggi in commercio, rintracciabili nelle case e negli uffici di molti, che consentono a ben vedere il funzionamento della città intelligente. D'altro canto, gli elementi virtuali non possono prescindere dall'esperienza fisica, sicché i «flussi non sostituiscono gli spazi e i bit non rimpiazzano gli atomi»[8]. Proprio perché si sta assistendo alla creazione di uno spazio ibrido, a cavallo tra digitale e reale, sta venendo a formarsi un "non luogo" dove tecnologia e spazi fisici si incontrano, i cittadini vengono posti al centro di una vera e propria rivoluzione in cui si interfacciano non solo con la dimensione prettamente atomica, ma anche con gli elementi digitali che a mano a mano popolano la città del futuro. Orbene, il processo evolutivo della *smart city* non riguarda solamente l'urbanizzazione, ma tocca nel profondo il cittadino, il quale, già fortemente contaminato dalle moderne tecnologie digitali, si trova a vivere il contesto urbano in modo differente.[9]

Alla luce di quanto premesso, è evidente che la corsa alla digitalizzazione dello spazio urbano stia coinvolgendo ogni settore, pubblico e privato, portando alla luce una serie di riflessioni che concernono sicuramente il mercato, ma anche il nuovo assetto di poteri. In questo contesto, è richiesto al costituzionalista di interrogarsi su talune tematiche che discendono dall'interazione con questo nuovo spazio, dove digitale e reale sono posti su piani quanto meno paralleli. Difatti, è innegabile che la città, così come ogni altro aspetto legato alla quotidianità degli individui, abbia subito una forte influenza derivata e causata dalla digitalizzazione grazie alla costituzione di un sistema in cui gli algoritmi sono utilizzati per raccogliere, collezionare e organizzare i dati dei cittadini al fine di prendere ogni tipologia di decisione[10]. Le problematiche legate alla realizzazione, nonché alla regolazione, della città intelligente non fanno altro che amplificarne delle altre che guardano in senso ancor più ampio alla traduzione nello spazio digitale delle garanzie tradizionalmente godute dagli individui nel mondo reale. Dunque, si profila una problematica di bilanciamento tra due perni, la protezione dei diritti e gli interessi di investimento, tra protezione della riservatezza e incoraggiamento alla circolazione dei dati. In questo dualismo, che a ben vedere ha sempre caratterizzato il sistema normativo comunitario della protezione dei dati personali[11], si inseriscono anche le ultime proposte normative del legislatore europeo. Quest'ultimo, anche attraverso il *Digital markets act*[12] e il *Data Act*[13], sta muovendo da un sistema tutto incentrato sul controllo e sull'*accountability*, a uno più aperto, che possa favorire e

[8] C. Ratti, *La città di domani. Come le reti stanno cambiando il futuro urbano,* Torino, 2017, spec. 17.

[9] Si veda nel merito S. Ranchordás, *Nudging citizens through technology in smart cities*, in *International Review of Law, Computers & Technology*, 34 (3), 2020, 254 ss.

[10] J. Danaher, *The Threat of Algocracy: Reality, Resistance and Accommodation,* in *Philosophy & Technology*, 29 (3), 2016, 245 ss.

[11] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Si veda, in particolare, il considerando 7.

[12] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[13] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Brussels, 23.2.2022 COM(2022) 68 final.

incrementare la circolazione dei dati. In questo nuovo sistema, che sarà la necessaria benzina per permettere alle città intelligenti di ulteriormente svilupparsi, come si evidenzierà nella seconda parte di questo contributo, si stanno impiantando una serie di diritti e obblighi che erano già stati previsti nel regolamento (UE) 2016/679[14], come la portabilità, e che, sulla base di determinati presupposti, riguarderanno sia i dati personali sia quelli non personali. La circolazione dei dati diviene, dunque, in questo contesto, la principale infrastruttura della città intelligente. D'altro canto, come si premetteva, da questo quadro emergono delle chiare problematiche di sicurezza dei dati raccolti e di garanzia di protezione da interferenze esterne. Pertanto, la profilazione dei cittadini, la protezione della loro riservatezza, la creazione di un sistema di *governance* attuale che sia consapevole dei rischi ma anche delle opportunità, sembrano le principali sfide che si ritiene necessario affrontare per salire consapevolmente sul treno dell'innovazione.

A partire, dunque, da una cornice generale ove si è cercherà di porre in evidenza come i diritti individuali vengono messi ulteriormente in discussione nell'assetto della città intelligente, l'analisi riguarderà nel particolare la sfida posta al sistema della privacy europeo. La tematica in esame verrà trattata considerando anche la diffusione di questo modello anche al di fuori dell'ambito comunitario. In secondo luogo, si evidenzierà come in questo spazio dove i confini tra pubblico e privato sono sempre più labili, il legislatore è chiamato ad assumere un ruolo prospettico, onde evitare una stagnazione in modelli normativi e tecnologici che faticano a stare al passo dell'evoluzione del digitale.

2. Quale riservatezza nella città intelligente: spunti di riflessione

Da un punto di vista prettamente definitorio, la città intelligente indica una serie di strategie di pianificazione urbanistica correlate all'innovazione e in particolare alle opportunità offerte dalle nuove tecnologie della comunicazione per migliorare la qualità della vita dei cittadini, alimentando una crescita economica sostenibile, attraverso una sapiente gestione delle risorse naturali e ricorrendo ad una *governance* partecipativa[15]. È indubbio il fatto che l'innovazione e la tecnologia rappresentano degli importanti alleati nella lotta al cambiamento climatico[16], nell'ottimizzazione degli spazi urbani, nello sviluppo ed utilizzo sostenibile di tutte le fonti di energia, nonché nella garanzia

[14] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati). Qui di seguito, GDPR.

[15] F. Toni, *Smart city: innovazione e sostenibilità*, in *EAI Energia, Ambiente, Innovazione*, 5, 2021, 35 ss.

[16] A tal riguardo, si rimanda ai *17 UN Sustainable Goals*, ossia una serie di iniziative che l'Organizzazione delle Nazioni Unite intende intraprendere per provocare un cambiamento entro il 2030, nella prospettiva di realizzare un futuro migliore per gli individui. Peraltro, numerose organizzazioni tra cui la AI For Good hanno evidenziato come ciascun obiettivo può essere effettivamente realizzato e accelerato grazie all'impiego di tecnologie automatizzate e AI, nel particolare. Si veda *AI 4 Good* consultato in data 25 marzo 2022.

di maggiore sicurezza. Ebbene, si ritiene che ciò debba imprescindibilmente passare attraverso un ripensamento dell'assetto rubano, della mobilità dei cittadini[17] e delle infrastrutture ICT. Detto passaggio può avvenire mettendo in relazione le infrastrutture materiali con il capitale umano, intellettuale e sociale, facendo sì che quest'ultimo assuma un ruolo centrale nel modello di pianificazione urbana intelligente. Infatti, almeno astrattamente, le *smart city* sono città in cui uno strato tecnologico viene sovrapposto all' intelaiatura urbana esistente, consentendo ai suoi cittadini e utenti di connettersi alla rete, interagire tra loro e con altri attori, quali la pubblica amministrazione, fornitori di beni e servizi e soggetti privati. Nello specifico, il fine delle città intelligente è quello di condurre ad un generale innalzamento della qualità dei servizi offerti al cittadino, quali il trasporto (pubblico e non), la distribuzione energetica, la cura della persona, la salute, il monitoraggio dell'ambiente, la risposta alle emergenze e le attività sociali e, più in generale, per le imprese coinvolte, la realizzazione di nuovi modelli di *business* sempre più efficaci e mirati sulla figura del cittadino-utente-cliente. In sostanza, le fasi del processo di raccolta dei *big urban data* dovrebbero creare meccanismi di sviluppo virtuosi sia in relazione ai servizi che alla riprogettazione della città del futuro[18].

Come si premetteva, lo spazio urbano *smart* è considerabile un punto di incontro tra mondo virtuale e mondo materiale, tra digitale e analogico, all'interno del quale interagiscono sia soggetti biologici che artificiali[19]. Nonostante, dunque, le menzionate opportunità, occorre chiedersi se un tale assetto sia in grado di essere non solo funzionale, ma anche tutelante dei diritti fondamentali dei cittadini, permettendo loro di vivere e partecipare liberamente alla vita della comunità[20].

Difatti, è possibile notare che l'opera di espansione dei diritti nel digitale[21] raggiunge la sua pienezza nel contesto della città intelligente. Come è già stato possibile osservare in riferimento ad altri spazi virtuali, quali, ad esempio, i *social network*, questi ultimi hanno acquisito un ruolo eminentemente pubblico, assimilabile a quello che le piazze esercitavano nella dimensione atomica[22]. Ed è, peraltro, attraverso di essi che si rea-

[17] Nelle parole di Musa, «*the goal of building a smart city is to improve the quality of life by using technology, to improve the efficiency of services and meet residents' needs.* [...] *The purpose of building smart cities is to make the lives of the residents easier and safe»,* S. Musa, *Smart Cities - A Roadmap for Development*, in *J. Telecommun. Syst. Manage,* 5 (3), 2016.

[18] G. Pedrazzi, *Big Urban Data nella smart city*, in G.F. Ferrari (a cura di), *La prossima città*, Milano, 2017, spec. 557-576.

[19] A tal riguardo, si rimanda a L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2012*,* spec. 106, chiarisce che «stiamo lentamente accettando l'idea per cui non siamo agenti newtoniani isolati e unici, ma organismi informazionali, inforg, reciprocamente connessi e parte di un ambiente informazionale (infosfera), che condividiamo con altri agenti informazionali».

[20] A tal proposito, si veda l'analisi di P. Cardullo - C. Di Feliciantonio - R. Kitchin, (a cura di), *The right to the smart city*, Bingley (UK), 2019, spec. 27.

[21] A tal riguardo, si rimanda all'annoso dibattito guidato da F.H. Easterbrook, *Cyberspace and the Law of the Horse,* in *University of Chicago Legal Forum,* 207, 1996. Peraltro, detto dibattito è alimentato da amplissima e anche recente letteratura, circa la necessità di creare, ovvero, d'altro canto, adattare la compiutezza dei diritti tradizionalmente garantiti alle nuove sfide del digitale.

[22] Giova menzionare il dibattito anche statunitense sul tema nell'ambito del quale la qualificazione giuridica dei social network «costituisce un nodo da cui dipende l'effettività della tutela garantita dal Primo Emendamento», M. Bassini*, Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione,* in *Rivista Italiana di Diritto dell'Informatica*, 2, 2021. Peraltro, la recente pronuncia nel

lizzano i diritti democratici dei cittadini, come nel caso della libertà di assemblea o di associazione. Nella *smart city*, al contrario, ogni aspetto tende invece a essere governato "digitalmente" da soggetti privati o da tecnologie sviluppate da quest'ultimi, facendo di quegli spazi essenzialmente pubblici, degli «*pseudo private places*»[23].

In questo inedito contesto, dunque, i diritti che per loro natura rappresentano la massima garanzia statale, – e, precipuamente, il diritto all'informazione; il diritto di libertà di espressione; il diritto alla cultura; il diritto all'identità e all'autonomia; il diritto all'autodeterminazione; il diritto alla privacy – vengono materialmente mediati dai soggetti privati. Si realizza, dunque, un'inscindibile unione tra la persona *offline* e *online*. Tale aspetto, seppur non nuovo, in quanto tematica che emerge anche dai profili legati alla c.d. "società algoritmica"[24], profila per il costituzionalista una serie di sfide legate non solo alla garanzia di diritti fondamentali all'interno delle città, ma anche alla risoluzione del delicato rapporto attori pubblici e attori privati. Infatti, è necessario comprendere sia come permettere anche tramite strumenti normativi la reale partecipazione del cittadino, sia come mitigare e regolare l'ingerenza dell'attore privato nei progetti di pianificazione urbana[25]. In particolare, è necessario chiedersi: in una città che tutto vede, tutto processa, come può darsi il diritto all'identità, il diritto all'autodeterminazione, il diritto alla privacy? È inevitabile che l'individuo stesso diventi parte integrante dell'ambiente ibrido assumendo allo stesso tempo, il ruolo di *user*, cliente e cittadino, peraltro, non sempre consapevolmente[26]. Per tale ragione, è necessario trovare un bilanciamento, in quanto l'integrazione di intelligenze artificiali e robotica nel tessuto urbano per fini di *governance* implica la necessaria adozione di cautele estreme, onde evitare, la creazione di uno sregolato sistema di sorveglianza a scapito dei diritti dei singoli[27]. La sfida non ricade solamente sull'attore privato che deve avere chiaramente un ruolo prominente nel progettare sistemi tecnologici rispettosi dei diritti umani. Tuttavia, è altresì vero che il principale ruolo è rivestito dai pubblici poteri, che vengono chiamati a dotarsi di un nuovo sistema di *governance* ove le tradizionali risorse del diritto devono attagliarsi a scenari inediti, come si dirà nella seconda parte di questo contributo.

In merito, dunque, alla tutela dell'identità di ognuno nello spazio intelligente, un note-

caso *Joseph Biden, Jr., President of the United States, et al., v. Knight First Amendment Institute at Columbia University,* et al., 593 U. S. BBBB (2021), e, in particolare, la *concurring opionin* di Justice Thomas, è stata in grado di portare alla luce un'idea di social network intesi come "*common carrier*", ossia *"essential facilities"*. In altre parole, vengono intesi come infrastrutture essenziali per l'esercizio e l'alimentazione del dibattito pubblico, considerando spazi come Twitter, non solo "semplici" piattaforme private ma "*public forum*".

[23] D. Mac Sithigh, *Virtual walls? The law of pseudo-public spaces*, in *International Journal of Law in Context*, 8 (3) 2012, 394 ss.

[24] Cfr. J. Danaher, *he Threat of Algocracy,* cit.

[25] C. Ratti, *La città di domani. Come le reti stanno cambiando il futuro urbano,* cit.

[26] L. Taylor - C. Richter – S. Jameson - C. Perez de Pulgar, *Customers, users or citizens? Inclusion, spatial data and governance in the smart city. Inclusion, Spatial Data and Governance in the Smart City,* in *SSRN*, 2016.

[27] Per l'appunto, senza specifiche regole si rischia, di «alimentare un regime della sorveglianza tale da rendere l'uomo una non-persona, l'individuo da addestrare o classificare, normalizzare o escludere». Indicativo in questo senso è l'allarme lanciato dal presidente dell'Autorità garante per la protezione dei dati personali italiano che nell'ambito dei modelli di *smart city* ha addirittura paventato il pericolo di un "nuovo totalitarismo digitale", A. Soro, '*Discorso del Presidente Antonello Soro'*, Relazione 2018, 5.

vole valore deve essere dato alla *privacy*. È proprio nella facoltà di aggirarsi liberamente per lo spazio urbano, senza il rischio di eccessive intrusioni nella sfera privata[28], che si sostanzia l'ancillare concezione della *privacy*, così come venne intesa da Warren e Brandeis[29].

Giova rammentare, a tal proposito, che in ambito europeo il percorso di costituzionalizzazione ha compiuto un ulteriore passo con l'adozione del GDPR. Il primo obiettivo è stato quello di garantire il diritto alla protezione dei dati personali in quanto diritto fondamentale degli interessati. Nonostante l'elevato grado di salvaguardia di cui questi godono nel panorama comunitario, vale la pena evidenziare come questo diritto non goda di una tutela assoluta ma che «de[bba] essere considerato in relazione alla sua funzione nella società e bilanciato con altri diritti fondamentali, conformemente con il principio di proporzionalità»[30]. Infatti, tali diritti possono essere limitati per proteggere altri diritti costituzionali o per scopi legittimi. Taluni dei principi cardine del GDPR soggiacciono ad alcune considerazioni di rischio, o di cautela, nell'affrontare trattamenti di dati personali che possano eccessivamente limitare le libertà degli individui. A tal proposito, il Considerando 39 stabilisce il principio della minimizzazione[31]. Come suggerisce lo stesso termine, è richiesto di ridurre non solo in termini quantitativi, ma anche qualitativi, i confini del trattamento del dato personale, ma anche di adoperare delle cautele, attraverso misure come la pseudonimizzazione per diminuire la facilità con cui i dati possono essere collegati agli individui. Almeno in astratto, dunque, la *smart city* mal si presta a un contesto improntato alla minimizzazione. La raccolta di dati attraverso *IoT*, la modalità di trattamento automatizzata di grandi quantità di informazioni attraverso tecniche di *big data analytics* e la conservazione su *cloud* sono solo alcuni degli elementi che si crede possano mettere in crisi il sistema del GDPR all'interno della città intelligente[32].

Sebbene vi siano delle proposte su come creare un bilanciamento tra esposizione e riservatezza, tra intrusione e *privacy*[33], queste non appaiono del tutto convincenti, poiché ancora relegate su un piano di *compliance* che poco tiene in considerazione l'impatto sui diritti fondamentali. Proporre come soluzione un *data protection impact assessment* su larga scala, non appare logico rispetto alla dimensione tanto quantitativa quanto

---

[28] M. Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology*, in *Connecticut Law Review*, 49 (5), 2017, 1591.

[29] S. D. Warren - L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review,* 4, 1890.

[30] GDPR, considerando 4.

[31] Considerando 39: «È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento».

[32] Per una maggiore riflessione sull'argomento, G. Vojković - T. Katulić, *Data Protection and Smart Cities,* in J.C. Augusto (a cura di), *Handbook of Smart Cities,* Berlino, 2021.

[33] K. Finch - O. Tene, *Smart Cities: Privacy, Transparency, and Community*, in E. Selinger - J. Polonetsky - O. Tene (a cura di), *Cambridge Handbook of Consumer Privacy*, Cambridge (MA), 2018. Accanto alle questioni legate alla *data protection*, si profilano anche le problematiche che interessano i *bias* algoritmici e i rischi di discriminazione, derivanti dalla creazione di algoritmi non sempre trasparenti.

qualitativa della città intelligente. Al contrario, è importante sottolineare la necessità di riflettere, da un lato, sulle singole situazioni di rischio condotte dai singoli elementi tecnologici che si affastellano nello spazio urbano (del presente) e del futuro; dall'altro, occorre ripensare taluni principi della *data protection*, e, in particolare, il sistema di cui all'art. 6 del GDPR, e la raccolta del consenso dell'interessato[34]. Pertanto, si impone una riflessione organica che guardi all'interezza del diritto alla *privacy* e alla protezione dei dati personali in un ambiente sempre più complesso, in cui il tessuto urbano si trasforma, al fine di limitare *ex ante* fenomeni di sorveglianza e controllo indiscriminati.
A tal riguardo, questa operazione trasformativa travolge a pieno la riservatezza e la permeabilità dei requisiti che l'hanno elevata a Primo Emendamento europeo. Difatti, in questo novellato contesto anche la tenuta degli standard precedentemente applicati è aspetto di rilevante importanza se si vuole assicurare la replicabilità delle garanzie ai diritti individuali. La fortezza europea della privacy è, dunque, ancora una volta assediata da nuove sfide che mettono in discussione la replicabilità interna ed esterna, nonché la sua complementarità rispetto alle sempre nuove sfide della tecnologia. Difatti, il mondo cui ci si sta affacciando – e le iniziative europee sembrano andare in questa direzione –, che, peraltro, è l'unico mondo in cui possa esistere una vera e propria *smart city*, reclama la circolazione dei dati, la portabilità e l'interoperabilità come suoi cardini.
Conclusi questi brevi cenni, occorre iniziare a rispondere alla domanda che, seppur non ancora esplicitata, necessariamente sorge, una volta compresa la dimensione d'indagine: è lo standard europeo in grado di farsi portatore di un sistema globale, replicabile nel contesto della *smart city*? A tale complesso quesito si tenterà di rispondere nel prossimo paragrafo.

2.1 (segue) La fortezza europea della privacy alla prova della *smart city*

La privacy degli individui e la protezione della loro riservatezza sono due delle sfide cardinali dell'epoca moderna. L'esposizione alla raccolta di massa di dati personali è un aspetto notissimo, così come le garanzie che ovunque, ma soprattutto in Europa[35], sono state messe in atto per assicurare uno dei diritti fondamentali protetti dalla Carta di Nizza[36]. Pertanto, è importante considerare come e se tale diritto possa trovare applicazione nella *smart city*. La *datafication* è una caratteristica centrale di ogni città intelligente, indipendentemente dalla prospettiva che si adotta per definirla e progettarla. L'incessante raccolta e trattamento di dati che provengono da molteplici fonti mette a rischio la protezione dei dati personali e la loro confidenzialità. In secondo luogo, si

[34] G. De Gregorio, *Città, cittadino e diritti digitali*, in G.F. Ferrari (a cura di), *Smart city. L'evoluzione di un'idea*, Milano, 2020, 493 ss.

[35] Si fa riferimento, in particolare, a quella cultura della privacy che ruota attorno all'importanza assegnata a questo diritto nelle scelte di *policy* delle istituzioni comunitarie. Peraltro, Bilyana Petkova ha brillantemente riassunto tale paradigma costituzionale nell'espressione «*privacy as EU First Amendment*», proprio a sancire la centralità della protezione dei dati personali in Europa. B. Petkova, *Privacy as Europe's First Amendment*, in *European Law Journal*, 25(2), 2019, 140 ss.

[36] Art. 7 e art. 8 Carta dei diritti fondamentali dell'Unione europea (2000/C 364/01).

rinviene un problema di privacy biometrica rispetto alla propria salute, alle caratteristiche fisiche in grado di identificare il cittadino; ma anche una privacy "territoriale", ossia riguardante lo spazio personale, gli oggetti e la proprietà. Infine, si rileva un problema di privacy delle comunicazioni e delle transazioni. Queste preoccupazioni sorgono perché le città intelligenti collocano sensori nell'arredo urbano, dai cestini dei rifiuti ai lampioni, tracciano gli identificatori telefonici e i sistemi di mobilità intelligente, basandosi su ampi apparati di geolocalizzazione[37]. Perché, dunque, è rilevante parlare di *privacy* della *smart city*, anziché di *privacy* degli IoT, o degli *smart objects*? La risposta è necessariamente che la città intelligente rappresenta una sommatoria di tutte queste circostanze, come si premetteva in introduzione.

La *smart city* diventa un perfetto strumento di raccolta dei dati comunicati e condivisi dai cittadini, ove i dati non vengono solo venduti per interessi commerciali, ma vengono anche utilizzati per plasmare i comportamenti e il carattere dell'essere umano[38]. Sostanzialmente, nella città intelligente, i sistemi di sorveglianza, come circuiti di telecamere sempre funzionanti, diventano parte integrante dello sfondo urbano integrandosi nella quotidianità del cittadino[39].

Dunque, occorre quanto meno soffermarsi sulle *externalities* che vengono in evidenza dal momento in cui si basa il funzionamento della vita – e, dunque della città – *smart* sul flusso e sul trasferimento dei dati in input e in output. L'ambiente intelligente, come si diceva nel paragrafo precedente, creano le condizioni perché si possa pienamente parlare di sistema *onlife*: vale a dire l'esperienza di una realtà iper-connessa ove è impossibile scindere tra identità analogica e digitale[40].

La tutela, dunque, di questo spazio, almeno in Europa, pare essere ancorata alla disciplina a protezione dei dati personali che, com'è noto, in questo contesto va ben oltre il diritto derivato, in quanto è tutelata anche come diritto fondamentale o quasi "costituzionale" ai sensi della Carta dei diritti fondamentali dell'Unione europea. In particolare, gli artt. 7 e 8 della Carta prevedono, in modo unico, due diritti distinti, ossia la protezione della vita privata (privacy) e la protezione dei dati personali: una novità rispetto ai tradizionali strumenti di tutela dei diritti umani e, soprattutto, la prima volta in cui la protezione dei dati ha acquisito lo status di diritto fondamentale a sé stante nell'ambito degli strumenti normativi internazionali esistenti[41].

---

[37] Si veda S. Ranchordas, *Cities of God: Smart Cities and Surveillance,* in *VerfBlog,* 2021.

[38] J. Sadowski - F. Pasquale, *The Spectrum of Control: A Social Theory of the Smart City*, in *U. of Maryland Legal Studies Research Paper*, 26, 2015.

[39] Come si vedrà, non sorreggono, peraltro, nemmeno i limiti imposti dal GDPR in quanto non tutti i dati raccolti nelle città intelligenti saranno qualificabili come dati personali, poiché molti di essi si riferiscono alla gestione della folla, ai dati urbani o ambientali (ad esempio, i livelli di inquinamento atmosferico, la densità del traffico, il livello dell'acqua). Inoltre, parte dei dati raccolti diventerà disponibile sotto forma di dati aperti che consentiranno molteplici miglioramenti urbani. E, inoltre, e città intelligenti non raccolgono solo dati sulla città e i suoi arredi (ad esempio, i sondaggi delle lampade) ma anche sui loro cittadini. Di questi ultimi non sono raccolti solamente i dati personali, bensì anche i c.d. metadati, ossia quelle informazioni che non sono riconducibili a un interessato identificato o identificabile, ma che forniscono ad ogni modo preziosi dettagli sul cittadino.

[40] Detto termine, è un neologismo coniato dal filosofo Luciano Floridi, di cui viene data ampia descrizione e spiegazione nel volume *The onlife manifesto: Being human in a hyperconnected era*, Berlino, 2015.

[41] Y. Ivanova, *The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World,*

Bisogna, dunque, domandarsi: quale standard di tutela verrà applicato nella città digitale? E, soprattutto, vivendo in un mondo globalizzato, quale standard di protezione viene assicurato alla persona fisica e digitale nella città *smart*? Domande che sono tutt'altro che banali se si tiene in considerazione l'immensa problematica che tutt'ora soggiace al trasferimento dei dati personali verso paesi terzi e la nota casistica che ha soprattutto coinvolto gli Stati Uniti d'America, dove il conflitto si è giocato proprio sul livello di protezione che viene assicurato agli individui da illecite interferenze nella loro vita privata. Tale aspetto viene ivi in rilievo non solo con riguardo alla programmazione delle architetture-fondamenta della *smart city*; le domande su cui il costituzionalista deve interrogarsi riguardano altresì l'interazione degli utenti-cittadini con gli strumenti tecnologici che fisicamente consentiranno alla città intelligente di materializzarsi. A tal riguardo, emerge un rilevante problema riguardante l'accompagnamento e l'educazione all'utilizzo di questi ultimi, giacché è inimmaginabile delegare tale aspetto alla maieutica. Non essendo, tuttavia, la sede per affrontare questo aspetto, la presente analisi si interrogherà in merito alla scelta dello standard cui elevare la tutela della riservatezza pare rilevante se si pensa sia alla programmazione *ex ante* sia all'interazione uomo-tecnologica *ex post*.

Chiarire lo standard e l'adeguatezza delle tutele ha una cruciale significanza nell'ambiente della città tecnologica sotto molteplici punti di vista. La necessità di chiarire quale standard di protezione applicare è inerentemente connessa dapprima ai dati con cui gli elementi architettonici della città *smart* funzionano; in secondo luogo, dal livello di tutela assicurato, discende altresì la possibilità di poter azionare detti diritti e reclamarli in via diretta dinanzi a un *provider* o a un organo giudiziario. Pertanto, le problematiche che ancora permangono con riguardo al trasferimento dei dati personali verso paesi terzi è un aspetto che acquista un'importanza sostanziale non solo a livello di *compliance,* ma proprio nell'ottica di garantire la protezione orizzontale dei diritti degli individui.

Ebbene, anche se un livello di protezione adeguato non richiede necessariamente che i Paesi terzi adottino standard identici, le persone fisiche devono comunque godere di un grado di protezione che sia "sostanzialmente equivalente" a quello offerto dal diritto dell'UE[42]. L'equivalenza nel grado di protezione è richiesta, secondo la Corte, in virtù di un'interpretazione della direttiva 95/46/CE alla luce della Carta di Nizza.

in *SSRN,* 2020.

[42] Si vedano in tal senso anche le Conclusioni dell'Avvocato Generale in *Maximillian Schrems c Data Protection Commissioner (Schrems I)*. In particolare, al § 141 argomenta: «è per questo motivo che ritengo che la Commissione possa constatare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, che un paese terzo assicura un livello di protezione adeguato solo qualora, al termine di una valutazione di insieme del diritto e della prassi nel paese terzo in questione, essa sia in grado di dimostrare che tale paese offre un livello di protezione sostanzialmente equivalente a quello offerto da tale direttiva, anche se le modalità di tale protezione possono essere diverse da quelle generalmente vigenti all'interno dell'Unione». Pertanto, è stato in primo luogo l'Avvocato Generale a manipolare l'interpretazione della direttiva. Dopo aver fatta sua questa argomentazione cruciale, peraltro, l'AG sostiene al § 142: « Benché il termine inglese «*adequate*» possa essere inteso, dal punto di vista linguistico, nel senso che esso designa un livello di protezione appena soddisfacente o sufficiente, ed avere pertanto un campo semantico diverso dal termine francese «*adéquat*», si deve osservare che il solo criterio che deve guidare l'interpretazione di tale termine è l'obiettivo consistente nel conseguimento di un livello elevato di protezione dei diritti fondamentali, come richiesto dalla direttiva 95/46».

Giova, quindi, rammentare che, nel contesto europeo, la Carta, anche a grazie all'opera creativa della Corte di Giustizia, è lo strumento giuridico utile per l'avanzamento del livello di tutela richiesto dal diritto dell'UE attraverso un'interpretazione elastica del parametro di "adeguatezza". Questo approccio è tutt'altro che retorico in quanto la Corte di giustizia era ispirata dall'entrata in vigore della Carta di Nizza a rivisitare le norme contenute nella direttiva sulla protezione dei dati personali e a rinnovarne l'interpretazione. Pertanto, il significato delle norme della direttiva andava mutando e, coerentemente, il livello di protezione accordato ai dati personali divenne molto più ampio anche prima dell'adozione del GDPR.

Per rispondere alla domanda che è stata precedentemente posta, ossia la replicabilità delle tutele assegnate all'individuo dalla normativa sulla protezione dei dati personali in altre giurisdizioni, occorre necessariamente guardare all'estensione del campo di applicazione del diritto dell'UE, secondo l'interpretazione della Corte di Giustizia.

Tale aspetto è di assoluto rilievo nelle notissime sentenze *Google Spain*[43] e *Schrems I*[44], ove la Corte di giustizia applicò le norme dell'Unione, alla luce dei diritti fondamentali tutelati dalla Carta di Nizza, al di là dei confini europei, affermando così la propria sovranità digitale. In *Google Spain*, attraverso un'interpretazione espansiva della nozione di stabilimento, la Corte limitò il potere dei gestori di motori di ricerca, come attori privati, di condurre le loro attività economiche su scala globale senza essere soggetti alle normative dei Paesi in cui essi operano[45]. Similmente, in *Schrems I*, la valutazione effettuata dalla Corte di giustizia con riferimento alla *Safe Harbour Decision* era mossa eminentemente dalla necessità di assicurare che la nozione formale di territorio e giurisdizione non minassero sostanzialmente l'effettiva protezione dei diritti fondamentali nell'ecosistema digitale.

Ciò detto, occorre considerare se l'attivismo giudiziario possa mutare alla luce dell'ambito di applicazione territoriale del GDPR. In questa prospettiva, è interessante considerare una decisione della Corte Suprema della Columbia Britannica del 2014[46], resa prima che la Corte di giustizia, in *Google c. CNIL*[47], adottasse una nuova posizione chiarificatrice del fatto che il diritto all'oblio contenuto nell'art. 17 GDPR non può essere applicato al di fuori dell'UE. Nella sua decisione, la Corte Suprema della Columbia Britannica – menzionando espressamente il caso *Google Spain* – si occupò del problema dell'applicazione extraterritoriale della protezione accordata a livello domestico ai dati personali e, più in generale, della mancanza soluzioni efficaci elaborate su base meramente locale (e non necessariamente nazionale).

L'attore aveva richiesto un'ingiunzione provvisoria che proibisse a Google di mostrare i risultati di ricerca connessi a sito che web accusato di violare i diritti di proprietà

[43] CGUE, C-131/12 *Google Spain SL e Google Inc c Agencia Española de Protección de Datos, Mario Costeja González* (2014).

[44] CGUE, C-362/14, *Maximillian Schrems c Data Protection Commissioner (Schrems I)* (2015), § 38.

[45] Sulle conseguenze di queste decisioni si veda C. Docksay, *The EU Approach to the Protection of Rights in the Digital Environment: Today and Tomorrow – State Obligations and Responsibilities of Private Parties – GDPR Rules on Data Protection, and What to Expect from the Upcoming ePrivacy Regulation*, in Consiglio d'Europa, *Human Rights Challenges in the Digital Age: Judicial Perspectives*, Strasburg, 2020, 47 ss.

[46] BCSC, *Equustek Solutions Inc v Jack,* [2014], 1063.

[47] CGUE, C-507/17, *Google c CNIL* (2019).

intellettuale dell'attore stesso. Google aveva obbedito all'ordine, anche se la rimozione aveva riguardato soltanto la versione canadese del motore di ricerca (google.ca). Pertanto, i *link* al sito in questione erano ancora forniti da altri motori di ricerca non canadesi operati da Google. La Corte Suprema Canadese della Columbia Britannica, di conseguenza, ordinò a Google di rimuovere le pagine di alcuni siti web dai risultati della ricerca su base globale e non meramente nazionale. Il caso, pertanto, concerneva un ordine di rimozione a livello mondiale, il che costituiva in tutta probabilità un tentativo di rispondere al problema della frammentazione della protezione giuridica connessa alla natura locale delle giurisdizioni impegnate nell'applicazione dei diritti fondamentali in gioco[48].

La Corte d'Appello della Columbia Britannica rigettò l'appello di Google, sostenendo che la Corte aveva giurisdizione territoriale nel pronunciare quella decisione non solo in Canada, ma altresì al di fuori del suo territorio[49].

In maniera simile a *Google Spain*, il problema concerneva la necessità di fornire un'effettiva tutela dei diritti dell'attore e di prevenire il rischio che la legge venisse aggirata attraverso il ricorso all'ambiente online. Se in *Google Spain* l'obiettivo era propriamente quello di proteggere i diritti dei cittadini dell'UE, le corti canadesi si concentrarono invece su considerazioni legate all'equità[50]. Secondo la Corte la soluzione adottata da Google era del tutto insoddisfacente dal punto di vista degli attori[51]. Di conseguenza, la Corte ritenne essere in suo potere la possibilità di emanare un'ingiunzione contro terze parti, quand'anche stabilite in Paesi terzi, laddove le circostanze lo richiedano. Il fatto che un'ingiunzione di siffatto tipo non fosse mai stata emanata nei confronti di un gestore di un motore di ricerca, quale Google, richiedeva di procedere con cautela, ma non ostava alla competenza della corte canadese in tale materia[52]. Pertanto, se anche i siti dei convenuti fossero stati rimossi dalle ricerche condotte attraverso www.google.ca, gli utenti canadesi avrebbero comunque potuto ricorrere ai siti www.google.

---

[48] BCCA, *Equustek Solutions Inc v Google Inc,* [2015], 265.

[49] Google argomentò in particolare che, poiché operava online, la giurisdizione territoriale della corte canadese non doveva applicarsi a Internet. Qui, in particolare, è interessante osservare come la corte si sia basata sulla sentenza *Google Spain*, ove la stessa argomentazione addotta da Google non era stata accolta dalla CGUE. La Corte d'Appello della Columbia Britannica concluse infatti che, sebbene Google sostenesse di offrire un sito meramente passivo ai residenti della Columbia Britannica che vogliano operare una ricerca su Internet e che i suoi programmi generino in automatico i risultati della ricerca senza che Google sia attivamente coinvolto nel processo, in realtà i siti di ricerca su Internet gestiti da Google non erano in realtà veramente siti passivi di informazione. Infatti, non appena un utente inserisce alcune lettere o una parola nella barra di ricerca, Google anticipa la richiesta e offre un menù a tendina contenente alcuni suggerimenti di possibili *query*. Google inoltre vendeva pubblicità ai clienti residenti nella Columbia Britannica: anzi, aveva stipulato precipuamente un contratto di pubblicità con i convenuti e aveva pubblicizzato i loro prodotti fin all'udienza stessa. Si vedano §§ 47-48 e 50

[50] L'argomentazione delle corti della Columbia Britannica si basava sulla sez. 39 del *Law and Equity Act*. Secondo questa legge, le ingiunzioni possono essere emanate in tutti i casi in cui la corte ritenga giusto o conveniente emanare l'ordine, sulla base dei termini e delle condizioni che la corte stessa ritenga giuste.

[51] Al posto dei siti Internet deindicizzati, una quantità di nuovi siti era andata a sostituirli, avanzando in termini di *ranking*. I siti, argomentò la Corte, possono essere generati automaticamente, cosicché gli attori possono trovarsi a dover continuamente identificare nuovi URL da indicare a Google per chiederne la rimozione. Pertanto, uno schema di tutela che si basi sulla rimozione del singolo URL risultava inefficace.

[52] *Equustek Solutions Inc v Jack*, cit. §§ 72 e 133.

co.uk o www.google.fr per accedere a tali siti[53]. Google tentò di argomentare, tra l'altro, che le corti godono di una limitata giurisdizione entro i propri territori e che non possano imporre ordini aventi portata extraterritoriale ai gestori di motori di ricerca[54]. Tuttavia, poiché l'ambiente digitale difficilmente riesce a imporsi con barriere e confini, giacché il suo habitat naturale è globale, il caso in esame ha avuto il pregio di dimostrare la necessaria interlocuzione, anche per il tramite delle corti di merito e di legittimità nella scelta e applicazione dello standard di tutela più garantista. Difatti, la Corte canadese comprese che l'unico modo per assicurare che un'ingiunzione interlocutoria raggiunga i suoi obiettivi è che essa si applichi nel luogo in cui opera Google – e cioè a livello globale[55]. Avendo a che fare con Internet, il giudizio di bilanciamento doveva tenere in piena considerazione l'inevitabile scenario globale comportato dalla richiesta di un'ingiunzione a carico di un attore quale Google. Inoltre, la Corte sottolineò come l'ordine in questione non aveva lo scopo di rimuovere alcuna espressione rilevante, *prima facie*, per i valori della libertà in questione: si trattava invero di un ordine di deindicizzazione di siti che violavano diversi ordini giudiziali. In tal senso, la Corte ritenne che non fosse accettabile il principio in base al cui la libertà di espressione richieda di ammettere la facilitazione della vendita di beni illeciti[56].

Tutto questo *excursus* appare utile per comprendere il margine di replicabilità di detti diritti nel contesto della città *smart*, ove il confine tra azione *online* e azione reale semplicemente non esiste. Inoltre, l'ambito di applicazione extraterritoriale del GDPR codifica attualmente i tentavi della Corte digiustizia di assicurare un'effettiva protezione per i diritti dei propri cittadini sotto il profilo transnazionale. In particolare, l'art. 3, par. 2, GDPR può essere considerato il risultato di uno standard di protezione di alto livello per la privacy in Unione europea, che, nella società dell'informazione, non può più essere limitato esclusivamente al territorio europeo ma deve essere assicurato a livello globale.[57]

La conseguenza di tale norma è duplice. In primo luogo, essa concerne il problema della giurisdizione. In particolare, tutti i casi di trattamento di dati personali che ricadano nell'ambito di applicazione dell'art. 3, par. 2, GDPR saranno soggetti alla giurisdizione dell'Unione. Questo approccio permette di superare la dottrina dello stabilimento elaborata dalla Corte di giustizia in *Google Spain*, in quanto persino quegli enti che non siano stabiliti in UE potranno essere soggetti al GDPR. Ancora più importante

[53] Ivi, § 148.

[54] SCC, G*oogle Inc v Equustek Solutions Inc,* [2017], § 34.

[55] Tra l'altro, la maggioranza delle vendite operate dai siti dei convenuti avveniva proprio all'estero, cosicché, se l'ingiunzione fosse stata ristretta nel suo campo al solo territorio canadese o al sito google.ca, come richiesto da Google, il rimedio sarebbe stato incapace di prevenire un danno irreparabile. Secondo la Corte Suprema canadese, pertanto, non vi era alcuna equità nell'ordinare un'ingiunzione interlocutoria che non avesse alcuna prospettiva realistica di prevenire un danno irreparabile.

[56] Ivi, §§ 47-48.

[57] In particolare, l'art. 3, par. 2, GDPR recita: «il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure (b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione».

è tuttavia la seconda conseguenza, ovverosia l'estensione delle regole euro-unitarie sulla privacy al contesto globale – e questa è, piuttosto una questione di sovranità digitale. Se, come sottolineato sopra, la Corte di giustizia in *Schrems I* si è occupata degli standard di protezione presenti nel sistema statunitense atti a governare il trattamento di dati personali di cittadini dell'UE, ora il parametro operativo di riferimento potrà essere direttamente quello europeo, come definito dal GDPR.

Dunque, la natura transnazionale degli strumenti digitali, di cui la città *smart* appare essere un amplificatore, sembra essere incompatibile con i tentativi di "regionalizzazione", non solo della privacy, ma anche della tecnologia tout court, sicché questo processo deve tendere verso l'aumento di un sufficiente grado di tutela dei diritti fondamentali. Questo processo di regionalizzazione, che rappresenta il riflesso dell'amplificazione di un impulso regolativo da parte delle corti, potrebbe verosimilmente risultare in una frammentazione e, forse, balcanizzazione tecnologica e dei relativi strumenti giuridici che governano suddetti sistemi.[58]

È evidente che il contrasto tra i limiti territoriali alla giurisdizione dei legislatori e delle corti, e la natura globale dei servizi digitali potrebbe comportare il rischio di una gara al ribasso nella protezione dei diritti in gioco e a una ridotta efficacia dei relativi meccanismi di tutela. Ciò rappresenta un ulteriore riflesso del conflitto tra diritto locale e diritto globale che caratterizza la globalizzazione del ruolo delle corti. L'analisi della giurisprudenza di cui sopra rivela una migrazione di idee giuridiche (o costituzionali) da un lato all'altro dell'Atlantico. Finora, tale migrazione è stata quasi esclusivamente unidirezionale. I giudici europei "esportano" le idee europee al di fuori dell'Europa. In altre parole, le decisioni delle corti europee, che sono ampiamente citate al fine di corroborare la legittimità e persuasività delle loro stesse conclusioni, ispirano e influenzano i giudici non europei, come accaduto per esempio in Canada. Attualmente, qualsiasi procedimento inverso sembra lungi dall'avvenire. Le corti europee sembrano essere più inclini a "insegnare" piuttosto che "imparare" quando si tratti di discutere della protezione, *erga omnes*, di valori costituzionali europei, anche al di là dei confini europei.

Orbene, l'estensione del potere dei paradigmi europei, che stanno rendendo l'Europa, quasi paradossalmente, una fortezza per la protezione dei dati, non considera gli impatti politici e giuridici che esso ha sulle relazioni con i Paesi terzi. Questa scelta politica dell'UE può essere letta come un tentativo di codificare il diritto alla privacy digitale. Ciononostante, il ruolo delle corti in relazione alla tutela transnazionale della privacy e della protezione dei dati è solo ai suoi inizi.

---

[58] Un problema che si manifesta anche nell'ambito del *cloud computing,* come *supra* si accennava. Difatti, nell'ambito di questo servizio, l'esercizio di sovranità digitale dell'Unione europea appare ancora agli albori, mancando di quel necessario focus sulla tutela dei diritti considerati in senso ampissimo, tenuto conto delle problematiche già emerse con riguardo alla disciplina a protezione dei dati personali. A tal proposito, appare necessario guardare alle spinte globali che interessano il *cloud* e il *free flow* di dati, anche non personali. Ebbene, considerando altre esperienze, come, ad esempio quella statunitense e cinese, emerge un atteggiamento volto all'adozione di misure difensive del proprio patrimonio digitale. D'altro canto, i *big players,* tra cui Google e Amazon, che, nell'ottica di adeguarsi a tali approcci limitati e limitanti, hanno sempre più regionalizzato e localizzato le loro risorse. Ancora una volta preoccupa come la scelta di proteggere o meno i propri clienti da accessi desiderati o indesiderati, sia se previsti dal CLOUD Act, sia se previsti dalle iniziative del governo cinese, ricadano su attori privati che, alla base di tali scelte cruciali, non pongono la *rule of law,* ma le più convenienti logiche di *business.*

3. La città tra pubblico e privato

La sovranità e l'applicazione del modello europeo di protezione dei dati non coinvolge solamente i rapporti tra Stati e l'emersione di corrispondenti modelli di tutela. L'inevitabile contributo degli attori privati nel *design*, produzione, commercializzazione di quelle che abbiamo identificato come le architetture della *smart city,* rende i soggetti detentori di queste ultime in grado di esercitare una grande influenza sui cittadini[59]. Il profilo che riguarda il controllo e la sorveglianza massivi desta negli interpreti forti preoccupazioni sulla capacità di garantire l'applicazione dei diritti fondamentali. Da ciò, nasce l'esigenza di definire una nuova dimensione del diritto alla riservatezza, nonché di quello all'autonomia e alla libera determinazione anche in relazione agli spazi pubblici.

La giurisprudenza della Corte europea dei diritti dell'uomo ha interpretato l'art. 8 della Convenzione europea sui diritti dell'uomo nel senso di ricomprendervi il diritto di ciascuna persona una propria vita sociale privata[60]. Sebbene in un contesto pubblico, sussiste una zona di interazione dei cittadini con gli altri, nella quale si estrinseca un'aspettativa alla *privacy*[61]. Un'accezione che fa da eco al concetto di Quarto Emendamento e a quella *"expectation of privacy"* elaborata dal giudice statunitense nella decisione del notissimo caso *Katz v. US* del 1967[62], già ripresa da diverse Corti americane[63], le quali hanno avuto modo di chiarire che «*advances in technology can increase the potential for unreasonable intrusions into personal privacy*»[64].

Pertanto, anche e soprattutto nella *smart city*, la *privacy* deve essere una condizione infrastrutturale che permette il pieno esercizio dei diritti fondamentali e lo sviluppo dell'autonomia e della libera determinazione degli individui sia in spazi privati che in spazi pubblici. A tal proposito, va ricordato come il diritto alla *privacy* nella società digitale non possa limitarsi al non subire interferenze esterne nell'esercizio dei propri diritti individuali. Per esser davvero efficace, il diritto alla riservatezza e alla protezione dei dati personali deve connettersi in modo esplicito e rigoroso alla costruzione d'uno spazio comune di salvaguardia della dignità, delle libertà e della sicurezza delle

[59] *Ex multis,* su questo argomento, si cita C. O'neil, *Weapons of math destruction: How big data increases inequality and threatens democracy*, Washington D.C., 2016.

[60] Si vedano, tra altri precedenti, CEDU, *Botta c. Italia*, ric. 21439/93 (1998)*;* CEDU, *Barbulescu c. Romania*, ric. 61496/08 (2017).

[61] Si vedano, tra altri precedenti, CEDU, *Peck c. Regno Unito*, ric. 44647/98 (2003); CEDU, *Von Hannover c. Germania*, ric. 40660/08 e 60641/08 (2012); CEDU, *Uzun c. Germania*, ric. 35623/05 (2010); CEDU, *Altay c. Turchia*, ric. 11236/09 (2019).

[62] Ivi il giudicante si esprimeva in questi termini: «*t]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy'. That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's general right to privacy – his right to be let alone by other people – is, like the protection of his property and of his very life, left largely to the law of the individual States ... For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection*», in *Katz v United States* 389 US 347 (1967), 350.

[63] In particolare, ci si riferisce a diverse importati decisioni, come in *United States v. Jones,* 565 U.S. 400 (2012); *Riley v. California,* 573 U.S. 373, (2014) e in *Carpenter v. United States,* 585 U.S.*,* (2018).

[64] *Patel v. Facebook, Inc*., No. 18-15982 (9th Cir. 2019).

persone[65].

Tuttavia, si rileva che la realizzazione di una simile condizione infrastrutturale all'interno delle città intelligenti non passa solo attraverso le decisioni dell'attore pubblico, bensì è subordinata anche alle volontà dei soggetti privati, detentori delle tecnologie più innovative. Infatti, deve ricordarsi come i modelli di *smart cities* finora proposti vedano l'utilizzo di sistemi ICT essenzialmente e quasi sistematicamente basati su partenariati pubblico-privati. Dal momento che le tecnologie utilizzate nelle città intelligenti hanno la capacità di aumentare il controllo e il grado di sorveglianza su ogni aspetto della vita dei cittadini, ne discende che, inevitabilmente, tale potere sarà ancora una volta appannaggio anche dei soggetti privati. Basti pensare, ad esempio, al ruolo che già ricoprono società come Amazon, Uber, AirBnB, le quali offrono servizi a vario titolo alle amministrazioni cittadine. Queste realtà, consce del binomio informazione-potere, sono massimamente attratte dalle incredibili opportunità che l'utilizzo di dati personali e informazioni dei cittadini può creare. Ciò, non tanto e non solo per aumentare la precisione dei propri spazi pubblicitari, ma soprattutto al fine di alimentare i loro algoritmi di intelligenza artificiale, impiegati a loro volta nei modelli di *smart cities*.

Un esempio di quanto accennato è la crisi che questo spazio *uber* pubblico provoca all'esercizio della libertà di manifestazione del pensiero. Come già ampia letteratura ha messo in evidenza[66], l'attuale esercizio di questa libertà è sostanzialmente mediato da una serie di infrastrutture, tra cui i *social network,* che, attraverso il sistema di moderazione dei contenuti e dei filtri, dirige e amministra la formazione delle opinioni e delle idee nonché la circolazione delle medesime. La commercializzazione e la diffusione di sistemi automatizzati non hanno delle ricadute solamente sull'esercizio passivo della libertà d'espressione, ma vi sono delle importanti conseguenze con riguardo al profilo attivo, ossia la possibilità garantita al cittadino di manifestare liberamente il proprio pensiero.

Ebbene, anche da recente giurisprudenza della Corte europea dei diritti dell'uomo e dall'interpretazione dell'art. 10 della Convenzione[67], è possibile evincere che la dimensione attiva abbia un'immensa centralità, non solo in rispetto al *medium* tecnologico, ma anche nella sua dimensione atomica[68]. Proprio in questo contesto, dunque, il paci-

[65] Infatti, come indicò Stefano Rodotà nella sua relazione introduttiva alla ventiseiesima Conferenza internazionale sulla protezione dei dati: «noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro».

[66] Il riferimento ricade, in particolare, sull'analisi di J. M. Balkin, *Free speech is a triangle*, in *Colum. L. Rev.*, 118, 2018, 2011.

[67] Si veda, ad esempio, la decisione della Corte EDU, *Stern Taulats and Roura Capellera c. Spagna,* ric. 51168/15 e 51186/15 (2018); *Z.B. c. Francia,* ric. 46883/15 (2021).

[68] Questo concetto emerge nella pronuncia *Stern Tautlas c. Spagna* ove al § 30 la Corte si è espressa in questi termini: *«La liberté d'expression constitue l'un des fondements essentiels d'une société démocratique, l'une des conditions primordiales de son progrès et de l'épanouissement de chacun. Sous réserve du paragraphe 2 de l'article 10 de la Convention, elle vaut non seulement pour les « informations » ou les « idées » accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent : ainsi le veulent le pluralisme, la tolérance et l'esprit d'ouverture sans lesquels il n'est pas de « société démocratique » (Handyside c. Royaume-Uni, 7 décembre 1976, § 49, série A no 24, et Lindon, Otchakovsky-Laurens et July c. France [GC], nos 21279/02 et 36448/02, § 45, CEDH 2007-IV). Telle que la consacre l'article 10 de la Convention, la liberté d'expression est assortie d'exceptions qui appellent toutefois une interprétation étroite, et le besoin de la restreindre doit se trouver établi de manière convaincante».*

fico esercizio della libertà d'espressione viene posto in crisi dalla presenza di *always-on devices,* come quelli sopra descritti, che popolano la città del futuro. Sebbene una parte della letteratura ritenga che tali meccanismi possano persino aumentare la partecipazione dei cittadini - si pensi alla circolazione di piattaforme di *e-voting* - d'altro canto preoccupano le possibili intrusioni e l'inasprimento di perduranti situazioni iniquità e discriminazione.

Il far passare l'esercizio delle libertà democratiche per l'impiego di strumenti digitalizzati porta alla luce un grave problema di *digital literacy*, da un lato, e, dall'altro, la creazione dei c.d. *chilling effects.* In particolare, allo stato dell'arte, l'educazione alla digitalizzazione è ancora un problema parzialmente irrisolto, così come l'accesso alle stesse e a Internet[69]. Lo stesso impiego di queste tecnologie, indipendentemente dal grado di connettività della popolazione, a causa della mancanza di equità degli algoritmi, può, come si premetteva, radicare ancor di più determinate disuguaglianze. Tali tecnologie, riflettendo inevitabilmente scelte etiche e politiche e tendenze storiche, effettuano dei giudizi di valore[70] col rischio di acerbare l'esclusione di minoranze, non solo dall'utilizzo del mezzo tecnologico, ma anche dalla partecipazione alla *res publica.* Di conseguenza, e con riguardo al secondo aspetto, la struttura stessa dalla città intelligente è in grado di provocare un *vulnus* alle libertà fondamentali di tipo, ad esempio, associativo. In particolare, si prefigura il rischio di c.d. *chilling effects*[71]: una modificazione delle abitudini individuali per evitare di sottostare all'occhio indiscreto di una telecamera, pur di tutelare la riservatezza personale. Peraltro, la sempre maggiore presenza di attori privati nel triangolo della libertà d'espressione complica ulteriormente il quadro, non solo nel lato passivo, ma anche attivo dell'esercizio di tali libertà. Pertanto, sebbene la rete costituisca una possibilità di sviluppo della *smart city* e di integrazione per il cittadino, quest'ultima pone, allo stesso tempo, diverse sfide per i diritti fondamentali per via della riduzione degli spazi privati dei cittadini che rischia di condurre ad uno sgretolamento della distinzione tra spazi pubblici e privati. Su tale aspetto dovrà imperniarsi l'intera sfida di *governance* statale che, oltre a tener conto dei rischi alla sicurezza e alla riservatezza, dovrà senza dubbio guardare all'impatto sui diritti e le libertà fondamentali nel redigere *policy* che siano in grado di traghettare il cittadino verso lo spazio urbano *smart.*

3.1 (segue) Una sfida per il legislatore europeo

Alla luce della panoramica che si è delineata e che finora ha riguardato la privacy, la protezione dei dati personali, e la libertà d'espressione, si evince che le sfide che il legislatore dovrà affrontare sono numerosissime e dovranno essere sostenute da un apparato di *policy* che tenda alla ricerca della complementarità della città intelligente con

[69] A tal riguardo, si rimanda al ricco dibattito sul tema, alimentato, *ex multis,* da M. R. Allegri - G. d'Ippolito (a cura di), *Accesso a Internet e neutralità della Rete, tra principi costituzionali e regole europee*, Roma 2017.

[70] F. Pasquale, *The Black Box Society,* Cambridge (MA), 2015.

[71] M. Büchi, *Chilling Effects of Profiling Activities: Mapping the Issues*, in *Computer Law & Security Review,* 36, 2020.

i principi fondamentali, onde evitare la creazione di antinomie. Quest'ultime preoccupano non solo dal punto di vista dei diritti individuali, ma anche per le conseguenze sul mercato digitale.

A tal proposito, come si menzionava all'inizio, l'Unione europea ha dato avvio a delle iniziative anche in tal senso. Una di queste è il regolamento sui mercati digitali, o *Digital Markets Act* (DMA), la cui proposta è stata presentata insieme al *Digital Services Act*[72]. Essa consiste in una iniziativa legislativa volta a garantire un mercato unico competitivo per i servizi digitali e, in particolare, mercati delle piattaforme equi e contendibili. Difatti, equità (*fairness*) contendibilità (*contestability*) dei mercati digitali sembrano essere le due parole chiave su cui si appunta l'intera normativa[73].

Il collegamento di questa normativa con il tema in oggetto è quanto mai tautologico. Come più volte si è detto, il ruolo dei dati e, dunque, delle imprese che hanno fatto di questi il loro *core business,* sono asset essenziali nella città *smart.*[74] D'altro canto, però, i medesimi possono rafforzare situazione di monopolio che consentono il governo del mercato digitale e, per converso, della città digitale. Orbene, nonostante il legislatore europeo abbia dato avvio a quest'opera di regolazione, come evidenziano taluni commentatori[75] un aspetto di cruciale importanza è stato trascurato. Il DMA ragiona attorno a un concetto di internet fatto di persone e non di cose. In altre parole, manca di guardare oltre la staccionata dove vi sono importanti novità strutturali della rete, tra cui il 5G, le quali avranno un feroce impatto su taluni settori dell'internet delle cose, come l'*automotive,* che hanno bisogno di una rete infrastrutturale solidissima, anche dal punto di vista della cybersicurezza[76]. Difatti, uno dei principali aspetti della *smart city* riguarda proprio la gestione del traffico[77], su cui si basano i servizi che vengono già resi da taluni *player*, quale Google Maps. Ebbene, il fatto che il DMA non si interroghi sulla tenuta della struttura proposta rispetto al già annunciato avvento di nuovi servizi, nuove piattaforme e quindi nuovi *gatekeepers*, è un aspetto problematico che evidenzia la mancanza di una visione prospettica che possa declinare al futuro il paradigma europeo, non solo dei dati personali.

Inoltre, il Regolamento non contiene alcun riferimento a concetti quali la nuova generazione di reti-servizio di oggetti connessi, pur imponendo, però, la garanzia di interoperabilità e portabilità dei sistemi sulla falsariga di quanto già previsto dal GDPR[78].

---

[72] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[73] Si veda considerando 28 e 32.

[74] Tale aspetto è chiaramente riconosciuto nel DMA al considerando 36.

[75] M. Polo - A. Sassano, *Dma: Digital Markets Act o Digital Markets Armistice?,* in *Mercato Concorrenza Regole*, 3, 2021.

[76] H. Olufowobi - G. Bloom, *Connected cars: Automotive cybersecurity and privacy for smart cities,* in *Smart cities cybersecurity and privacy*, in D. B. Rawat – K. Z. Ghafoor (a cura di) *Smart Cities Cybersecurity and Privacy,* Amsterdam, 2019, 227 ss.

[77] A tal riguardo, si rimanda all'esempio di Venezia, come analizzato da F. Meneghetti - C. Carlo Rossi Chauvenet - G. Fioroni, *Rapporto 3/2022 – SMART cities e intelligenza artificiale*, in *BioLaw*, 1, 2022.

[78] Non ci si può ivi soffermare sulla criticità di garantire portabilità e interoperabilità, già ampiamente riscontrate nel settore. Si rimanda a J. Wong - T. Henderson, *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, in *International Data Privacy Law*, 9 (3), 2019, come pure a M. Polo - A. Sassano, *Dma: Digital Markets Act or Digital Markets Armistice?*, cit.

In breve, tali soluzioni non permettono di soffermarsi adeguatamente sul controllo e sull'utilizzo effettivo dei dati, tema chiave nel mercato digitale, e, ancor più, nella città digitale. Dette problematiche, necessitano, anche alla luce dell'estesa ricostruzione che si è fatta del modello europeo della privacy, di essere esaminate nella prospettiva del potere digitale, ossia della sovranità tanto statale dei dati (e di coloro che li detengono). Il DMA, così come altre iniziative, non guarda al controllo dei dati. O meglio, pare esserci un conflitto tra controlli legittimamente reclamabili: da un lato, quello dell'interessato sui propri dati personali, e, dall'altro quello delle imprese sui dati, spesso non personali, che consentono il loro funzionamento. Tali dati sono altresì espressivi della realizzazione di due diritti contrapposti: la protezione dei dati, e la libertà d'impresa.
Il conflitto tra controllo e circolazione, tra artt. 7 e 8, e 16 della Carta di Nizza, si inserisce nel tema della regolazione del mercato digitale, ma anche in quello dell'intelligenza artificiale. In definitiva, quel che manca è un ponte tra *governance* dei dati personali e quella dei dati non-personali, con la conseguenza di amplificare il conflitto tra interessi contrapposti e opposti. Allo stato dell'arte, i due sistemi sono *"lost in translation"* e questo ponte mancante minaccia direttamente i diritti umani delle persone e lo sviluppo sicuro dei sistemi di apprendimento automatico. Le leggi europee sulla protezione dei dati, astrattamente il miglior modello possibile, si rivelano spesso inadeguate a fornire in concreto una protezione adeguata e duratura.
Si crede, dunque, che sia questa la principale sfida che dovrà affrontare il legislatore europeo, non solo nello spirito di garantire un efficace sviluppo della *smart city*, a prova di diritti. Occorre altresì che tale sviluppo comprenda proprio tutti gli interessi in gioco e consenta la comunicabilità dei sistemi di *governance* che vengono tutti toccati dalla rivoluzione digitale. In secondo luogo, è richiesto l'individuazione di un sistema su cui basare tale nuova collaborazione tra gli attori pubblici e privati. Senza alcuna pretesa di esaustività, dato l'immenso dibattito sul tema[79], si ritiene quanto mai necessario incorporare i valori dei diritti costituzionali sin dalla fase di progettazione delle macchine, e, per estensione, della città *smart*. Per tal ragione, è richiesto al costituzionalista di avvicinarsi alle necessità del digitale e di creare una nuova dimensione in cui l'*humus* sostanziale sia quello dei diritti umani fondamentali tradotto nel linguaggio della tecnologia. La mancanza di questo processo di ibridazione, è di tutta evidenza in alcuni, seppur importanti, sforzi della Commissione europea, ove nella proposta di Regolamento dell'Intelligenza Artificiale ancora manca una comunicazione effettiva tra problematiche tecnologiche e accentramento del focus sulla figura umana[80]. Pertanto, la sfida si situa nella costruzione di una cornice normativa che sia in grado di sostenere gli obbiettivi del mercato unico e, d'altro canto, che sia tutelante dei valori europei, quali il principio della *rule of law*, la protezione dei diritti fondamentali, la dignità umana.
L'Europa sembra aver compiuto alcuni passi al fine di trovare un bilanciamento tra innovazione e tutela dei diritti. Favorendo, dunque, lo sviluppo di un tale modello, si

[79] G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 19 (1), 2020, 41 ss.; M.F. Cuéllar, - A.Z. Huq, *Toward the Democratic Regulation of AI Systems: A Prolegomenon*, in *U. of Chicago, Public Law Working Paper*, n. 753, 2020.

[80] L. Floridi, *The European Legislation on AI: A brief analysis of its philosophical approach*, in *Philosophy & Technology,* 34 (2), 2021, 215 ss.

potrebbe fondare una catena preziosa, capace di spingere verso un mercato del digitale che ricomprenda la scala valoriale dell'UE. Infatti, dall'entrata in vigore del GDPR, l'Unione europea si è imposta nel settore come un importante attore, consentendo all'*acquis* comunitario di definire proporre un modello del quale la privacy rappresenta il Primo Emendamento [81].

Accanto alla collaborazione e alla *policy* «*by education*», è necessario pensare a modelli pratici di interazione. Queste misure assomiglieranno meno agli strumenti di *policy* coercitiva del ventesimo secolo e più ai modelli di prevenzione e controllo apparentemente consensuale che si trovano anche nella *soft law*. Poiché molti degli strumenti che consentono il funzionamento delle *smart city* saranno stati sviluppati con la collaborazione dei privati, ci saranno maggiori difficoltà nel mantenere una visione della *policy* urbana tutelante le posizioni dei singoli[82]. Si ritiene, in conclusione, che la *data driven regulation*[83] debba essere continuamente assistita da un'analisi di impatto che abbia il suo fondamento nei diritti fondamentali dei cittadini[84]. Una realtà la cui concretizzazione si auspica non attenda la posa della prima pietra della città intelligente, ma che possa essere recepita nel *design* delle tecnologie, in particolare, quelle automatizzate, già ampiamente presenti nella realtà atomica e digitali dell'oggi.

4. Conclusione

La *smart city* rappresenta l'unione di una serie di difficoltà cui il diritto costituzionale, e, per converso, la protezione delle libertà fondamentali sono già ampiamente esposte nell'ambito della digitalizzazione. Considerando le sfide poste alla riservatezza degli individui, nel corso della trattazione si sono indagati elementi di complementarità tra la città di domani e la città di oggi nell'ottica di delineare varchi in cui possano essere garantiti i diritti fondamentali di ciascuno anche nella città progredita dalla tecnologia e dalla diffusione delle reti.

Si tratta di uno "stress test" resosi necessario dall'annessione di sensori e tecnologie intelligenti nell'ambiente urbano: uno spazio in cui pubblico e privato sono necessariamente posti su piani inediti.

A ben vedere, sono argomenti che si inquadrano nel più ampio spettro delle proble-

[81] B. Petkova, *Privacy as Europe's First Amendment: A Brief Analysis of its Philosophical Approach*, cit.

[82] E. Joh, *Policing the smart city*, in *International Journal of Law in Context,* 15(2), 2019, 177-182.

[83] S. Ranchordas - A. Klop, *Data-Driven Regulation and Governance in Smart Cities*, in A. Berlee - V. Mak - E. Tjong Tjin Tai (eds.), *Research Handbook on Data Science and Law*, Groningen, 2018.

[84] Si veda, a tal proposito, la Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, adottata dal Council of Europe l'8 aprile 2020, ove al punto 14 si legge che: *«the design, development and ongoing deployment of algorithmic systems involves many actors, including software designers, programmers, data sources, data workers, proprietors, sellers, users or customers, providers of infrastructure, and public and private actors and institutions. In addition, many algorithmic systems, whether learning or non-learning, operate with significant levels of opacity, sometimes even deliberately. Even the designer or operator, who will usually establish the overarching aim and parameters of the system, including the input data, the optimisation target and the model, will often not know what information the system relies upon to make its decision, and is likely to encounter uncertainty about the direct and indirect effects of the system on users and the broader environments in which these systems are intended to operate».*

matiche provocate dalla digitalizzazione e con cui il diritto ha avuto a che fare negli ultimi dieci anni. In quest'ottica, la *smart city,* se regolata per tempo, non rappresenta assolutamente un'antinomia per il diritto, potendosi ben individuare nuovi sistemi di *governance,* ove pubblico e privato devono necessariamente collaborare. La *compliance* imposta dall'uno a scapito dell'altro non dovrà sostanziarsi in un sistema unilaterale di limiti, ma dovrà guardare all'integrazione e all'innovazione di differenti sistemi bilanciando rischi e opportunità. In definitiva, sarà necessario sviluppare modelli di *smart city* idonei a garantire una *governance* trasparente, inclusiva, capace di sviluppare una visione chiara e condivisa del benessere, della qualità della vita e della sostenibilità[85].
«Siamo chiamati a essere costruttori non vittime del futuro», scriveva Fuller.[86] Volendo far tesoro di questo monito, si crede che l'Europa, più di altri attori, appaia assolutamente in grado di poter guardare al futuro e poter guidare la creazione di un nuovo modello regolatorio[87], non solo con riguardo al tema della *smart city*, e senza commettere l'errore di ricadere in modelli stagnanti. Assumendo come faro la dignità umana e il rispetto di principi e diritti fondamentali, si potrà realizzare un ambiente in cui prevale la complementarità tra tecnologia e diritto, tra innovazione e protezione.

[85] F. Toni, *Smart city: innovazione e sostenibilità,* cit.

[86] R. Buckminster Fuller - K. Kuromiya, *Cosmography. A posthumous scenario for the future of humanity,* New York, 1992, 8.

[87] In tal senso, si ricorda non solo il menzionato AI Act, ma anche la European Data Strategy, di cui il nodo centrale è rappresentato dal *Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data*, meglio noto come Data Act (COM(2022) 68, proposta pubblicata il 23 febbraio 2022), norma con la quale si andranno a rivedere anche taluni aspetti della Database Directive, ossia la Direttiva 96/9/EC. Tali proposte *policy* vanno, per l'appunto, nella direzione di stabilire un unico quadro di *governance* intersettoriale per l'uso di dati, sia da parte dei privati sia da parte degli attori pubblici.

La lotta alla disinformazione nei rapporti tra Unione e Stati terzi alla luce del conflitto russo-ucraino*

Sarah Lattanzi

Abstract

A seguito dell'aggressione militare della Russia in Ucraina, il primo marzo del 2022 il Consiglio dell'Unione europea ha adottato un nuovo pacchetto di misure avente ad oggetto l'inedita misura della sospensione di alcuni alcuni organi di informazione ed agenzie di stampa sottoposti sotto il controllo della Federazione Russa. Questo scritto analizza questa nuova misura dal punto di vista della base giuridica fornita per la sua adozione in ambito PESC e delle ripercussioni che essa ha su altri ambiti materiali, quali quello dei media audiovisivi e del pluralismo dell'informazione. Secondo l'A. le interazioni tra questi diversi ambiti sollevano una serie di criticità sotto il profilo della legittimità e della coerenza delle azioni recentemente intraprese dall'Unione nella dimensione esterna ed interna in materia di lotta alla disinformazione e, oggi, alla "propaganda del Cremlino".

On 1 March 2022, the Council of the European Union adopted a new package of restrictive measures against Russia following the military aggression in Ukraine, concerning the suspension of certain media outlets and information agencies under the control of the Russian Federation. This paper analyses this measure of an unprecedented nature, in the light of the legal basis provided for its adoption under the CFSP framework and the impact it has on other areas, such as the audiovisual media and the protection of information pluralism. In my view, the interactions between these different areas raise a number of critical issues from the point of view of the legitimacy and coherence of the actions recently undertaken by the European Union against disinformation and now the "Kremlin propaganda", both in its external and internal dimensions.

Sommario

1. Introduzione: la sospensione delle attività di diffusione di alcuni organi di informazione russi nel contesto del conflitto Russo-Ucraino – 2. La lotta alla disinformazione nell'Unione europea: un quadro normativo "integrato" – 3. La lotta alla disinformazione nelle relazioni esterne dell'Unione: le misure restrittive applicate all'ambito dei

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

media controllati da Stati terzi – 4. Conclusioni: l'*infowar* e i limiti del diritto sovranazionale.

Keywords

conflitto russo-ucraino - misure restrittive - PESC - disinformazione - pluralismo dei media e del'informazione

1. Introduzione: la sospensione delle attività di diffusione di alcuni organi di informazione russi nel contesto del conflitto Russo-Ucraino

All'indomani dell'attacco sferrato dai convogli militari della Federazione russa su alcune cittadine ucraine all'alba del 24 febbraio del 2022, la Presidente della Commissione europea Ursula von der Leyen ha, in una conferenza stampa tenuta il 27 febbraio congiuntamente all'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, Joseph Borrell, annunciato l'adozione di una nuova serie di misure sanzionatorie nei confronti della Russia[1].

Contando le misure restrittive sin ora adottate, partendo da quelle annunciate il 27 febbraio sino a quelle più recenti del mese di giugno, risulta che l'Unione europea ha, ad oggi, all'attivo sei diversi pacchetti di misure sanzionatorie nei confronti della Federazione russa[2], il cui contenuto è estremamente vario per oggetto, scopo e intensità. A prima vista potrebbe ritenersi che anche queste ultime misure si inseriscano in linea di continuità con quanto l'Unione ha cominciato a fare sin dal 2014, a seguito dell'annessione russa della Crimea e di Sebastopoli. Sicuramente ciò che accomuna tutte queste sanzioni è un medesimo presupposto giustificativo, radicato nella necessità di rispondere a una situazione di forte tensione internazionale, degenerata in un conflitto armato.

Mentre però i primi pacchetti adottati dall'Unione nel 2014 avevano ad oggetto misure economico-finanziarie di tipo selettivo, tradizionalmente volte a limitare l'accesso della Federazione a quei mercati quali quello dei capitali, della difesa, dei beni a duplice uso, delle tecnologie sensibili e in parte anche a quello petrolifero, ritenuti suscettibili di aumentare le capacità belliche dello Stato aggressore, le misure più recenti, pur sempre adottate conformemente alla duplice base giuridica prevista in ambito PESC dagli artt. 29 TUE e 215 TFUE, coprono ambiti materiali nuovi e sempre più estesi[3], con la conseguenza che risulta sempre meno evidente la connessione tra il "mezzo" costituito dalla misura sanzionatoria e lo "scopo" perseguito.

[1] Dichiarazione del 27 febbraio 2022 della Presidente della Commissione Von der Leyen.

[2] Per la cronistoria delle misure restrittive si veda Cronistoria – Misure restrittive dell'UE nei confronti della Russia in relazione all'Ucraina.

[3] Il terzo pacchetto sanzionatorio è stato definito dalla Presidente della Commissione come «*another unprecedented step*» nel quadro della risposta dall'Unione al conflitto russo-urcraino, per cui si veda Dichiarazione del 27 febbraio 2022, cit.

In particolare, sfugge come alcune delle ultime misure adottate possano eventualmente essere in grado di ridurre la capacità militare russa o a indurre l'autore della condotta antigiuridica «a cessare o modificare tale condotta»[4].

Ciò è tanto più evidente con riferimento al terzo pacchetto adottato nel marzo del 2022 tra cui figura anche la misura, del tutto inedita, dell'immediata sospensione della diffusione sul territorio europeo dell'agenzia di informazione *Sputnik* e del canale TV *RT/Russia Today* (insieme alle sue filiali *RT English*, *RT UK, RT Germany*, *RT France e RT Spanish*)[5], a cui ne è seguito un sesto adottato il 4 giugno del 2022 volto alla sospensione delle emittenti televisive *Rossiya RTR*, *RTR Planeta*, *Rossiya 24*, *Russia 24* e *TV Centre International*[6].

La misura di sospensione di tali canali è stata innanzitutto adottata in virtù del regolamento (UE) 2022/350 del Consiglio, del 1° marzo 2022, che modifica il regolamento (UE) 833/2014 concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, e a seguito della decisione (PESC) 2022/351 del Consiglio, del 1° marzo 2022, che modifica la decisione (PESC) 2014/512 concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina. A questi atti si sono successivamente aggiunti la decisione (PESC) 2022/884 del Consiglio del 3 giugno 2022 che modifica la decisione (PESC) 2014/512, concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina e il regolamento (UE) del Consiglio 2022/879, dello stesso giorno che ugualmente modifica il regolamento (UE) 833/2014[7]. La lotta alla "propaganda del Cremlino" è l'oggetto degli atti citati, i quali sembrano destinati, in prospettiva, ad ampliare notevolmente le capacità sanzionatorie dell'Unione[8].

Attraverso di essi, l'Unione europea ha inteso colpire la Federazione russa questa volta sotto il profilo della sua capacità di operare una «sistematica campagna internazionale di manipolazione dei media e di distorsione dei fatti, nell'intento di rafforzare la sua strategia di destabilizzazione dei paesi limitrofi e dell'Unione e dei suoi Stati membri»[9]. Questa campagna troverebbe infatti un'eco «in vari organi di informazione sotto lo stabile controllo diretto o indiretto della leadership della Federazione russa», tra cui figurano le agenzie sanzionate, le quali svolgono «un ruolo essenziale, strumentale ai fini della promozione e del sostegno dell'aggressione nei confronti dell'Ucraina e della

[4] CGUE, C-440/14 P, *National Iranian Oil Company/Consiglio* (2016), § 82.

[5] Allegato XV del regolamento (UE) 2022/350 del Consiglio del 1° marzo 2022 che modifica il reg. (UE) n. 833/2014 concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, in *GUUE* L *65, 1–4*.

[6] Allegato VI del regolamento (UE) 2022/879 del Consiglio del 3 giugno 2022 che modifica il regolamento (UE) n. 833/2014, concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina, in *GUUE* L 153, *53–74*.

[7] Per un commento a questa misura si v. L. Ciliberti, *Free flow of information – Il contrasto alla disinformazione in tempi di guerra*, in questa *Rivista*, 2, 2022, 349 ss.

[8] Seppure implicitamente poiché questo temine non compare nel testo negli atti citati, come nota C. Di Turi, *Il conflitto in Ucraina e la propaganda di guerra della Federazione russa: quali reazioni da parte dell'Unione europea?*, in *Eurojus*, 2022, 333.

[9] Sesto considerando del regolamento (UE) 2022/350 e della decisione (PESC) 2022/351.

destabilizzazione dei paesi ad essa limitrofi»[10] e pertanto rappresentano una «minaccia consistente e diretta all'ordine pubblico e alla sicurezza dell'Unione»[11]. L'ottavo considerando del successivo regolamento (UE) 2022/879 precisa, inoltre, come «da tempo la Federazione russa attua una sistematica campagna internazionale di manipolazione dei media e di distorsione dei fatti, nell'intento di rafforzare la sua strategia di destabilizzazione dei paesi limitrofi e dell'Unione e dei suoi Stati membri. In particolare, la propaganda ha preso di mira, ripetutamente e costantemente, i partiti politici europei, soprattutto durante i periodi elettorali, la società civile, i richiedenti asilo, le minoranze etniche russe, le minoranze di genere e il funzionamento delle istituzioni democratiche nell'Unione e nei suoi Stati membri».

Per tutte queste ragioni, il regolamento 2022/350 sopra citato, pone un divieto generalizzato a tutti gli operatori, pubblici privati, e attraverso qualsiasi mezzo, sia esso via cavo, satellite, IP-TV, attraverso fornitori di servizi internet, piattaforma o applicazione di condivisione di video su internet, di diffondere i loro contenuti. A questo fine, il suo art. 12 precisa inoltre che «sono sospesi qualsiasi licenza o autorizzazione di radiodiffusione e qualsiasi accordo di trasmissione e distribuzione con le persone giuridiche, le entità o gli organismi elencati nell'allegato XV» e ora anche nell'allegato VI del regolamento 2022/879.

Questa misura, seppure adottata nell'ambito delle relazioni esterne pone il preciso obiettivo di tutelare i cittadini e l'ordine pubblico europeo e deve pertanto essere letta alla luce della più ampia e intensa gamma di sforzi che l'Unione sta intraprendendo ormai da alcuni anni nella lotta alla disinformazione, recentemente coadiuvata dal tentativo di contrastare anche le minacce ibride che da essa possono nascere[12].

La connessione tra lotta alla disinformazione e contrasto alle minacce ibride si salda nel concetto di propaganda[13], il quale, in quanto specificazione di quello di disinformazione, fa proprie anche una serie di finalità di più ampio respiro politico. Da questo punto di vista sembrerebbe allora necessario considerare propaganda e disinformazione quali concetti attigui[14], alla stessa maniera in cui lo sono "disinformazione" e "discorsi d'odio" o "discorsi di odio" e reati di apologia[15]. Si tenga presente, nondimeno, che l'ampiezza concettuale di questi termini impatta sulla loro - altrettanto ampia - definizione giuridica la quale a sua volta rischia di consentire uno spostamento caso per caso dei fatti controversi da una categoria concettuale, e da un atto illecito o un

[10] Nono considerando del regolamento (UE) 2022/350 e della decisione (PESC) 2022/351.

[11] Ottavo considerando del regolamento (UE) 2022/350 e della decisione (PESC) 2022/351.

[12] *Joint Framework on countering hybrid threats: a European Union response*, JOIN(2016) 18 final.

[13] Termine per il quale non esiste una definizione univoca e su cui si v., in generale, J. B. Whitton, *Aggressive Propaganda*, in C. Bassiouni - N.P. Nanda (eds.), *International Criminal Law*, Springfield, 1974, 239.

[14] Questo perché alcuni fatti potrebbero facilmente confluire in una categoria e successivamente in un'altra. Si pensi, per un esempio, alle speculazioni legate ai Protocolli dei Savi di Sion, notizie false o parziali, a loro volta funzionali alla diffusione di posizioni antisemite. Sul tema si v. S. Quintarelli, *Content moderation: i rimedi tecnici*, in G. Pitruzzella - O. Pollicino - S. Quintarelli, *Parole e potere: Libertà d'espressione, hate speech e fake news*, Milano, 2017.

[15] M. Castellaneta, *L'hate speech: da limite alla libertà di espressione a crimine contro l'umanità*, in G. Venturini - S. Bariatti (eds.), *Droits individuels et justice internationale*, Milano, 2009, 157 ss.

reato, all'altro[16].

Certamente, però, il richiamo espresso alla categoria della propaganda operato nel regolamento e nella decisione citati rappresenta un salto di qualità nella lotta alla disinformazione, la quale finisce così per assumere una forte coloritura politica e un sapore, peraltro, decisamente novecentesco[17]. Infatti, attraverso il richiamo al concetto di propaganda, la disinformazione entra in una specifica dimensione politica quale è quella della creazione, attraverso la manipolazione dell'informazione, di un consenso di massa indotto; con le relative conseguenze che una tale manipolazione ingenera sia sul piano esterno dei rapporti tra Stati e tra Stati ed organizzazioni internazionali sia sul piano del corretto funzionamento interno delle società democratiche.

Al fine di cogliere al meglio i cambiamenti che su questo terreno si stanno rapidamente avvicendando o ancora di analizzare i recenti sviluppi intervenuti in occasione della guerra in Ucraina sul piano della lotta alla disinformazione, occorrerà anzitutto effettuare una panoramica del quadro di azioni che l'Unione ha intrapreso prima dello scoppio della guerra (§2). Ciò consentirà, nel capitolo successivo, di valutare gli elementi di novità ricavabili dall'analisi delle misure di sospensione recentemente adottate nei confronti delle agenzie di informazione russe (§3) e, infine, di valutare come questi elementi di novità si innestino sulla struttura istituzionale dell'Unione con uno sguardo alle implicazioni sistematiche che essi rischiano di produrre sulla struttura stessa della società europea (§4). Come spesso accade in tempo di crisi, infatti, queste misure, solo apparentemente limitate, recano in sé il germe di mutamenti più profondi della nostra società[18].

2. La lotta alla disinformazione nell'Unione europea: un quadro normativo integrato

La panoramica del quadro di azioni che l'Unione ha intrapreso nella lotta alla disinformazione deve essere condotta secondo quello che le stesse istituzioni definiscono sempre più spesso come una strategia integrata o globale[19]. I due aggettivi sono

[16] Su queste definizioni e le loro rispettive discipline si v. G.M. Ruotolo, *A Little Hate, Worldwide! Di libertà d'opinione e discorsi politici d'odio on-line nel diritto internazionale ed europeo*, in *Diritti umani e diritto internazionale*, 2020, 549 ss.

[17] P. Gerbaudo, *Controllare e proteggere. Il ritorno dello Stato*, Milano, 2022.

[18] J. Ferejohn - P. Pasquino, *The Law of the exception: A typology of emergency powers*, in *International Journal of Constitutional Law*, 2004, 210 ss.; V.V. Ramraj (eds.), *Emergencies and the limits of Legality*, Cambridge, 2008; A. Zwitter, *The Rule of Law in Times of Crisis: A Legal Theory on the State of Emergency in the Liberal Democracy*, in *ARSP: Archiv Für Rechts-Und Sozialphilosophie/Archives for Philosophy of Law and Social Philosophy,* 2012, 95 ss.; P. M. Rodríguez, *A missing piece of European Emergency Law: legal certainty and individuals' expectations in the EU response to the crisis*, in *European Constitutional Law Review*, 2016, 265 ss.

[19] Per alcuni esempi, si v. la Comunicazione Congiunta dell'11 dicembre 2013 al Parlamento europeo e al Consiglio, L'approccio globale dell'UE alle crisi e ai conflitti esterni, JOIN/2013/030 final. Da parte del Consiglio europeo si le più recenti Conclusioni del 28 settembre 2021: L'approccio globale alla ricerca e all'innovazione - La strategia dell'Europa per la cooperazione internazionale in un mondo che cambia. In merito all'approccio seguito per rispondere alla aggressione russa dell'Ucraina, si v. anche Trib. UE, ord. del 20 marzo 2022, T-125/22 R, *RT France/Consiglio,* §61: «*Il s'agit ainsi d'intérêts publics qui visent à protéger la société européenne et s'insèrent dans une stratégie globale, laquelle vise à mettre un terme, aussi vite que*

usati spesso in maniera interscambiabile, sebbene, già ad un primo livello semantico, l'approccio integrato dovrebbe riferirsi alla permutabilità di regole sufficientemente generali così da poter essere utilizzate in settori diversi, seppur trasversali, mentre l'approccio globale dovrebbe riferirsi alla presenza di regole diverse che, formalmente adottate su piani distinti, come quello interno e quello dell'azione esterna dell'Unione, risultino complementari nella disciplina complessiva di un determinato fenomeno[20].

Le azioni e gli strumenti adottati sin ora dall'Unione per far fronte alla disinformazione, concetto relativamente nuovo nel panorama giuridico dell'Unione, sono stati, da un lato, traslati da concetti già esistenti, come quelli relativi ai contenuti illegali[21], dall'altro hanno integrato concetti altrettanto nuovi come quello della lotta alle minacce ibride condotta sul piano delle relazioni esterne[22].

Già solo da ciò si evince come la distinzione tra il piano esterno e quello interno risulti essere in questo settore particolarmente sfumata, cosicché l'azione intrapresa nella lotta alla disinformazione può essere considerata, nel suo complesso, il frutto dell'uso di un approccio integrato *e* di un approccio globale.

D'altronde, che la categoria della disinformazione e quella, affine ma distinta, della propaganda chiamino in causa una inedita interazione tra piano interno ed esterno, e tra diversi settori, come quello audiovisivo, penale e da ultimo quello relativo alla regolamentazione dei servizi digitali, è evincibile guardando alla panoramica dei singoli strumenti di cui l'Unione si è finora dotata per far fronte ai suddetti problemi.

Il complesso quadro normativo unionale che ne risulta è costruito attorno a strumenti estremamente vari, nella forma e nella sostanza[23].

Anzitutto, l'Unione europea si è per la prima volta preoccupata della disinformazione proprio con riferimento all'annessione russa della Crimea e di Sebastopoli condanna-

possible, à l'agression subie par l'Ukraine», sottolineato aggiunto.

[20] Sul "*comprehensive approach*" all'ambito di difesa si v. A. H. Kammel - Z. Benjamin, *The comprehensive approach to EU crisis management: Contexts, lessons identified, and policy implications*, in *Journal of Regional Security*, 2018, 39 ss. e anche S. Blockmans - L. Debuysere, *Institutionalising the integrated approach to external* conflict, in R. Haar - T. Christiansen, S. Lange - S. Vanhoonacker (eds.), *The Making of European Security Policy,* Abingdon-on-Thames, 2021, 124 ss.

[21] Disciplinati nella direttiva (UE) 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi, in GUUE L 095, 1; la decisione quadro 2008/913/GAI, del Consiglio, del 28 novembre 2008, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale, in *GUUE* L 328, *55–58;* la direttiva (UE) 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio, in GUUE L 335, 1–14; la direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, L 88, 6–21.

[22] Joint Framework on countering hybrid threats, cit. e la decisione (PESC) 2019/797 del Consiglio del 17 maggio 2019 concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri e il regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri, in GUUE *L 129I, 1-12.*

[23] Per una panoramica si v. O. Pollicino - G.E. Vigevani - C. Melzi d'Eril - M. Cuniberti - M. Bassini, *Diritto dell'informazione*, Torino, 2019 e anche G. Pitruzzella - O. Pollicino, *Hate speech and Fake news. A Comparative Constitutional Perspective*, Milano, 2020.

ta in quanto annessione illegale nelle conclusioni del Consiglio europeo del 19 e 20 marzo del 2015, in occasione delle quali il Consiglio europeo aveva sottolineato «l'esigenza di contrastare le campagne di disinformazione in corso da parte della Russia»[24], invitando l'Alto rappresentante a elaborare, in collaborazione con gli Stati membri e le istituzioni dell'UE, un piano d'azione in materia di comunicazione strategica[25].

Da questa sollecitazione è nata all'interno del Servizio europeo per l'azione esterna la task force *East StratCom* con l'obiettivo di sviluppare una "comunicazione efficace" sulla promozione delle attività dell'Unione europea nell'Europa orientale e oltre[26]. A questa ne sono seguite altre due nel 2017, la *Task Force South* e la *Task Force Western Balkans*. Esse formano nel loro complesso, con l'aggiunta di un gruppo trasversale «with a focus on emerging threats, data analysis, policy development and international cooperation» che lavora in stretta collaborazione con il Sistema di Allerta rapido, la Strategic Communications and Information Analysis Division[27], stabilita in seno al Servizio europeo per l'azione esterna.

Progetto di punta della *East StratCom* è la *EuvsDisinfo*, una piattaforma multilingue creata con lo scopo di «affrontare e rispondere meglio alle campagne di disinformazione della Federazione Russa che riguardano l'Unione europea, i suoi Stati membri e i paesi confinanti comuni»[28]. Questa piattaforma è divisa in diverse sezioni di cui la più interessante è senza dubbio la banca dati sulla disinformazione costituita dal richiamo ad una serie di articoli il cui contenuto è sistematicamente smentito dai *fact-checkers*[29] che operano in seno alla task force[30].

Il metodo qui seguito è quello della smentita di contenuti disinformativi, diffusi da giornali e giornalisti vettori di propaganda. Diversamente, la decisione e il regolamento adottati nei confronti dell'agenzia *Sputnik* e del canale *TV Russia Today* a cui hanno fatto seguito quelli adottati nei confronti di *Rossiya RTR / RTR Planeta*, *Rossiya 24 / Russia 24* e *TV Centre International* non si basano sulla «content moderation», eventualmente operando attraverso lo strumento classico della rettifica[31], bensì attraverso l'oscuramento preventivo della diffusione di qualsivoglia contenuto.

---

[24] Conclusioni del Consiglio europeo, 19 e 20 marzo 2015, § 13.

[25] Hanno identificato la nascita della lotta alla disinformazione anzitutto come bisogno di «politica estera», G. Pitruzzella - O. Pollicino, *Hate speech,* cit., 100.

[26] Questa task force è stata a sua volta adottata sul modello del *NATO Strategic Communications Centre of Excellence (NATO StratCom COE)*, prevista da un *Memorandum of understanding* tra Estonia, Germania, Italia, Lettonia, Lithuania, Polonia e il Regno Unito firmato il 1° luglio 2014.

[27] Questa struttura amministrativa mette insieme la lotta contro la disinformazione e quella contro le minacce ibride, di cui la disinformazione farebbe parte.

[28] euvsdisinfo.eu/it/il-progetto/

[29] La cui identità, almeno guardando alla mancanza di firma apposta alla fine degli articoli di smentita, rimane anonima. Il sito riporta inoltre l'esistenza di una clausola di elusione di responsabilità per gli autori delle smentite pubblicate sul sito.

[30] «I casi presenti nella banca dati di EUvsDisinfo si concentrano sui messaggi nello spazio informativo internazionale nei quali è stata individuata una rappresentazione parziale, distorta o falsa della realtà nonché la diffusione di messaggi pro-Cremlino. Ciò non implica necessariamente che un determinato canale sia collegato al Cremlino o sia editorialmente pro-Cremlino, oppure che abbia intenzionalmente cercato di disinformare», in *euvsdisinfo.eu.*

[31] M. Castellaneta, *La libertà di stampa nel diritto internazionale ed europeo*, Bari, 2012, 197.

Non v'è dubbio, allora, del salto di qualità di cui si è detto precedentemente, il quale si è realizzato, come sempre più frequentemente accade, proprio sul piano delle relazioni esterne. A seguito degli atti adottati ai fini della sospensione delle agenzie di informazione russe, i contenuti controversi da queste riportati - tra cui spiccava, in particolare, il controverso discorso che il Presidente Putin ha tenuto il 22 febbraio 2022 in occasione del riconoscimento da parte della Duma di Stato delle Repubbliche di Donetsk e di Lugansk sulle cause dell'aggressione e sulle sue finalità- non sono più presenti sulla piattaforma: il loro contenuto, d'altronde, non necessita più di essere smentito essendo stato reso automaticamente indisponibile.

Viceversa, il controllo sulla moderazione dei contenuti rimane uno dei pilastri della lotta alla disinformazione nella sua dimensione interna. Questa ha preso avvio in vista delle elezioni al Parlamento europeo del maggio del 2019 al fine di proteggerle dalle interferenze esterne, con l'adozione di una prima Comunicazione della Commissione nell'aprile del 2018 intitolata «Contrastare la disinformazione online: un approccio europeo» ed una seconda del dicembre dello stesso anno contenente un «Piano d'azione contro la disinformazione»[32].

A questo primo pacchetto di misure si sono poi aggiunti una serie di strumenti di *soft law*, quali il Codice di buone pratiche dell'UE sulla disinformazione che è stato recentemente oggetto di modifica[33] e il Codice di condotta per lottare contro le forme illegali di incitamento all'odio online[34], i quali vanno letti alla luce del Piano d'azione per la democrazia europea[35] e della proposta di regolamento relativo a un mercato unico dei servizi digitali[36].

Per le grandi piattaforme, come per il social media *Twitter* e la piattaforma di condivisione di video YouTube, il nuovo Codice di buone pratiche, così come la proposta di regolamento nota come *Digital Service Act*, modifica significativamente il loro ruolo

[32] Rispettivamente, Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni «Contrastare la disinformazione online: un approccio europeo», COM/2018/236 final e Comunicazione congiunta della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni Piano d'azione contro la disinformazione, (JOIN(2018) 36 final).

[33] Codice rafforzato di buone pratiche dell'UE sulla disinformazione, 2022. Per dei primi commenti si v. M. Monti, *Lo strengthened Code of Practice on Disinformation: un'altra pietra della nuova fortezza digitale europea?*, in questa *Rivista*, 2, 2022, 317 ss.; G. Caggiano, *Il contrasto alla disinformazione tra nuovi obblighi delle piattaforme online e tutela dei diritti fondamentali nel quadro del Digital Service Act e della co-regolamentazione*, in *Papers di diritto europeo*, 1, 2021, 45 ss. e P. Cavaliere, *The Truth in Fake News: How Disinformation Laws Are Reframing the Concepts of Truth and Accuracy on Digital Platforms*, in *Edinburgh School of Law Research Paper*, 12, 2022.

[34] Codice di condotta per lottare contro le forme illegali di incitamento all'odio online.

[35] Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni sul piano d'azione per la democrazia europea, COM/2020/790 final. Inoltre il piano d'azione si propone di migliorare gli strumenti di cui l'UE dispone per lottare contro le interferenze straniere, presentando la possibilità di introdurre nuovi strumenti che consentano di imporre sanzioni finanziarie ai Governi responsabili di propaganda.

[36] Si v. in particolare gli artt. 5, par. 1, e 8, par. 1, della proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (DSA) e che modifica la direttiva 2000/31/CE, COM/2020/825 final, che disciplinano le ipotesi in cui *cade* l'esenzione dalla responsabilità. Si v. sul tema C. Caggiano - G. Contaldi - P. Manzini (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021.

affinché esse si impegnino, rispettivamente, a non trarre proventi dall'attività di disinformazione, ad aumentare la trasparenza della pubblicità politica e della pubblicità tematica, a garantire una copertura completa dei comportamenti manipolativi attuali ed emergenti, ad ampliare rafforzare gli strumenti che consentono agli utenti di individuare e a segnalare contenuti falsi o fuorvianti, ad aumentare la copertura delle azioni di verifica dei fatti in tutti i paesi dell'UE e nelle loro lingue e, infine, a fornire ai ricercatori un maggiore accesso ai dati, nell'ottica di una co-regolamentazione degli obblighi e delle responsabilità su di esse gravanti.

Del monitoraggio del codice di buone pratiche è incaricato ERGA, ovvero lo *European Regulators Group for Audiovisual Media Services* istituito dalla direttiva sui servizi di media audiovisivi, congiuntamente al nuovo *European Digital Media Observatory* e alla Commissione[37]. Il ruolo di ERGA si spiega alla luce del fatto che il controllo dei contenuti audiovisivi, indipendentemente dalla piattaforma di trasmissione, è materia che rientra tradizionalmente nella rispettiva direttiva sui media audiovisivi, recentemente modificata proprio al fine di rafforzare la protezione degli utenti, in particolare di quelli più vulnerabili come i minori, e di estendere le regole concernenti i contenuti illegali e i discorsi di incitamento alla violenza e all'odio anche alle piattaforme di condivisione dei video e ai contenuti audiovisivi contenuti su determinati servizi di social media[38].

Il processo di recepimento di questa direttiva da parte degli Stati membri, soprattutto con riferimento alla regolamentazione dei contenuti di incitamento alla violenza e all'odio è risultato piuttosto difficile[39], dato il non perfetto allineamento di vedute da parte di tutti gli Stati membri[40], né di una chiara comprensione del problema da parte della società civile europea[41].

Così, ad esempio, la legge francese di trasposizione della direttiva è stata cassata dal *Conseil Constitutionnel*, nella sua funzione di controllo *ex ante* della costituzionalità delle leggi, in particolare sotto il profilo della mancata necessità e proporzionalità di una legge che, per come novellata dal legislatore nazionale, imponeva ai fornitori di servizi di ritirare i contenuti illegali alla sola domanda dell'amministrazione competente, senza garantire la possibilità di un ricorso effettivo[42].

In un'ottica diametralmente opposta, la Lituania ha invece presentato nel 2021 un progetto di legge[43] volto a rafforzare la «Legge sull'informazione pubblica», proibendo la

[37] Measure 40.5 Strenghtened code of practice, 2022, cit.

[38] Modificata dalla Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018. Si v. sul punto E. Apa - G. Abbamonte - O. Pollicino (a cura di), *Il nuovo quadro regolamentare del mercato audiovisivo europe*o, Torino, 2020.

[39] Sebbene il termine per il recepimento negli ordinamenti nazionali della direttiva sui media audiovisivi fosse fissato al 19 settembre 2020, solo la Danimarca, i Paesi Bassi, la Svezia e l'Ungheria hanno notificato le misure di recepimento e confermato la completezza della notifica. Per questo la Commissione ha avviato, in data 23 novembre 2020, 23 procedimenti di infrazione, ec.europa.eu/commission/presscorner/detail/it/ip_20_2165.

[40] Anche nello spazio europeo si oppone la visione di una «democrazia militante» e quella di una «tollerante», su cui si v. G. Pitruzzella, O. Pollicino, *Hate Speech*, cit.

[41] A cui la Commissione europea cerca di ovviare con l'uso delle consultazioni pubbliche.

[42] Conseil Constitutionnel, Décision n° 2020-801 DC du 18 juin 2020, Loi visant à lutter contre les contenus haineux sur internet, § 7-9.

[43] European audiovisual Observatory, *Mapping of national rules applicable to video-sharing platforms: illegal*

pubblicazione di contenuti che incitino «alla propaganda di guerra, alla guerra e alla violazione della [sua] sovranità»[44]. Qui la connessione tra propaganda e guerra e dunque, in senso più ampio, tra disinformazione e relazioni esterne è esplicitamente posta.

3. La lotta alla disinformazione nelle relazioni esterne dell'Unione: Le misure restrittive applicate all'ambito dei media e dell'informazione controllati da Stati terzi

Il salto di qualità, come lo abbiamo definito, sancito dagli atti oggetto di analisi pone una serie di profili problematici, innanzitutto derivanti dal carattere inedito delle misure di sospensione adottate, le quali rappresentano per estensione e intensità delle evidenti novità nel panorama delle misure restrittive sin ora adottate dall'Unione[45].
Gli aspetti problematici che esse sollevano sono oggetto in questo paragrafo di particolare attenzione sia sotto il profilo all'adeguatezza della base giuridica utilizzata e della interazione che essa produce tra PESC e settore dei media e dell'informazione, sia dal punto di vista del possibile contenzioso e dei motivi suscettibili di essere sollevati in sede di sindacato giurisdizionale per farne valere l'illegittimità[46].
A tale proposito occorre sin d'ora menzionare che la società *RT France* ha presentato un ricorso d'annullamento del regolamento 350/2022, sulla base del diritto all'impugnazione che il diritto dell'Unione le riconosce ai sensi dell'art. 275, par. 2, TFUE. Insieme al ricorso d'annullamento ha anche presentato una domanda di provvedimenti urgenti sulla quale il Tribunale dell'Unione europea si è già pronunciato[47]. Nella sua ordinanza, il Presidente del Tribunale ha rigettato la domanda di sospensione della decisione impugnata, non ritenendo cumulativamente soddisfatte le condizioni relative all'urgenza e al pregiudizio grave e irreparabile[48], presupposti che, per giurisprudenza

and harmful content online, 26 October 2021, 308-309.

44 Trad. dell'Autore. L'art. 19, c. 1 della Public Information Law recita: «*It shall be prohibited to publish in the media information if: … war propaganda is incited, and the soveregnity of the Republic of Lithuania is forcibly violated*».

45 Così già S. Poli, *La portata e i limiti delle misure restrittive dell'Unione europea nel conflitto tra Russia e Ucraina*, in *SidiBlog*, 22 marzo 2022; e anche S. Lattanzi, *Il Consiglio sanziona "la propaganda del Cremlino" e sospende le attività di diffusione dell'agenzia di informazione Sputnik e del canale RT/Russia Today*, in *Quaderni Aisdue*, 1, 2022, 343 ss.

46 Sul punto si v. anche L. Ciliberti, *Free flow of information,* cit.

47 Sentenza *RT France/Consiglio*, cit. Per un commento si v. A. Maffeo, *Misure restrittive contro la Russia: il Tribunale rigetta la richiesta di sospensione di RT France*, in *Eurojus,* 2022 e C. Di Turi, *Il conflitto in Ucraina e la propaganda di guerra,* cit.

48 Ivi, § 31: «*en l'espèce, du point de vue social, les données fournies par la requérante ne permettent pas de comprendre le nombre d'emplois directement menacés à court terme, la date à laquelle la requérante cesserait de disposer des fonds nécessaires pour rémunérer ses employées, ainsi que les contours du plan social que la requérante serait susceptible de mettre en place, notamment en termes de possibilités de redéploiement ou de réembauche du personnel affecté. Dès lors qu'il n'est pas possible d'apprécier si le préjudice invoqué par la requérante a une dimension sociale, il convient de conclure que le préjudice est d'ordre purement économique et financier*». Con la conseguenza che un pregiudizio finanziario non è irreparabile: «*À cet égard, il importe de rappeler que, selon une jurisprudence constante, un préjudice d'ordre pécuniaire ne saurait, sauf circonstances exceptionnelles, être considéré comme irréparable, une compensation pécuniaire étant, en règle générale, à même de rétablir la personne lésée dans la situation antérieure à la survenance du préjudice. Un tel préjudice pourrait notamment être réparé dans le cadre d'un recours en indemnité introduit sur la base des articles*

costante, sono necessari all'emanazione di provvedimenti urgenti[49]. In fase di revisione delle bozze di questo scritto, si segnala inoltre che anche la Grande sezione del Tribunale si è, il 27 luglio del 2022, per la prima volta con rito accelerato, pronunziata sulla validità della misura. Questa non ha rilevato profili di incompatibilità né sotto il profilo della competenza del Consiglio ad agire in tale materia, né sotto quello della violazione dei diritti alla difesa della ricorrente, né, infine, in merito al rispetto degli artt. 11, 16 e 17 della Carta dei diritti fondamentali dell'Unione europea[50].

Numerosi sono tuttavia i profili problematici che permangono su un piano più sistematico e generale. Quelli che occorre qui segnalare possono essere suddivisi in tre principali categorie. La prima afferisce alla tipologia della misura di sospensione adottata, identificabile guardando al suo oggetto e al suo ambito di applicazione soggettivo. Su quest'ultimo profilo si innesta quello, strettamente connesso, dell'estensione della tutela giurisdizionale e dei possibili profili di illegittimità della misura. In ultimo, gli atti adottati risultano essere problematici dal punto di vista della loro implementazione e della corretta suddivisione dei compiti spettanti alle autorità nazionali e a quelle sovranazionali.

Analizzando il primo profilo controverso, occorre ricordare che le misure restrittive possono essere adottate, conformemente all'art. 215 TFUE, ai fini di dare applicazione a una risoluzione onusiana o quali misure "autonome". Esse possono essere rivolte sia contro uno o più Stati terzi (art. 215, c. 1) sia nei confronti di persone fisiche o giuridiche, di gruppi o di entità non statali (art. 215, c. 2)[51].

In assenza di una definizione espressa nei Trattati della nozione di "misura restrittiva"[52], nella prassi è invalsa la pratica di adottare sanzioni tendenzialmente di natura economico-finanziaria nei confronti degli Stati terzi, lasciando invece che le misure individuali colpiscano vari soggetti in ambiti tra loro molto disparati[53].

Fino ad ora, le tipologie di misure sanzionatorie adottabili dall'Unione potevano essere economiche, finanziarie, settoriali e individuali[54]. In particolare, queste ultime sembrano però aver subito dei mutamenti incrementali a seguito dell'aggressione russa dell'Ucraina, tanto da essere state correttamente ulteriormente suddivise in tre

268 et 340 TFUE».

[49] Ivi, §21: «*Ainsi,le sursis à exécution et les autres mesures provisoires peuvent être accordés par le juge des référés s'il est établi que leur octroi est justifié à première vue en fait et en droit (fumus boni juris) et qu'ils sont urgents, en ce sens qu'il est nécessaire, pour éviter un préjudice grave et irréparable aux intérêts dela partie qui les sollicite, qu'ils soient édictés et produisent leurs effets avant la décision dans l'affaire principale. Ces conditions sont cumulatives, de telle sorte que les demandes de mesures provisoires doivent être rejetées dès lors que l'une d'elles fait défaut. Le juge des référés procède également, le cas échéant, à la mise en balance des intérêts en présence*».

[50] Trib. UE, T-125/22, *RT France/Consiglio* (2022).

[51] Si v. sul punto S. Poli, *Le misure restrittive autonome dell'Unione europea*, Napoli, 2019 e M.E. Bartoloni - S. Poli, *L'Azione esterna dell'Unione europea*, Napoli, 2022.

[52] Ciò da cui si ingenera una certa confusione, soprattutto in merito alla loro distinzione tra queste e le contromisure internazionali, sul punto C. Morviducci, *Le misure restrittive dell'Unione europea e il diritto internazionale: alcuni aspetti problematici*, in *Eurojus*, 2019, 77 ss.

[53] F. Giumelli - F. Hoffmann - A. Książczaková, *The when, what, where and why of European Union sanctions*, in *European security*, 2021, 1 ss.

[54] Così anche sul sito del Consiglio nella sua "spiegazione" dei sei pacchetti adottati, su *consilium.europa.eu*.

gruppi[55] a seconda che esse riguardino «membri del governo, alti funzionari militari, dirigenti di media (*Russia Today*), e altre entità (quali banche statali), per una serie eterogenea di attività da essi condotte in Crimea a sostegno della politica governativa russa in tale territorio e in violazione dell'integrità territoriale ucraina»[56]; membri di organi statali «in quanto responsabili diretti della decisione assunta in violazione di obblighi internazionali»[57] e infine una «cerchia di persone non direttamente coinvolte nelle violazioni di cui sopra», ma che «traggono vantaggio dal governo o lo sostengono»[58].

Gli atti di esecuzione delle misure in oggetto non precisano, conformemente alla prassi invalsa, il paragrafo dell'art. 215 TFUE facente da base giuridica, operando un rinvio generale all'intero articolo. Tuttavia, i successivi allegati n. XV del regolamento 2022/350 e n. VI del regolamento (UE) 2022/879 stilano la lista dei «soggetti sanzionati», da cui dovrebbe evincersi in maniera pacifica la natura individuale della misura adottata[59].

Questa potrebbe, tipologicamente, essere considerata una misura individuale *ed* economica, considerando che il regolamento in questione modifica il precedente regolamento 833/2014 avente ad oggetto restrizioni nell'accesso ai mercati dei capitali, della difesa, dei beni a duplice uso e delle tecnologie sensibili. La ascrizione di questa nuova misura nel novero di quelle di natura economica risulta insoddisfacente alla luce del fatto che i servizi di informazione sono servizi economici che svolgono una attività culturale[60].

In secondo luogo, e in maniera ancora più evidente, è l'estensione individuale della misura a risultare particolarmente problematica. Fino ad ora le pur numerosissime misure restrittive individuali adottate dall'Unione nei confronti della Russia erano state rivolte nella maggior parte dei casi verso individui aventi una statura tale da poter assumere una responsabilità, diretta o indiretta, nell'aggressione militare dell'Ucraina. L'esistenza di un legame funzionale tra la commissione diretta o indiretta di un illecito internazionale quale quello della compromissione dell'integrità territoriale di uno Stato e la misura adottata individualmente nei confronti di singoli attori statali o non statali è stata ritenuta fondamentale da parte della Corte di giustizia in passato e potrebbe esserlo di nuovo in futuro, nel caso in cui si dovesse pronunciare in sede di appello sulla correttezza del ragionamento seguito dal Tribunale nella sentenza *RT/France*. L'esito di questa valutazione dipenderebbe anche dalla *necessarietà* della stessa, ovvero dalla sua concreta capacità di raggiungere nel medio e lungo periodo (essendo

[55] In S. Poli, *La portata e i limiti...*, cit. e, più in generale, Id., *Le misure restrittive e la tutela dei diritti dei singoli*, in M.E. Bartoloni - S. Poli (a cura di), *L'Azione esterna dell'Unione europea*, cit., 263 ss.

[56] Il riferimento è alla decisione (PESC) 2022/265 del Consiglio e al regolamento di esecuzione (UE) 2022/260 del Consiglio.

[57] Il riferimento è alla decisione (UE) 2022/267 e al regolamento (UE) 2022/261.

[58] Il riferimento è alla decisione (PESC) 2022/329 del Consiglio art. 1(1) e). Così la decisione (PESC) 2022/337 del Consiglio.

[59] Si v. per analogia, Trib. UE, T-798/14, *DenizBank/Consiglio* (2018), § 73 e CGUE, C-72/15, *Rosneft* (2017), §100 e 119.

[60] Si v. R. Mastroianni, *Competenze normative dell'Unione europea e disciplina del pluralismo informative: regolazione o concorrenza nel settore audiovisivo?*, in R. Pisillo Mazzeschi - A. Del Vecchio - M. Manetti, P. Pustorino (a cura di), Il diritto al pluralismo in Europa e in Italia, Roma, 2012, 179 ss.

il breve già, invano, trascorso) lo scopo che essa si prefigge, il quale deve essere in linea con le finalità generali delle misure restrittive che devono essere volte ad «indurre a un cambiamento nella politica o nelle attività del paese, della regione di un paese, del governo, dell'entità o dei singoli cui sono dirette»[61].

Orbene, nella decisione e nel regolamento controversi le agenzie di stampa sono state accusate di fare da «cassa di risonanza»[62] della propaganda russa e dunque di agire al fine di destabilizzare la società civile dell'Unione e dei paesi limitrofi per il solo fatto di essere poste «sotto lo stabile controllo diretto o indiretto della leadership della Federazione russa»[63]. Nondimeno, gli atti in questione non specificano in virtù di cosa questo controllo sia esercitato, né in che modo concretamente questo controllo influisce sul contenuto degli articoli pubblicati[64]. Il Tribunale, sul punto, applicando un citerio poggiante «*sur une base factuelle suffisamment solide*»[65] ha verificato che la *società RT France* fosse posta sotto il controllo permanente, diretto o indiretto, della Federazione russa in base ad elementi tratti, rispettivamente, dall'origine finanziaria del suo capitale sociale e dallo scopo della società, per come delineato da alcuni dei suoi dirigenti in specifiche dichiarazioni pubbliche[66].

Tale legame appare dirimente sia sotto il profilo della necessarietà della misura (ovvero nel merito della fondatezza dei motivi), sia sotto il profilo della fondatezza, formale, della motivazione, ovvero sotto il profilo del rispetto dell'obbligo di motivazione prescritto ai sensi dell'art. 296, par. 2, TFUE.

Quest'articolo impone al Consiglio, nell'ambito dell'adozione di misure restrittive, di indicare «i motivi specifici concreti per i quali […] ritiene, nell'esercizio del suo potere discrezionale, che l'interessato debba essere assoggettato a una misura di questo tipo»[67]. Suddetto obbligo risponde «allo scopo, da un lato, di fornire all'interessato indicazioni sufficienti per giudicare se l'atto sia fondato oppure se sia eventualmente inficiato da un vizio che consenta di contestarne la validità dinanzi al giudice dell'Unione e, dall'altro lato, di consentire a quest'ultimo di esercitare il suo sindacato di legittimità su tale atto»[68]. In questo quadro il Consiglio è pertanto «tenuto a portare a conoscenza di una persona o di un'entità interessata da misure restrittive le ragioni specifiche e concrete per le quali ritenga che dette misure dovessero essere adottate»[69]. Inoltre, esso deve «menzionare gli elementi di fatto e di diritto da cui dipende la giustificazione giuridica delle misure di cui trattasi e le considerazioni che l'hanno indotto

[61] Orientamenti sull'attuazione e la valutazione delle misure restrittive (sanzioni) nel contesto della politica estera e di sicurezza comune dell'UE (aggiornamento), doc. 5664/18, 4 maggio 2018, 5 (§4) e 46.

[62] Settimo considerando del regolamento (UE) 2022/350 e della decisione (PESC) 2022/351.

[63] Ottavo considerando del regolamento (UE) 2022/350 e della decisione (PESC) 2022/351.

[64] Al di là della proprietà statuale russa della società. La società RT France, per esempio, è una «*société par action simplifiée*» di cui l'unico azionario è la Federazione russa. Per le informazioni societarie, in *infogreffe.fr*.

[65] Sentenza *RT France/Consiglio*, cit., § 170.

[66] Ivi, § 170.

[67] Trib. UE, T-565/12, *National Iranian Tanker Company/Consiglio* (2014), § 38.

[68] Trib. UE, T-262/15, *Kiselev* (2017), § 39.

[69] Ivi, § 40.

ad adottarle»[70].

Sulla base di tali criteri, il Tribunale ha ritenuto che il Consiglio avesse adempiuto all'obbligo di motivazione, iscrivendo il giornalista Dimitrii Kiselev negli allegati del regolamento 269/2014, in quanto egli era stato nominato direttore dell'agenzia di stampa *Rossiya Segodnya* con decreto del presidente russo e aveva «con le sue dichiarazioni di giornalista […] fatto propaganda a favore di azioni militari della Federazione russa in Ucraina»[71]. In tal caso la soluzione del Tribunale, limitata alla valutazione, formale, della rispondenza all'obbligo di motivazione, sembra essere stata anche determinata dal fatto che l'intensità di quest'obbligo varia a seconda della natura dell'atto e, soprattutto, del «contesto» in cui la misura viene adottata[72]. Così in quel caso il Tribunale aveva ritenuto l'atto sufficientemente motivato a fronte del fatto che esso era stato emanato in un contesto noto all'interessato, quale quello dell'imminente annessione della Crimea e di Sebastopoli.

Tuttavia a fronte dell'estensione di queste misure, non più selettivamente indirizzate ad alcuni dei giornalisti di punta dei servizi di informazione russi, bensì a una persona giuridica nel suo complesso, la prova di un sostegno concreto alle azioni o alle politiche che compromettono o minacciano l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina o la stabilità e la sicurezza dell'Unione attraverso azioni di propaganda, in sé per sé non considerabili quali atti illeciti (poiché, come detto, la propaganda di guerra non rientra tra le manifestazioni del pensiero integranti contenuti illegali o discriminatori[73]), dovrebbe a nostro avviso risultare con estrema chiarezza.

Questa prova concreta non costituirebbe solo parte integrante dell'obbligo di motivazione che grava sul Consiglio, ma rappresenterebbe l'innesto causale su cui valutare le responsabilità connesse a una azione che con strumenti assai vari, intenzioni, fatti e opinioni, intende mistificare la realtà.

Questo elemento di responsabilità, seppure intesa in senso lato, appare fondamentale in un quadro sanzionatorio costruito attorno a una logica di tipo precauzionale, e non di tipo punitivo[74]. Se così non fosse, infatti, la sanzione dipenderebbe dal solo fatto di essere cittadini russi o di lavorare per società finanziate dalla Federazione russa, risultando così evidentemente discriminatoria[75].

Permane pertanto lecito chiedersi se, come sembra avvenire nella specie, il solo finanziamento pubblico da parte di uno Stato terzo, seppure aggressore, di società che

---

[70] Trib. UE, T-307/12 e T-408/13, *Mayaleh/Consiglio* (2014), § 86 e giurisprudenza citata.

[71] Sentenza *Kiselev*, cit., § 45 e 48.

[72] Ivi, § 41.

[73] Nel diritto italiano esiste il reato di propaganda fascio-nazista disciplinato all'art. 604-*bis*, c. 3, c.p. Questo reato deve essere assimilato ai reati di pericolo concreto secondo M. Cuniberti, *Il buon costume e i reati di opinione*, in G. Vigevano (a cura di), *Diritto dell'informazione e dei media*, Torino, 2019, 171 ss. Sul punto si v. anche F. Donati, *Fake news e libertà di informazione*, in questa *Rivista*, 2, 2018, 440 ss.

[74] Per cui desta una certa preoccupazione il comunicato stampa del 30 giugno 2022, initolato *Sanctions: Council requests European Parliament consent to add the violation of restrictive measures to the list of EU crimes*.

[75] Nota S. Poli che in questo caso «a differenza delle sentenze rese nei ricorsi presentati da Kiselev e Cabello Róndon, il Tribunale ha dimostrato con esempi concreti i motivi per cui non è eccessivo restringere la libertà di espressione della ricorrente, considerata la qualità delle informazioni fornite», in S. Poli, *Prime riflessioni sulla sentenza del Tribunale "RT France" sulle misure restrittive contro le attività di disinformazione russe*, in *I Post di Aisdue*, 5 settembre 2022, 126.

operano stabilmente nel territorio dell'Unione e che hanno sulla base di questo diritto ottenuto le licenze necessarie allo svolgimento di un sevizio di informazione, costituisca una motivazione sufficiente all'iscrizione nelle liste; o se, invece, non dovrebbero fornirsi ulteriori specificazioni dal punto di vista dell'accuratezza dei fatti che hanno condotto all'iscrizione nell'allegato[76].

A nostro modo di vedere, questi fatti dovrebbero attenere alla prova di specifiche e costanti pressioni governative sulle scelte editoriali effettuate dalle agenzie di stampa[77]; criterio, questo, che risulta peraltro maggiormente in linea con la regolamentazione applicata ai servizi di informazione in virtù della direttiva (UE) 2010/13 sui servizi di media audiovisivi.

Questa richiama il concetto di «responsabilità editoriale», in quanto «essenziale per la definizione del ruolo del fornitore di servizi di media»[78], definendolo, al suo art. 1, par. 1, lett. *c)*, come «l'esercizio di un controllo effettivo sia sulla selezione dei programmi sia sulla loro organizzazione in un palinsesto cronologico, nel caso delle radiodiffusioni televisive, o in un catalogo, nel caso dei servizi di media audiovisivi a richiesta». Inoltre, gli Stati membri possono specificare ulteriormente questi concetti nei loro atti di trasposizione.

Passando poi dall'analisi dell'obbligo di motivazione a quello della fondatezza dei motivi, questione che attiene alla legittimità sostanziale dell'atto controverso, non va dimenticato che il Consiglio è tenuto ad agire conformemente al rispetto del diritto primario e dei diritti fondamentali sanciti dalla Carta, considerata la natura di fonte secondaria della decisione e del regolamento adottati in ambito PESC[79]. Pertanto, le

[76] Conformemente a quanto stabilito dalla giurisprudenza, CGUE C-280/12 P, *Consiglio/Fulmen e Mahmoudian* (2013), § 58.

[77] D'altronde questo sembra avvenire con maggiore rigore nelle sanzioni «propriamente individuali» adottate, *inter alia*, in virtù della decisione (PESC) 2022/337 del Consiglio del 28 febbraio 2022 che modifica la decisione 2014/145/PESC concernente misure restrittive relative ad azioni che compromettono o minacciano l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina nei confronti del sigor Tigran Keosayan, è specificato come si tratti di giornalista «che ha diffuso propaganda anti-ucraina nei media russi. Nel suo show televisivo finanziato dallo Stato "International Sawmill with Tigran Keosayan" (segheria internazionale con Tigran Keosayan), ha costantemente ritratto l'Ucraina come un paese debole e corrotto, che si manteneva solo grazie all'aiuto occidentale. Ha suggerito che le autorità ucraine non erano legittime. Ha ripetutamente dichiarato che la Crimea apparteneva alla Russia e che il Donbas non faceva parte dell'Ucraina. Il sig. Keosayan ha partecipato al forum "Donbas russo" che è stato organizzato dalle autorità della cosiddetta "Repubblica popolare di Donetsk" nel Donetsk con lo scopo di diffondere la dottrina del "Donbas russo". Ha pubblicamente accusato l'Ucraina dell'escalation del conflitto. Pertanto, è responsabile di sostenere attivamente o realizzare azioni o politiche che compromettono o minacciano l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina, nonché la stabilità e la sicurezza in Ucraina». O, ancora, la giustificazione nell'elenco di Margarita Simonyan considerata «una figura centrale della propaganda del governo. È anche caporedattore della rete televisiva di informazione in lingua inglese RT (Russia Today). Attraverso il suo ruolo ha promosso un atteggiamento positivo nei confronti dell'annessione della Crimea e delle azioni dei separatisti nel Donbas. Ha pertanto fornito sostegno ad azioni e politiche che compromettono l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina» in virtù della decisione (PESC) 2022/265 del Consiglio, del 23 febbraio 2022, che modifica la decisione 2014/145/PESC concernente misure restrittive relative ad azioni che compromettono o minacciano l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina.

[78] Considerando 25 della direttiva (UE) 2010/13.

[79] Sebbene la natura della decisione adottata dal Consiglio non sia equiparabile a quelle iscritte dall'art. 288 TFUE, per cui ci permettiamo di rinviare a S. Lattanzi, *Nello scenario post-Brexit il Tribunale offre dei*

misure restrittive dovrebbero, come peraltro menzionano gli stessi atti controversi, rispettare il diritto alla libertà di espressione e di informazione stabilito all'art. 11 della Carta[80].

Si tratta di un diritto non assoluto la cui possibile restrizione deve essere valutata sotto i profili della necessità, proporzionalità e giustificazione della misura[81], alla luce del contesto in cui la restrizione si è verificata[82].

A tal fine, gli atti in questione specificano la natura temporanea della sospensione[83] e sottolineano l'eccezionalità del contesto da cui traggono origine. In queste circostanze, le limitazioni alle libertà individuali[84] risentono tradizionalmente di un bilanciamento suscettibile di pendere verso la protezione di interessi diffusi e collettivi, quale quello della sicurezza pubblica[85]. Il contesto bellico è ripetutamente richiamato dagli atti oggetto di esame, i quali considerano che la diffusione della popaganda a mezzo dei canali oggetto di sanziona costituisca la manifestazione di una Guerra ibrida condotta dalla Russia direttamente contro la popolazione europea a colpi di fatti non veritieri e di mistificazioni della realtà. Tale contesto, inoltre, è stato richiamato dal Tribunale, il quale lo ha definito «*extraordinaire*»[86].

E tuttavia, pure in tale contesto, desta tuttavia una certa preoccupazione il richiamo al concetto di «minaccia ibrida»[87] per qualificare alcune attività giornalistiche. Questo è infatti un concetto che deriva dalla dottrina militare russa, la c.d. *dottrina Gerasimov*[88], secondo cui le guerre contemporanee si combatterebbero su più fronti non solo per mezzo di strumenti tradizionali ma anche utilizzando soggetti non appartenenti ai

chiarimenti in merito alla natura dell'accordo di recesso e delle decisioni ad esso relative, in *Quaderni Aisdue*, 1, 2021, 211 ss.

[80] In base al quale: «Ogni individuo ha diritto alla libertà di espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera».

[81] Conformemente a quanto prevede l'art. 52, par. 1, della Carta dei diritti fondamentali. Sul tema si v. R. Cisotta, *Brevi note sulla giurisprudenza sull'articolo 52, par. 1 della della Carta dei diritti fondamentali dell'UE in materia di limitazioni ai diritti fondamentali …con uno sguardo in avanti*, in *Osservatorio sulle fonti*, 2021, 19 ss.

[82] Ciò permette, anche in periodi eccezionali, di utilizzare gli strumenti ordinari del sindacato sulla validità degli atti in quegli ordinamenti, come è anche quello europeo, che non prevedono apposite clausole di deroga all'ordine costituito. Questi strumenti hanno la capacità di essere già di per sè contestualizzati in presenza di eventi eccezionali, senza bisogno di essere sostituiti con strumenti ad hoc. Per un riferimento al diritto costituzionale italiano si v. M. Cartabia, *Relazione sull'attività della Corte nel 2019*, in *cortecostituzionale.it* e, per il diritto europeo, S. Vezzani, *La Carta dei diritti fondamentali negli Stati di emergenza*, in Aa. Vv., *Le situazioni emergenziali tra diritti e restrizioni. L'esigenza di un approccio precauzionale alla gestione delle emergenze*, Torino, 2022, 39 ss.

[83] La quale doveva durare fino al 31 luglio 2022 o, in alternativa, poteva essere prolungata, come sembra essere, sino alla fine del conflitto, conformemente a quanto previsto ai sensi dell'art. 9 della Decisione (PESC) 351/2022 di modifica della Decisione (PESC) 512/2014.

[84] Ma la libertà di stampa e di informazione conosce anche un altro *volet*, di cui ci occuperemo nell'ultimo capitolo.

[85] In generale si v. sul tema C. Schepisi (a cura di), *Le risposte del diritto in situazioni di emergenza tra ordinamento italiano e dell'Unione europea*, Torino, 2021.

[86] Sentenza *RT France/Consiglio*, cit., § 86, 198 e 213.

[87] P. Pawlak, *Understanding hybrid threats*, in *European Parliamentary Research Services,* 24 giugno 2015.

[88] Nome coniato da M. Galeotti, *The mythical 'Gerasimov Doctrine' and the language of threat*, in *Critical Studies on Security*, 2019, 157 ss.

ranghi militari[89]. Questa dottrina originata da un paese ostile sembra essere condivisa dalla stessa Unione, che si sta adoperando a combattere tali minacce sotto vari fronti[90]. Il richiamo alla guerra, seppure ibrida, consente di giustificare tali decisioni sotto il profilo dell'obiettivo primario di tutelare l'ordine pubblico e la sicurezza dell'Unione. Coerentemente, il perseguimento di un tale scopo e la predisposizione dei relativi mezzi per farvi fronte spostano il piano del discorso da quello della legittimità e del bilanciamento con beni costituzionalmente protetti - quali quelli del pluralismo dell'informazione a quello della sicurezza pubblica- a quello delle ingerenze straniere oggi anche declinato sul piano sovranazionale[91].

È solo in questa prospettiva, infatti, che ci pare possibile trattare gli operatori in questione non più come giornalisti che producono servizi informativi, bensì come spie di Stati esteri la cui voce non costituisce un elemento di arricchimento dell'arena democratica[92], bensì la diffusione di idee pericolose per la sicurezza e la tenuta dell'ordine costituzionale.

Non è un caso che proprio seguendo questa logica già nel 2017 *RT America* sia stata costretta a registrarsi in tale Stato quale agente straniero presso il Dipartimento di Giustizia degli Stati Uniti, conformemente a quanto previsto dal «*Foreign Agents Registration Act*»[93]. In ambito italiano, è notizia degli ultimi giorni rispetto al momento in cui scriviamo che è stata condotta una indagine da parte del Copasir (Comitato parlamentare per la sicurezza della Repubblica) che, su incarico della Commissione di vigilanza RAI, ha stilato un bollettino sulla disinformazione in Italia, in cui compaiono i nomi di numerosi giornalisti e di un parlamentare. Questi soggetti sono finiti nell'indagine di un organo quale il Copasir, istituito al fine di verificare che «l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione, delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni»[94], per il rischio che non si tratti di veri e propri giornalisti, bensì di infiltrati[95].

Questa sovrapposizione tra l'ambito della sicurezza e quello dell'informazione, già messa in luce dal recente «Piano d'azione per la democrazia europea», il quale sotto-

[89] N. Cristadoro, *La dottrina Gerasimov e la filosofia della guerra non convenzionale nella strategia russa contemporanea*, Solarussa, 2022.

[90] Da ultimo, la già citata decisione (PESC) 2019/797 del Consiglio del 17 maggio 2019 concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri e il regolamento (UE) 2019/796.

[91] Questo attacco alla sicurezza dovrebbe peraltro essere transfrontaliero considerando che, come specifica lo stesso *Joint Framework on countering hybrid threats*, cit., la lotta contro le minacce ibride attiene alla sicurezza e alla difesa nazionale e al mantenimento dell'ordine pubblico, la cui responsabilità principale ricade sugli Stati membri.

[92] O. Pollicino, *Fake News, Internet and Metaphors (to Be Handled Carefully)*, in quesa *Rivista*, 1, 2017, 24-25 e anche Id., *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, ivi, 1, 2018, 48 ss.

[93] Su cui si v. S. Jaroszynski, *Defending the Right to Know: The Foreign Agent Registration Act and the Fight Against Disinformation,* su *commlawreview.org* e K.D. Schafer, *The Foreign Agents Registration Act in the Age of the Russian Federation: Combating Interference by Russian Media in the United States*, in *Southwestern's Journal of International Law*, 2019, 447 ss.

[94] Art. 30, c. 2 della legge n. 124/2007.

[95] Secondo un articolo pubblicato dalla redazione dell'ANSA, il Copasir dovrebbe rispondere al quesito se «i cronisti ospitati possano essere considerati funzionari del Cremlino ed eventualmente espressione dei servizi segreti, e se ciò metta a rischio la sicurezza nazionale».

lineava l'esistenza di «ingerenze straniere nello spazio informativo, che spesso si verificano nell'ambito di un'operazione ibrida più ampia»[96] e recentemente ripresa dalla relazione del Parlamento europeo «sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione»[97], ha delle ripercussioni anche rispetto alla corretta ripartizione dei compiti relativi all'implementazione delle misure restrittive in oggetto.

In base alla lettera dei regolamenti esecutivi delle decisioni PESC, l'attuazione delle misure deve essere assicurata dal Consiglio in coordinamento operativo con ERGA. L'implementazione solleva allora dei dubbi in merito alla corretta ripartizione di competenze tra questo e gli Stati membri ai sensi dell'art. 40 TUE, considerando che, se non ci fosse il rischio alla sicurezza, la sospensione delle licenze degli organi di informazione rientrerebbe senza ombra di dubbio nel novero della competenza degli Stati membri e delle rispettive autorità garanti delle comunicazioni, in base agli articoli dal 3 al 9 della direttiva.

Così era già avvenuto l'anno scorso, allorquando la Lettonia aveva deciso di sospendere la trasmissione sul suo territorio del canale TV *Rossiya RTR*, conformemente a quanto previsto dal secondo comma dell'art. 3 della direttiva (UE) 2010/13[98]. Secondo le autorità statali, il canale TV in questione trasmetteva contenuti di istigazione alla violenza o all'odio, in violazione dell'art. 6, c. 1, lett. *a)* della direttiva[99].

La Commissione, chiamata a valutare la compatibilità di questa decisione alla luce della direttiva, l'ha considerata legittima alla luce del carattere grave, evidente e serio delle violazioni commesse dalla TV russa[100], ma solo a seguito di un complesso procedimento di valutazione caratterizzato da una consultazione amichevole con lo Stato membro avente giurisdizione sul fornitore di servizi di media (in quel caso la Svezia) e la Commissione, suscettibile anche di chiamare eventualmente in causa un parere dell'ERGA, da formularsi ai sensi dell'art. 3, c. 2, lett. *d)* della direttiva. Queste garanzie procedimentali sono anche garanzie sostanziali in una materia, quale quella dell'audiovisivo, così politicamente sensibile e in cui entrano in gioco principi e valori diversi a seconda dell'ordinamento costituzionale in cui ci si colloca[101].

---

[96] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni sul piano d'azione per la democrazia europea, COM/2020/790 final, 20.

[97] Relazione del Parlamento europeo sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione/ 8.2.2022 – (2020/2268(INI)).

[98] La Lettonia aveva precedentemente già sospeso questo canale nel 2019. Essa aveva, inoltre, nel 2015, nel 2017 e nel 2018 sospeso la trasmissione del canale TV RTR Planeta.

[99] Ai sensi di tale articolo: «1. Fermo restando l'obbligo degli Stati membri di rispettare e proteggere la dignità umana, gli Stati membri assicurano mediante appositi mezzi che i servizi di media audiovisivi erogati dai fornitori di servizi di media soggetti alla loro giurisdizione non contengano: a) istigazione alla violenza o all'odio nei confronti di un gruppo di persone o un membro di un gruppo sulla base di uno dei motivi di cui all'articolo 21 della Carta; b) alcuna pubblica provocazione a commettere reati di terrorismo di cui all'articolo 5 della direttiva (UE) 2017/541».

[100] Decisione della Commissione europea del 7 maggio 2021 «*on the compatibility of the measures adopted by Latvia pursuant to Article 3(2) of Directive 2010/13/EU of the European Parliament and of the Council to restrict retransmission on its territory of an audivisual media service from another Member State*», C(2021) 3162 final.

[101] Similmente, è stata l'autorità garante delle comunicazioni tedesca a decidere di sospendere in Germania la diffusione del canale TV RT/Russia Today, solo quale giorno prima dello scoppio della

Inoltre, per bloccare la diffusione dei contenuti prodotti dalle due agenzie sulle piattaforme on-line e sulle apposite app sono state introdotte richieste legali di sospensione direttamente ai giganti delle Big-Tech[102], in quanto «operatori» interessati ai sensi dell'art. 2 *septies* del regolamento (UE) 2022/350[103].
Sia i social media come Twitter, sia i motori di ricerca come Google hanno accolto tali richieste e hanno pertanto proceduto a oscurare i contenuti informativi banditi. In un'ottica ancora di auto-regolazione, in pendenza dell'entrata in vigore del *DSA* e dell'applicazione del Codice di condotta rafforzato, nel marzo del 2022 le società in questione hanno dato immediatamente seguito a questa richiesta, avendo probabilmente ritenuto violati i loro «Termini di servizio». Di conseguenza, il risultato così ottenuto non sembra essere stato imposto in virtù di un obbligo giuridico cogente, quanto piuttosto grazie a una scelta discrezionale delle stesse piattaforme private. D'altronde suddetta richiesta, al momento in cui è intervenuta, non poteva ancora ancorarsi su nessun obbligo giuridico[104], a meno di non considerare il contenuto prodotto dalle agenzie russe come illegale ai sensi delle decisioni PESC e dei regolamenti citati. Ciò tuttavia costituirebbe una deroga al principio di neutralità imposto agli operatori digitali ai sensi dell'art. 15 della direttiva sul commercio elettronico e richiederebbe un'applicazione estensiva della direttiva sui media audiovisivi, con il rischio peraltro di non ottenere un risultato sufficientemente uniforme[105].

4. Conclusioni: l'"*infowar*" e i limiti del diritto sovranazionale

Le misure restrittive sono sempre produttive di effetti o esternalità meritevoli di essere considerate al fine di valutare complessivamente l'adeguatezza dello sforzo intrapreso dall'Unione per combattere la disinformazione sul piano delle relazioni esterne. È esploso negli ultimi mesi il dibattito relativo all'efficacia delle misure restrittive al settore energetico, da molti criticate per l'effetto negativo che esse sono in grado di produrre sull'approvvigionamento dei comparti industriali degli Stati membri.
Una riflessione non dissimile può essere proposta anche rispetto alle misure di sospensione degli organi di informazione russi. Infatti, anche questo genere di misure comporta delle esternalità tanto sul piano interno quanto su quello esterno. In merito a quest'ultimo, si segnala che la Federazione russa ha agito immediatamente in contromisura a seguito dell'adozione del terzo pacchetto di misure, chiudendo la sede moscovita dell'agenzia *Deutsche Welle* e annunciando l'adozione di due leggi pesantemente

guerra. Per cui si v. *politico.eu*.

[102] Facendo seguito alla *Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique*, 8 marzo 2022.

[103] Senza che la nozione di «operatori» sia definita nel regolamento in questione.

[104] Nella richiesta introdotta alle suddette società la Commissione ha fatto però valere l'esistenza della clausola di non elusione, iscritta all'art. 12 del regolamento (UE) 2022/350.

[105] Nella richiesta si legge: «*the decision to fully depart in the present Regulation from the E-commerce Directive has been a conscious one and justified on the ground of the situation and its temporary character*», in *lumendatabase.org*.

restrittive della libertà di stampa[106].

L'effetto domino della misura sanzionatoria sul piano interno e su quello esterno è certamente valutabile dal punto di vista politico e delle migliori strategie diplomatiche da adottare nei confronti di Stati terzi aggressori[107]. Nell'ambito del diritto dell'Unione, nondimeno, questo aspetto è anche valutabile in riferimento alla legittimità stessa delle misure adottate, considerando che queste sono vincolate a un esercizio del potere che sia conforme a quanto prescritto dalle rispettive basi giuridiche, nella specie fornite dagli artt. 215 TFUE e 29 TUE.

E l'art. 29, in particolare, pone dei limiti di contenuto alla decisione PESC, considerando che, come ha chiarito la giurisprudenza, nonostante l'ampio margine di discrezionalità di cui gode il Consiglio[108], questo non si traduce, nell'ambito del diritto dell'Unione europea, in un atto politico adottato in totale libertà[109], essendo la decisione PESC, presupposto del regolamento, vincolata a un obbligo di conformità con uno o più degli obiettivi elencati all'art. 21 TUE.

Orbene, l'effetto di impoverimento sul pluralismo e la libertà dei media ingenerato dai suddetti atti pone dunque, al di là della sfera politica, un problema giuridico importante dal punto di vista del diritto sovranazionale che si riflette in primo luogo nel problema della coerenza tra gli obiettivi che l'Unione persegue tanto sul piano interno quanto su quello esterno[110].

Sul piano esterno, il Trattato permette all'Unione di agire per perseguire una serie di obiettivi, tra cui figurano tanto la sicurezza dell'Unione[111], quanto il consolidamento e il sostegno della democrazia, dello Stato di diritto e dei diritti dell'uomo[112]. Occorre allora domandarsi, in primo luogo, se tra questi obiettivi intercorra una relazione gerarchica in base alla quale considerare l'uno prevalente sull'altro o se, invece, qualora essi siano considerati di pari rango, non sia necessario operare un ponderato bilanciamento, tenendo anche conto della lesione di obiettivi ugualmente legittimi e perseguibili sul piano delle relazioni esterne.

In secondo luogo, l'effetto domino colpisce sia il livello di tutela della libertà di stampa nella società russa sia in quella europea, considerando che tali misure incidono assai

---

106 en.kremlin.ru/acts/news/67908 e www.en.kremlin.ru/acts/news/67910.

107 È d'uopo sottolineare una differenza importante in merito alla eventuale simmetria/asimmetria delle contromisure adottate: la Federazione russa è formalmente in guerra con l'Ucraina mentre non lo sono i paesi europei né tantomeno l'Italia in cui lo Stato di guerra deve essere dichiarato secondo le forme prescritte all'art. art. 78 Cost e 87, nono comma Cost. Si tratta di una differenza importante se si pensa che anche molti ordinamenti occidentali conoscono l'introduzione di specifiche reati penali volti a punire la diffusione di notizie false in tempo di guerra (in Italia, ad esempio, l'art. 265 c.p.).

108 Sentenza *Rosneft*, cit., § 88.

109 «La decisione deve essere infatti conforme agli «scopi ed obiettivi della PESC, quali espressi all'articolo 3, paragrafo 5, TUE e all'articolo 21 TUE», ivi.

110 Sulla conformità e coerenza degli obiettivi dell'Unione sul piano delle relazioni esterne si v. E. Smith, *EU Foreign Policy in changing world*, Hoboken, 2014; P. Eeckhout - M. Lopez-Escudero (eds.), *The European Union's External Action in Times of Crisis*, London - New York - New Delhi - Oxford - Sydney, 2016; M. Cremona (eds.), *Structural principles in EU external relations law*, London - New York - New Delhi - Oxford - Sydney, 2018.

111 Art. 21, par. 2, lett. *a)*, TUE.

112 Art. 21, par. 2, lett. *b)*, TUE.

negativamente sulla libertà di stampa di prestatori di servizi stabilmente operativi sul territorio dell'Unione. Anche questa conseguenza imporrebbe una complessa opera di bilanciamento tra interessi collettivi e individuali talvolta opposti e talaltra intimamente legati tra loro. Infatti, se nel paragrafo precedente ci siamo limitati a richiamare l'aspetto "individualista" del diritto alla libertà di stampa e di informazione, occorre ricordare che a questo se ne aggiunge un altro di tipo "funzionalista"[113], in base al quale, come anche ripetutamente affermato dalla stessa Corte di giustizia, il diritto alla libertà di stampa non è un diritto che merita tutela solo di per sé, ma in quanto presupposto e fondamento di una società democratica[114], caratterizzata, come ricorda l'art. 2 TUE, dal pluralismo, dalla non discriminazione e dalla tolleranza[115].

Da un punto di vista procedurale, viene allora da domandarsi se questo accurato bilanciamento possa essere fatto d'urgenza, come imposto dall'adozione di misure restrittive, e in un quadro intergovernativo che limita fortemente la partecipazione del Parlamento europeo. Dal punto di vista sostanziale, se ciò sia coerente con i principi e i valori che l'Unione si preoccupa strenuamente di difendere sia *vis-à-vis* di Stati membri che di Stati terzi. Infatti, vedere libertà fondamentali costituzionalmente garantite cedere così facilmente dinanzi a esigenze di sicurezza *ibida* (perché *ibirida* è anche la minaccia), delinea un quadro che mal si confà al paradigma di democrazia militante che negli ultimi anni l'Unione ha incarnato sul piano delle relazioni esterne e che, sul piano interno, potrebbe facilmente essere rimesso in discussione, se non dalla Corte di giustizia, da parte delle Corti costituzionali degli Stati membri.

[113] *Inter alia*, M. Luciani, *La libertà di espressione, una prospettiva di diritto comparato: Italia*, in *Servizio Ricerca del Parlamento europeo*, ottobre 2019.

[114] CGUE, C-507/18, *Associazione Avvocatura per i diritti LGBTI* (2020), § 48: «Indubbiamente, la libertà di espressione, in quanto fondamento essenziale di una società democratica e pluralista rispecchiante i valori sui quali l'Unione si fonda, a norma dell'articolo 2 TUE, costituisce un diritto fondamentale garantito dall'articolo 11 della Carta». E non diversamente recentemente sentenza della Corte EDU, *Ozer/Turchia*, ric. 69270/12 (2020), § 40 sulla violazione dell'art. 10 CEDU, al quale le Spiegazioni della Carta rinviano.

[115] CGUE, C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.* (2020), § 114: «Tale diritto fondamentale, garantito dall'articolo 11 della Carta, costituisce uno dei fondamenti essenziali di una società democratica e pluralista, facente parte dei valori sui quali, a norma dell'articolo 2 TUE, l'Unione è fondata».

Dati sanitari e *e-Health* europea: tra trattamento dei dati personali e decisione amministrativa algoritmica*

Giuseppina Lofaro

Abstract

Il progressivo incremento del ruolo degli algoritmi nella società risulta di grande interesse nell'ambito sanitario. Il saggio presenta un'analisi tecnico-giuridica aggiornata, alla luce del recente dato normativo, dottrinale e giurisprudenziale, focalizzandosi su aspetti evolutivi ed elementi di criticità della valorizzazione dei dati sanitari nella prospettiva europea, tra informatizzazione (automazione) e ridefinizione del potere discrezionale, tra uso primario ed uso secondario dei dati, sottolineando la necessità di un algoritmo trasparente ed accessibile, specialmente quale condizione di correttezza delle decisioni amministrative assunte nei sistemi di IA qualificati "ad alto rischio", quali i dispositivi medici. Le misure di garanzia per la protezione dei dati personali si atteggiano quale strumento di flessibilità normativa legislativa e regolamentare, essendo orientate a consentire l'adattabilità all'evoluzione tecnologica, contribuendo alla ricerca di equilibrio tra tutela dei diritti e spazio comune europeo della circolazione dei dati.

The progressive increase in the role of algorithms in the society is of great interest in the healthcare sector. The essay presents an updated technical-legal analysis, in the light of recent regulatory, doctrinal and jurisprudential data, focusing on the evolutionary and critical aspects of the enhancement of health data in the European perspective, between computerization and redefinition of discretion, between primary use and secondary use of data, underlining the need for a transparent and accessible algorithm, as a particular condition for the correctness of administrative decisions taken in "high risk" AI qualification systems, such as medical devices. The safeguards for the protection of personal data act as an instrument of legislative and regulatory

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".
Il presente lavoro di ricerca ha origine e sviluppo nell'ambito del Progetto *iCare*, (CUP J39J14001400007 – Azione 10.5.12), in cui Giuseppina Lofaro è risultata vincitrice dell'assegno di ricerca in Diritto Amministrativo (Settore scientifico disciplinare IUS-10) presso il Dipartimento DIIES dell'Università degli Studi Mediterranea di Reggio Calabria, per l'espletamento del programma di ricerca dal titolo "Modelli procedimentali e semplificazione gestionale dei flussi informativi per la piattaforma di telemedicina *iCare*", finanziato nell'ambito del POR FESR FSE 2014/2020 della Regione Calabria con il concorso di risorse comunitarie del FESR ed FSE, dello Stato italiano e della Regione Calabria.

flexibility, being oriented at allowing adaptability to technological evolution, contributing to the search for a balance between protection of rights and European Health Data Space.

Sommario

1. Considerazioni preliminari sull'analisi dei dati nel settore sanitario. – 2. Misure di garanzia per il trattamento dei «dati relativi alla salute»: un'analisi in combinato disposto *ex* artt. 4 GDPR, 9 GDPR, 2-*septies* del Codice della privacy. – 2.1 L'impatto della legge di conversione del c.d. "Decreto Capienze" sulla protezione dei dati sanitari. – 3. Sicurezza nella formazione, circolazione, conservazione dei dati sanitari e rilievo del consenso quale eccezione al trattamento automatizzato *ex* art. 22 GDPR, tra decisione algoritmica e discrezionalità. – 4. Aspetti critici e profili evolutivi della valorizzazione dei dati sanitari nella prospettiva europea, tra informatizzazione e ridefinizione del potere discrezionale. – 4.1 La concentrazione dei dati quale strumento di avanzamento nella ricerca e di progresso nelle cure sanitarie: considerazioni conclusive.

Keywords

eHealth – dati sanitari – decisione amministrativa algoritmica – GDPR – discrezionalità amministrativa

1. Considerazioni preliminari sull'analisi dei dati nel settore sanitario

Lo sviluppo e la diffusione delle tecnologie dell'informazione e della comunicazione, (*ICT*, acronimo di *Information Communication Technology*)[1] ha ampliato enormemente la portata delle attività di produzione, raccolta, conservazione e condivisione di dati[2].
La proliferazione di dispositivi di registrazione digitale di dati in ambienti eterogenei consente di avere un'immagine digitale in *real time* di diversi sistemi sociali e tecnici, su scala globale, caratterizzata altresì da un'alta risoluzione dei comportamenti individuali. Tale innovativa capacità di misurazione delle persone porta con sé nuove sfide

[1] U. Pagallo, *Il diritto nell'età dell'informazione*, Torino, 2014, 174 ss.

[2] O. Pollicino - G. De Gregorio - M. Bassini, *Internet law and protection of fundamental rights*, Milano, 2022, presentano un'approfondita analisi sulla protezione dei diritti fondamentali nell'era digitale. Difatti, la massiccia diffusione delle tecnologie digitali ed algoritmiche solleva questioni intrinsecamente costituzionali. I diritti e le libertà sono esposti sia alle opportunità che alle sfide delle tecnologie digitali. Tale Opera offre una panoramica delle sfide più importanti poste dall'ascesa del cyberspazio dal punto di vista legale. Dopo alcuni capitoli preliminari sul panorama di internet, gli Autori si soffermano su come l'avvento delle tecnologie digitali abbia impattato su contenuti e dati, esplorandone gli effetti in termini di tutela della libertà di espressione, diritto alla privacy e protezione dei dati. In particolare, la terza parte (169-268) del libro analizza l'ambito della privacy e protezione dei dati guardando alle loro radici storiche, al ruolo del GDPR, incentrandosi specificamente anche sulla conservazione e sul trasferimento dei dati.

orientate a comprendere, permeare e controllare tali sistemi[3].

Nell'ambito delle scienze mediche, effetto diretto della variazione di scala della numerosità della popolazione contattabile e misurabile è stato uno straordinario sviluppo della ricerca clinica ed epidemiologica osservazionale, su dati *real word*, inclusiva della prevenzione primaria e secondaria nonché dell'assistenza sanitaria.

Questi studi osservazionali sui c.d. *big data*[4], mediante la disponibilità di innovative tecnologie computazionali, hanno consentito altresì di individuare la combinazione ottimale delle variabili disponibili, in un ambito controllato con finalità predittive rispetto ad un esito specifico. A tal proposito, si faccia riferimento agli studi finalizzati all'identificazione dei pazienti con una più alta probabilità di beneficiare di un trattamento sanitario.

La sfera biomedica è stata particolarmente incisa dalla rivoluzione digitale. Difatti, in tale ambito, il tasso di crescita dei dati elettronici è superiore rispetto alla media. Ciò avviene per effetto: della digitalizzazione della diagnostica per immagini nonché di cartelle cliniche e fascicoli sanitari, resi elettronici; della diffusione dell'*Internet of Things* ("*IoT*"), nonché dello sviluppo di tecniche di sequenziamento di *Next Generation Sequencing* ("*NGS*")[5].

Tale enorme quantità di dati, derivanti da fonti eterogenee che raccolgono ed aggiornano i dati per ragioni perlopiù differenti da quelle connesse alla ricerca clinica ed epidemiologica, se non analizzata ed integrata opportunamente, rischia di causare disfunzioni.

La disponibilità di tali dati costituisce un'opportunità rilevante al fine di addestrare algoritmi[6] di apprendimento automatico, elemento basilare nello sviluppo dell'intelli-

[3] O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Oxford, 2021, esplora l'impatto di internet sulla protezione dei diritti fondamentali, specialmente per quel che concerne la privacy, analizzando, inoltre, il rapporto tra nuove tecnologie e tutela dei diritti fondamentali all'interno del dibattito teorico sul processo di integrazione europea, con particolare attenzione al dialogo giudiziario. Tale innovativa monografia offre un'analisi approfondita delle forme, dei modelli e degli stili di tutela giurisdizionale dei diritti fondamentali nell'era digitale, nel confronto tra la visione europea con quella degli Stati Uniti.

[4] A tal proposito, si v. l'accurata analisi di O. Pollicino, *Costituzionalismo, privacy e neurodiritti*, in questa *Rivista*, 2, 2021, 9 ss., che esamina da una prospettiva comparata nonché di diritto costituzionale, la complessa tematica della tutela dei c.d. neurodiritti, ossia di una nuova dimensione nell'alveo delle consolidate categorie a protezione del diritto alla privacy, già sottoposte a rilevanti sollecitazioni dall'avvento delle tecnologie digitali.

[5] Il ricorso a tali tecniche ha consentito di offrire una visione globale dei processi cellulari e molecolari che caratterizzano gli individui, offrendo un contributo alla rivoluzione dello studio dei sistemi biologici complessi che, attraverso modalità integrative e modelli computazionali avanzati è orientata a rispondere a quesiti biologici caratterizzati da molteplici risvolti, come la patogenesi, la storia naturale e l'evoluzione delle malattie. Cfr. Aa. Vv., *e-Health Data Sharing, Best practices e soluzioni per la condivisione del dato, l'anonimizzazione e la creazione di data lake con dati sanitari*, Data Valley White Paper, 2021.

[6] O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, cit., spec. 99-146, 196-211, analizza in chiave ricostruttiva originale gli strumenti anche giudiziari per interpretare e far rispettare i diritti fondamentali nella "società algoritmica": «*Procedural rights will play a pivotal role in ensuring that these new substantive rights are actually protected and rendered enforceable vis-à-vis emerging private actors. Within the context of research into big data and predictive privacy violations (including those caused by the use of predictive algorithms), Crawford and Schultz have stressed the need to frame a form of "procedural data due process"*».

genza artificiale[7], da impiegare per la prevenzione delle malattie, per la diagnostica e lo sviluppo di nuovi farmaci[8]. Difatti, l'analisi di questi flussi di dati mediante il c.d. *data streaming*, ossia attraverso le tecniche di intelligenza artificiale e, nello specifico, con il *machine learning*[9], consente di individuare automaticamente delle correlazioni a partire da cui sarà possibile esprimere delle "predizioni" con ragionamenti di tipo induttivo e formulare così delle ipotesi. Perciò sarà possibile effettuare una sempre più precisa profilazione[10] del paziente ed adeguare la scelta del trattamento terapeutico in base al profilo genetico dell'individuo.

La *medicina di precisione* è «un approccio emergente di trattamento e prevenzione delle malattie che tiene conto della variabilità individuale di geni, ambiente e stili di vita»[11]. L'affermazione di tale approccio dipenderà dell'integrazione di enormi quantità di dati scaturenti dal ricorso a metodi ad alta processività per la caratterizzazione molecolare dei pazienti, assieme ad un altrettanto rilevante mole di dati fisiologici, clinici ed ambientali ricavati da tecnologie multicanali, ossia mediante gli s*martphon*e ed i sensori indossabili, – oltre che dalle informazioni ottenute tramite la frequentazione dei *social media* – e dalla loro analisi attraverso strumenti di apprendimento automatico.

Tale processo, sotto certi aspetti ancora in fase embrionale, potrebbe sostanziarsi in una rivoluzione epocale della pratica clinica e dell'assistenza sanitaria. In tutto ciò, la ricerca *data-intensive computing,* ossia l'elaborazione ad alta intensità di grandi volumi di dati di imponenti dimensioni, rappresenta il profilo cruciale che solleva una serie di criticità e questioni inedite. Sussistono difatti problematiche di ordine epistemologico, connesse alla reale affidabilità delle evidenze originate dall'analisi di dati eterogenei[12], nonché questioni di ordine tecnico, legate allo sviluppo di sistemi in grado

[7] A. Pajno - F. Donati - A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. II, *Amministrazione, responsabilità, giurisdizione*, Bologna, 2022.

[8] P. Guarda, *Ok Google, am I sick?: Artificial Intelligence, e-health and data protection regulation*, in *BioLaw Journal - Rivista di BioDiritto*, 1, 2019, 359.

[9] Il ricorso al *machine learning* per l'integrazione dei *big data* prodotti dalle tecniche di sequenziamento di seconda generazione impiegati nella biologia molecolare consente di oggettivare e quantificare la natura eterogenea di un numero significativo di malattie. Sotto un profilo terminologico collegato, si v. la recente giurisprudenza del Consiglio di Stato che con la sentenza della sez. III, 25 novembre 2021, n. 7891 ha affrontato la questione inerente al collegamento della nozione di "algoritmo" con quella di "automazione". Nello specifico, la gara riguardava l'acquisto di *Pacemaker* ed i Giudici di Palazzo Spada hanno affermato che: «Cosa diversa è l'intelligenza artificiale. In questo caso l'algoritmo contempla meccanismi di *machine learning* e crea un sistema che non si limita solo ad applicare le regole *software* e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico». Su tale pronuncia si v. *infra* la nota 32. Cfr. P. Bonini, Algoritmi, Intelligenza artificiale e machine learning nei processi decisionali pubblici, in *irpa.eu,* 22 aprile 2021; N. Cappellazzo, *Algoritmi, automazione e macchinismi di intelligenza artificiale: la classificazione proposta dal Consiglio di Stato*, in *Federalismi.it*, *Focus* Lavoro Persona Tecnologia – *Paper*, 2022, 1 ss.

[10] Criticamente, M. Interlandi, *Ma siamo davvero sicuri che l'intelligenza artificiale sia più efficiente di quell'umana? Spunti di riflessione sulla decisione amministrativa algoritmica rispetto alle garanzie personali e ai rischi di possibili discriminazioni (cd. Bias) e di minacce per la democrazia*, in *irpa.eu,* 20 novembre 2021. Più di recente, in chiave propositiva, cfr. M.G. Peluso, *Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato*, in questa *Rivista,* 2, 2022, 322 ss.

[11] *National Institute of Health*, *The promise of precision medicine*.

[12] V. Zeno-Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in questa *Rivista,*

di processare ed analizzare in maniera sicura un'enorme quantità di dati. Le criticità più intense e più diffuse sono di ordine etico e giuridico, sia per quel che concerne le ricerche osservazionali retrospettive su dati dal mondo reale, sia per quel che riguarda indagini nell'ambito della medicina di precisione. Queste ultime si fondano sull'utilizzo sistematico, sovente da parte di diversi centri di ricerca, di dati personali di natura sensibile ed ultra-sensibile (dati genetici) per un utilizzo c.d. secondario, ossia per finalità ulteriori rispetto a quelle per cui furono inizialmente raccolti. Difatti, alla luce della diffusione di sistemi di registrazione digitale, di dispositivi mobili, nonché dispositivi elettronici indossabili (c.d. *wearable device*) in ambito sanitario, considerato pure il valore intrinseco di ricerca dei dati sanitari e genetici, l'affermarsi della ricerca *data-driven*[13] implica l'impossibilità di prevedere, al momento della raccolta, tutti i futuri usi che potenzialmente potrebbero farsi dei dati. Tutto ciò mette in crisi il ricorso al consenso come base giuridica per il trattamento di tali dati. Difatti, il consenso, ai fini della sua validità, deve essere informato e specifico, ossia riferito ad uno o più fini determinati. Si provoca perciò uno squilibrio, considerato che tali dati verosimilmente necessiteranno di essere riutilizzati, condivisi ed aggregati ad altri per fini di ricerca. In questi casi, ricontattare ogni singolo paziente per informarlo sul nuovo fine di ricerca risulta eccessivamente costoso, praticamente complesso sotto un profilo organizzativo e, per di più, potrebbe mettere a rischio il conseguimento delle finalità della ricerca. Queste ultime sono finanche sconosciute al momento del trattamento nelle ricerche osservazionali fondate sull'uso di apprendimento automatico, neanche astrattamente prevedibili prima dell'analisi dei dati. Tali ricerche sono, infatti, finalizzate ad identificare l'ipotesi di studio e risultano scarsamente compatibili con l'approccio basato sul ri-consenso. Un'alternativa a quest'ultimo è la c.d. anonimizzazione, che tuttavia è difficile da perseguire nell'ambito dei *big data*[14].

2. Misure di garanzia per il trattamento dei «dati relativi alla salute»: un'analisi in combinato disposto *ex* artt. 4 GDPR, 9 GDPR, 2-*septies* del Codice della privacy

Il rispetto dei principi sanciti dal Regolamento in materia di sicurezza dei dati personali Regolamento (UE) 2016/679, c.d. GDPR (*General Data Protection Regulation*) deve essere garantito dalla struttura sanitaria, al fine di conseguire altresì la sicurezza delle cure. Difatti, la c.d. Legge Gelli-Bianco (l. 8 marzo 2017, n. 24), recante in Italia "Disposizioni in materia di sicurezza delle cure e della persona assistita, nonché in materia di responsabilità professionale degli esercenti le professioni sanitarie"[15], riconosce che

2, 2018, 37.

[13] B.D. Mittelsadt - L. Floridi, *The ethics of big data: Current and foreseeable issues in biomedical context*, in *Science and Engineering Ethics*, XXII, 2, 2016, 303 ss.

[14] A. Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI, in Information Technology and Law Series*, 2022.

[15] D. Amram - G. Comandé, *Sul non facile coordinamento degli obblighi imposti dal Regolamento europeo sulla*

la sicurezza delle cure, parte costitutiva del diritto alla salute *ex* art. 1, c. 1, si realizza anche mediante l'insieme di tutte le attività finalizzate alla «prevenzione e alla gestione del rischio connesso all'erogazione di prestazioni sanitarie e l'utilizzo appropriato delle risorse strutturali, tecnologiche ed organizzative» ai sensi dell'art. 1, c. 2.

Pare opportuno evidenziare che, pur non sussistendo una sezione dedicata *expressis verbis* al trattamento dei dati personali in ambito sanitario, il legislatore europeo del 2016, differentemente dalla Direttiva comunitaria del 1995, ha rivolto specifico riguardo ai «dati relativi alla salute», definendoli all'art. 4 GDPR come i «dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute» (definizione n. 15).

Il rilievo conferito dal Regolamento comunitario *de quo* a tali dati si evince anche dal successivo art. 9 GDPR[16], che li fa rientrare tra quelle «categorie particolari di dati personali» il cui trattamento è vietato, secondo limitazioni che gli Stati membri possono addirittura implementare (par. 4).

E' utile altresì sottolineare che il d.lgs. 10 agosto 2018, n. 101[17], emanato ai fini dell'adeguamento della normativa italiana alle disposizioni del GDPR, ha innestato nel d.lgs. 30 giugno 2003, n. 196, recante il Codice della privacy, l'art. 2-*septies*, rubricato «Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute», per cui i dati relativi alla salute possono essere oggetto di trattamento in conformità alle misure di garanzia disposte dal Garante per la protezione dei dati personali, da adottarsi, ai sensi dei c. 1 e 2, tenendo conto sia delle indicazioni enucleate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali, sia dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure di garanzia[18].

Nello specifico, esse devono concernere le cautele da adottare in relazione agli aspetti organizzativi e gestionali in ambito sanitario ed alle modalità ai fini della comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla sua salute *ex* c. 4. Esse, ai sensi del successivo c. 5, devono altresì individuare le misure di sicurezza, anche sotto un profilo tecnico, le misure di minimizzazione e le specifiche modalità per l'accesso selettivo ai dati.

Le misure di garanzia del Garante per la protezione dei dati personali si atteggiano

protezione dei dati personali UE/679/2016 e dalla legge n. 24/2017, in *Rivista italiana di medicina legale*, 2018, 1 ss.

[16] Si v. per le opportune precisazioni terminologiche il provvedimento n. 55 del 7 marzo 2019, recante *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, forniti dal *Garante per la protezione dei dati personali*, reperibile in *garanteprivacy.it*.

[17] Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

[18] Analiticamente il "D.L. capienze", d.l. 8 ottobre 2021, n. 139, che riforma il Codice della privacy su diversi aspetti ivi di interesse, su cui anche *infra* al par. 2.1 del presente contributo di ricerca. Si v. altresì F. Pizzetti (a cura di), *Protezione dei dati personali in Italia tra* GDPR *e Codice novellato*, Torino, 2021, 114 ss., cui si rinvia *funditus* per un'attenta riflessione sui contenuti dell'art. 2-*septies* e sulle problematiche dallo stesso scaturenti.

quale strumento di flessibilità normativa legislativa e regolamentare, essendo orientate a consentirne l'adattabilità all'evoluzione tecnologica, altresì dando un contributo alla ricerca di equilibrio tra tutela dei diritti e spazio comune europeo della circolazione dei dati.

L'analisi in combinato disposto delle norme pocanzi enucleate offre ulteriore evidenza del nesso funzionale tra sicurezza della formazione e sicurezza della conservazione e circolazione del dato sanitario[19].

L'art. 9, par. 2, GDPR esplicita un elenco di casi in cui il divieto di trattamento dei dati relativi alla salute non si applica, tra cui, ai sensi della lett. a), rientra quello in cui l'interessato abbia prestato «il proprio consenso esplicito al trattamento».

Certamente, in generale, è fondamentale che il consenso *tout court* sia il più possibile consapevole.

In ambito sanitario, la legge italiana 22 dicembre 2017, n. 219, ai sensi dell'art. 1, c. 2, promuove e valorizza «la relazione di cura e di fiducia tra paziente e medico» che si fonda sul consenso informato, in cui si incontrano «l'autonomia decisionale del paziente e la competenza, l'autonomia professionale e la responsabilità del medico», in una relazione di cura e di fiducia tra i due soggetti.

Pare opportuno riflettere perciò in merito a quale influenza generi su questa relazione l'impiego delle *smart technologies* e, altresì, su come si atteggi il rinnovato ruolo della struttura sanitaria nell'implementare tale consapevolezza anche sotto un profilo tecnico[20].

2.1 L'impatto della legge di conversione del c.d. "Decreto Capienze" sulla protezione dei dati sanitari

La legge 3 dicembre 2021, n. 205 di conversione del d.l. 8 ottobre 2021, n. 139, c.d. "Decreto Capienze", introduce alcune novità nel trattamento dei dati sanitari, in merito all'interconnessione dei sistemi informativi su base individuale – incluso il Fascicolo sanitario elettronico (FSE) –, con la *ratio* di implementare le reti di prossimità, la telemedicina, l'innovazione, la ricerca e la digitalizzazione del servizio sanitario nazionale (SSN)[21].

In particolare, la legge di conversione del "Decreto Capienze" interviene in materia di protezione dei dati personali anche per il settore sanitario.

Ante Decreto Capienze, i dati particolari – ossia i dati che rivelino l'origine razziale

[19] A tal proposito, acuta dottrina si domanda se esista in Italia una cultura del digitale così solida da sostenere il Garante nell'assolvimento dei compiti che la legge gli ha assegnato. Si v. sul punto P. Lombardi, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, in *Il diritto dell'economia*, 3, 2021, 64.

[20] C. Di Costanzo, *Consenso informato e impiego delle tecnologie. Implicazioni per il diritto pubblico e (auspicabile) ibridazione delle pratiche di cura*, in questa *Rivista*, 2, 2022, 180 ss.

[21] Legge 3 dicembre 2021, n. 205, pubblicata nella Gazzetta Ufficiale n. 291 del 7 dicembre 2021. Si v. per i lavori preparatori e per ricostruirne l'*iter*: Atto Camera n. 3374, Disegno di legge: S. 2409. - "Conversione in legge, con modificazioni, del decreto-legge 8 ottobre 2021, n. 139, recante disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali", approvato dal Senato, in *camera.it*.

o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale – potevano essere trattati per motivi di interesse pubblico rilevante, soltanto nei casi previsti da una norma di legge o, nei casi previsti dalla legge, da un regolamento.

La legge di conversione del "Decreto Capienze" prevede invece che il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico possa trovare fondamento giuridico, oltre che nella legge, anche in un atto amministrativo generale[22], per effetto della modifica intervenuta nell'art. 2-*ter* del Codice della privacy. Tale estensione si applica anche per il trattamento dei dati particolari (sanità pubblica, medicina del lavoro, archiviazione nel pubblico interesse o per ricerca scientifica o storica o a fini statistici) disciplinato dall'art. 2-*sexies* del Codice della privacy, rubricato "Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante". Il novellato art. 2-*sexies* prevede che i trattamenti di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, del GDPR, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi del soggetto interessato[23]. Gli atti amministrativi generali dovranno perciò specificare i tipi di dati che possono essere trattati, le operazioni eseguibili ed il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi.

Inoltre, la legge di conversione del "Decreto Capienze" prevede che la diffusione e la comunicazione di dati personali – trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri – a soggetti che intendono trattarli per altre finalità siano ammesse unicamente se previste ai sensi del c. 1 – sempre in presenza di base giuridica prevista dall'art. 6, par. 3, lett. b), del regolamento (GDPR), costituita da una norma di legge o di regolamento o da atti amministrativi generali – o se necessario ai sensi del c. 1-*bis* dell'art. 2-*ter* del Codice della privacy. In tal caso, deve esserne data notizia al Garante per la protezione dei dati personali almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

La legge di conversione non modifica il divieto di diffusione dei dati relativi alla salute,

[22] L'atto amministrativo generale, come enucleato dalla sentenza dell'Adunanza Plenaria del Consiglio di Stato, 4 maggio 2012, n. 9 ha destinatari indeterminabili a priori, ma certamente determinabili a posteriori in quanto è destinato a regolare non una serie indeterminata di casi, ma, conformemente alla sua natura amministrativa, un caso particolare, una vicenda determinata, esaurita la quale vengono meno anche i suoi effetti.

Secondo la dottrina la linea di *discrimen* tra il regolamento e l'atto amministrativo generale, è costituita dai criteri della generalità, astrattezza ed innovatività, propri del regolamento ed assenti nell'atto amministrativo generale che risponde alla necessità di concreta soddisfazione di specifiche esigenze pubbliche (ad es. bandi di concorso, gare). O. Sepe, *Atto normativo ed atto amministrativo generale*, in *Studi in onore di Ferdinando Carbone*, Milano, 1971, 261 ss.; P. Virga, *Diritto amministrativo*, Vol. 2, Atti e ricorsi, Milano, 2001; F. Satta, *Atto amministrativo*, in *Treccani - Diritto on line,* 2018.

[23] Art. 9, c. 5, d.l. 8 ottobre 2021, n. 139, convertito con modificazioni dalla l. 3 dicembre 2021, n. 205.

genetici e biometrici previsto dall'art. 2-*septies*, c. 8 del Codice della privacy che le amministrazioni pubbliche devono pertanto continuare a rispettare.

Nelle audizioni parlamentari[24], la previsione della possibilità del ricorso da parte degli enti pubblici ad un atto amministrativo generale come fondamento giuridico è stata motivata con la necessità di limitare la discrezionalità[25] degli enti nel definire i trattamenti di dati.

La previsione degli atti amministrativi generali come base giuridica può tuttavia comportare differenti regole sui trattamenti dei dati nei vari enti pubblici, con il rischio di una compressione del diritto alla protezione dei dati personali dei cittadini. Perciò, può ritenersi che le previsioni della legge di conversione del decreto Capienze ingenerino la necessità di acquisizione di ulteriore consapevolezza del valore dei dati da parte degli enti pubblici.

La legge di conversione del "Decreto Capienze" ha inoltre introdotto, all'interno dell'art. 2-*sexies* del Codice della privacy, il c. 1-*bis*[26], una norma specifica sui dati personali relativi alla salute, in considerazione della loro particolare rilevanza. La norma innestata è orientata a favorire l'interscambio di dati per fini sanitari in relazione alla

[24] Cfr. l'Audizione del Prof. M. Bassini al Senato della Repubblica – DDL 2409 ("Decreto Capienze"), alla Commissione Affari Costituzionali del Senato della Repubblica, in merito al contenuto del c.d. "Decreto capienze" (minuto 42:06 – 47:32). Nell'intervento sono state evidenziate le criticità sulle norme in materia di trattamento di dati personali che recano «un grave depotenziamento delle tutele degli individui» di fonte alla Pubblica Amministrazione. Nello specifico: - la dubbia sussistenza dei presupposti di straordinaria necessità e urgenza rispetto alle norme che modificano le condizioni di utilizzo della base giuridica dell'adempimento di un compito di interesse pubblico o dell'esercizio di pubblici poteri e di quelle che riducono – laddove non escludono – i poteri di intervento del Garante rispetto a tali trattamenti; - l'assenza di formali effrazioni rispetto al GDPR ma la sostanziale "torsione" del principio di legalità che si provoca affidando, con tale riforma, alla Pubblica Amministrazione il compito di definire le condizioni di accesso alla base giuridica in questione (con perplessità sulla tenuta della separazione tra poteri), «il tutto aggravato dalla preoccupante disinvoltura dimostrata da varie PA nel trattamento e soprattutto nella comunicazione di dati personali, come testimonia l'ampia casistica del Garante»; - il rischio che l'Autorità si ritrovi a conoscere moltissimi reclami, «nell'impossibilità di condurre una valutazione *ex ante* (facoltà di cui è espressamente privata *ope legis*, ora) e l'opportunità che se ne rivitalizzi in ogni caso il ruolo in questo frangente, anche con adeguate dotazioni di risorse, data la delicatezza del compito».

[25] M.S. Giannini, *Il potere discrezionale della pubblica amministrazione*, Milano, 1939; E. Casetta, *Attività e atto amministrativo*, in *Rivista trimestrale di diritto pubblico*, 1957, 300 ss.; C. Mortati, voce *Discrezionalità*, in *Novissimo Digesto Italiano*, Vol. V, 1960, 1098; F. Satta, *Principio di legalità e pubblica amministrazione nello stato democratico*, Padova, 1969; L. Benvenuti, *La discrezionalità amministrativa*, Padova, 1986; A. Angiuli, Studi *sulla discrezionalità amministrativa nel quando*, Bari, 1988; G. Azzariti, *Dalla discrezionalità al potere. La prima scienza del diritto amministrativo in Italia e le qualificazioni teoriche del potere discrezionale*, Padova, 1989.

[26] Cfr. c. 1-*bis* (dell'art. 2-*sexies*, Codice della privacy) introdotto dall'art. 9, c. 1, lett. b), del d.l. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla l. 3 dicembre 2021, n. 205: «I dati personali relativi alla salute, privi di elementi identificativi diretti, sono trattati, nel rispetto delle finalità istituzionali di ciascuno, dal Ministero della salute, dall'Istituto superiore di sanità, dall'Agenzia nazionale per i servizi sanitari regionali, dall'Agenzia italiana del farmaco, dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà e, relativamente ai propri assistiti, dalle regioni anche mediante l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, ivi incluso il Fascicolo sanitario elettronico (FSE), aventi finalità compatibili con quelle sottese al trattamento, con le modalità e per le finalità fissate con decreto del Ministro della salute, ai sensi del comma 1, previo parere del Garante, nel rispetto di quanto previsto dal Regolamento, dal presente codice, dal codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e dalle linee guida dell'Agenzia per l'Italia digitale in materia di interoperabilità».

missione del Piano di ripresa e resilienza nazionale (PNRR) che prevede il potenziamento della telemedicina per l'assistenza sanitaria territoriale. Difatti, la gestione dei dati è indispensabile ai fini della pianificazione a lungo termine delle attività da svolgere per la prevenzione ed il contrasto delle malattie croniche. Tuttavia, la norma introdotta non chiarisce nettamente cosa debba intendersi per "dati privi di elementi identificativi diretti"[27]. Si pone perciò il dubbio se fra questi rientrino esclusivamente dati anonimi o anche dati pseudonimizzati che possono essere ricondotti indirettamente a soggetti individuati.

Sempre nel nuovo c. 1-*bis* in analisi, la legge di conversione richiama poi l'attenzione delle Amministrazioni sul rispetto sia del Codice dell'Amministrazione Digitale (C.A.D.) sia delle Linee guida dell'Agenzia per l'Italia digitale (AgID) in materia di interoperabilità[28].

La legge di conversione del "Decreto Capienze" modifica altresì l'art. 7 del d. l. 19 maggio 2020, n. 34 avente ad oggetto "Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da *COVID-19*", intervenendo sul trattamento di dati personali da parte del Ministero della salute. Il precedente sopra citato d.l. n. 34 del 2020 prevedeva che il Ministero della salute fosse autorizzato *ex* art. 2-*sexies* a trattare i dati personali – anche relativi alla salute degli assistiti –, raccolti nei sistemi informativi del Servizio sanitario nazionale al fine di sviluppare metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione e demandava ad un decreto di natura regolamentare del Ministro della salute – adottato previo parere del Garante per la protezione dei dati personali – la definizione delle norme attuative. Invece, la legge di conversione del "Decreto Capienze" estende la possibilità di trattamenti da parte del Ministero della Salute anche a dati personali non sanitari.

Si prevede, inoltre, l'emanazione di un decreto di natura non regolamentare, da parte del Ministero della Salute, previo parere del Garante per la protezione dei dati personali, che individui i dati personali, anche inerenti alle categorie particolari di dati di cui all'art. 9 del regolamento (UE) 2016/679, che possono essere trattati, le operazioni eseguibili, le modalità di acquisizione dei dati dai sistemi informativi mediante i soggetti che li detengono e le misure appropriate e specifiche per tutelare i diritti degli interessati, nonché i tempi di conservazione dei dati trattati.

La legge di conversione del "Decreto Capienze", nel prevedere che il Ministero della salute sia autorizzato a trattare anche i dati personali non relativi alla salute, funzionalizza ciò ai fini dell'attuazione del corrispondente intervento di cui alla missione M6 del Piano nazionale di ripresa e resilienza, suddiviso in due componenti:

---

[27] Cfr. Camera dei Deputati, Ufficio Documentazione e Studi, *Dossier* n. 123, 1 dicembre 2021, in *camera.it*.

[28] Occorre sottolineare sul punto che il Decreto "Semplificazioni" (d.l. 31 maggio 2021 n. 77) ha novellato il Codice dell'Amministrazione Digitale (C.A.D.), prevedendo specifiche sanzioni per le Pubbliche Amministrazioni che rallentano la transizione digitale e specifici poteri di vigilanza di AgID in materia. L'art. 18-*bis* del C.A.D. prevede che «le violazioni accertate dall'AgID rilevano ai fini della misurazione e della valutazione della *performance* individuale dei dirigenti responsabili e comportano responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165».

- le reti di prossimità, strutture intermedie e telemedicina per l'assistenza sanitaria territoriale;
- l'innovazione, ricerca e digitalizzazione del servizio sanitario nazionale.

A tal proposito, la legge di conversione stabilisce che sia autorizzata l'interconnessione dei sistemi informativi su base individuale del Servizio sanitario nazionale, ivi incluso il Fascicolo sanitario elettronico (FSE), con i sistemi informativi gestiti da altre Amministrazioni Pubbliche che raccolgono i dati non relativi alla salute, con modalità tali da garantire che l'interessato non sia direttamente identificabile. La legge di conversione specifica poi che i trattamenti e le interconnessioni sono effettuate con le modalità e nei limiti stabiliti dal decreto e fatto salvo quanto previsto dall'art. 105 del codice di cui al d. l. 196/2003 avente ad oggetto le modalità del trattamento per fini di ricerca e statistica.

L'art. 105 del Codice della privacy prevede che i dati personali trattati a fini statistici o di ricerca scientifica non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per fini di altra natura. I fini statistici e di ricerca scientifica devono essere chiaramente determinati e resi noti all'interessato, nei modi di cui agli articoli 13 e 14 del Regolamento (GDPR) anche in relazione a quanto previsto dall'art. 106, c. 2, lett. b), del Codice della privacy e dall'art. 6-*bis* del decreto legislativo 6 settembre 1989, n. 322.

Per il trattamento effettuato a fini statistici o di ricerca scientifica rispetto a dati raccolti per altri fini, le informazioni all'interessato non sono dovute quando ciò richieda uno sforzo sproporzionato[29] rispetto al diritto tutelato, sempre che siano adottate le idonee forme di pubblicità individuate dalle regole deontologiche di cui all'art. 106 del Codice della privacy.

La legge di conversione del "Decreto capienze" contiene altresì una disposizione transitoria per cui nelle more dell'adozione del sopra citato decreto, il Ministero della salute ha avviato le attività relative alla classificazione delle patologie croniche presenti nella popolazione italiana, limitatamente alla costruzione di modelli analitici prodromici alla realizzazione del modello predittivo del fabbisogno di salute della popolazione, garantendo che gli interessati non siano direttamente identificabili.

In considerazione di quanto sin qui enucleato, sia pur in presenza delle criticità e dei rischi riscontrati, può ritenersi che la legge di conversione del "Decreto Capienze" abbia introdotto diverse disposizioni dal forte impatto sul settore sanitario nell'ottica di favorire l'interscambio e l'interconnessione dei dati, al fine di migliorare la gestione di dati aggregati per la pianificazione a lungo termine delle attività da svolgere per le malattie croniche, in relazione alla missione 6 del PNRR che prevede il potenziamento della telemedicina per l'assistenza sanitaria territoriale.

[29] M. Alovisio, *L'impatto della legge di conversione del d.l. 8 ottobre 2021 n. 139 "Decreto Capienze" sulla protezione dei dati in ambito sanitario*, in dirittoegiustizia.it, 2022.

3. Sicurezza nella formazione, circolazione, conservazione dei dati sanitari e rilievo del consenso quale eccezione al trattamento automatizzato *ex* art. 22 GDPR, tra decisione algoritmica e discrezionalità

La rilevanza del consenso in ambito sanitario risulta strettamente connessa alle questioni derivanti dalle norme di cui all'art. 22 GDPR per cui l'interessato ha il diritto di non essere sottoposto ad una decisione fondata unicamente sul trattamento automatizzato, compresa la profilazione, da cui scaturiscano effetti giuridici che lo riguardano o che incida analogamente in modo significativo sulla sua persona (par. 1)[30].
Come già rilevato, costituisce un'eccezione alla regola appena esplicitata, tra l'altro, la circostanza che la decisione «si basi sul consenso esplicito dell'interessato» (par. 2, lett. a), nel qual caso «il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione» (par. 3).
Pare utile evidenziare che, nell'ambito della questione incentrata sulla sicurezza del trattamento automatizzato dei dati personali, grande attenzione è attribuita alla decisione produttiva di effetti giuridici che su quel trattamento si fondi. Tale rilievo pone la disciplina in esame in un'ottica di protezione ancor più avanzata[31].
Queste disposizioni normative risultano connesse ad un'ampia questione, attualmente oggetto di analisi da parte della dottrina amministrativistica[32], concernente i limiti in cui è possibile demandare ad un algoritmo[33] l'assunzione di decisioni, di natura amministrativa o processual-amministrativa, lungo un itinerario tracciato da alcune recenti

[30] E. Pellecchia, *Privacy, decisioni automatizzate e algoritmi*, in E. Tosi (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, 429 ss. A tal proposito, il Comitato europeo per la protezione dei dati ha precisato che il diritto in analisi corrisponde ad un divieto generale operante *ex ante*, non rappresentando un mero diritto di opposizione *ex post* il cui esercizio sia affidato all'iniziativa dell'interessato.

[31] G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Napoli, 2019, 93 ss.; A. Masucci, *L'algoritmizzazione delle decisioni amministrative tra Regolamento europeo e leggi degli Stati membri*, in *Diritto pubblico*, 2020, 953 ss.

[32] V. per tutti A. Police, *Scelta discrezionale e decisione algoritmica*, 493 ss., in R. Giordano - A. Panzarola - A. Police - S. Preziosi - M. Proto (a cura di), *Il diritto nell'era digitale - Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022, in premessa, XXIV: «Non minori sfide il tema pone sul versante del diritto pubblico, e in particolare del diritto amministrativo, per le applicazioni che le pubbliche Amministrazioni sono incoraggiate a fare del mezzo informatico, della digitalizzazione degli atti e dei provvedimenti, dell'applicazione della IA ai processi decisionali pubblici. Il diritto amministrativo è quindi sollecitato ad occuparsi del tema con riguardo ad entrambe le polarità che alimentano il così detto "rapporto amministrativo": da un lato il versante degli interessi pubblici e delle Amministrazioni pubbliche cui la legge attribuisce il potere (ed il dovere) di assicurarne la cura; dall'altro, le situazioni giuridiche soggettive dei privati che con il pubblico potere dialogano e nei cui confronti invocano tutela nella ipotesi di patologico esercizio di tale potere. L'uso delle macchine e dei processi di IA incide quindi significativamente sul modo di svolgimento dei procedimenti amministrativi, sulle scelte discrezionali e vincolate delle pubbliche Amministrazioni, sul modo di produzione e comunicazione dei provvedimenti amministrativi».

[33] A. Celotto, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giuridica dell'economia*, 2019, 47 ss.

pronunce del giudice amministrativo[34].

In virtù del principio "*digital first*", la pubblica amministrazione considera la tecnologia e la digitalizzazione quali fattori chiave di trasformazione dei propri modelli decisionali e gestionali. Da ciò deriva l'uso incrementale degli algoritmi come strumento per automatizzare i procedimenti amministrativi. Tuttavia, la diffusione di decisioni amministrative algoritmiche non è stata accompagnata da un intervento legislativo orientato a proteggere i cittadini dai possibili rischi derivanti dall'uso dell'intelligenza artificiale[35]. Tale *vulnus* ha portato la giurisprudenza amministrativa ad elaborare alcuni principi di garanzia per un corretto utilizzo degli algoritmi da parte della pubblica amministrazione.

Fra le diverse pronunce, la sentenza del Consiglio di Stato n. 2270 del 2019 affronta il tema delle decisioni interamente automatizzate per mezzo di un algoritmo, di cui però non è possibile conoscere la formula e i criteri posti alla base della decisione. Nello specifico, il c.d. *e-governament*, ossia l'introduzione di modelli decisionali e di forme gestionali innovative, che si avvalgano delle tecnologie informatiche ed elettroniche, implementa la qualità dei servizi offerti ai cittadini, specialmente nel caso di utilizzo di algoritmi di automazione[36] di un processo decisionale amministrativo contraddistinto da un elevato tasso di standardizzazione. Per cui, l'utilizzo di una procedura informatica che conduca direttamente alla decisione finale comporta vantaggi quali, ad esempio, la notevole riduzione della tempistica procedimentale per operazioni meramente ripetitive e prive di discrezionalità, l'esclusione di interferenze dovute a negligenza (o in alcuni casi anche dolo) del funzionario - essere umano e la conseguente maggior

---

[34] Tar Campania, sez. III, 14 novembre 2022, n. 7003; Cons. Stato, sez. III, 25 novembre, 2021, n. 7891; Cons. Stato, sez. VI, 4 febbraio 2020, n. 881; Cons. Stato, sez. VI, 8 aprile 2019, n. 2270 e Tar Lazio, sez. III-*bis*, 27 maggio 2019, n. 6606, in giustizia-amministrativa.it. La giurisprudenza del Consiglio di Stato, inizialmente, ha sottolineato l'imprescindibilità della ricerca della regola tecnica che governa ogni algoritmo, con una motivazione incentrata sul diritto dell'Unione europea e sull'art. 22 GDPR. E. Carloni, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2020, 294 ss., acutamente, evidenzia che l'orientamento del Consiglio di Stato pare esplicitare una maggiore apertura rispetto alla disciplina contenuta nell'art. 22 GDPR, facendo riferimento «all'ammissibilità di un intervento umano anche solo in termini di validazione e controllo del risultato prodotto in autonomia dalla macchina». R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in *Diritto amministrativo*, 2019, 781 ss., rileva che la regola tecnica è una regola giuridica «elaborata dal pensiero dell'uomo che ne è e ne resta, sempre e comunque, il *dominus*, laddove alla "macchina" ne viene rimessa la semplice applicazione sul terreno, quando pure ciò avvenga in via "esclusiva"».

La discrezionalità amministrativa non può essere demandata al *software*, manifestando la propria persistente attualità e rilevanza nel momento alto e definitorio in cui la regola tecnica viene concretamente elaborata ed applicata. In quanto la tecnica appartiene, nella sua origine e nel suo sviluppo, al mondo umano e "la decisione affidata al *robot*" è comunque una decisione dell'uomo, «alla cui capacità d'*intelligere* inevitabilmente lascia l'innovazione e la creatività».

Cfr. altresì la sentenza del Consiglio di Stato, sez. VI, 13 dicembre 2019, n. 8472 nonché le chiare note di A. Bilancio, *La carente disciplina sull'uso degli algoritmi nella PA: come interviene il giudice amministrativo?* , in *medialaws.eu,* 7 ottobre 2021.

[35] G. Finocchiaro - O. Pollicino - L. Floridi, *Sull'intelligenza artificiale Ue indecisa tra armonizzazione e margini di libertà eccessivi*, in *Il Sole 24 Ore,* 2 marzo 2022.

[36] A. Masucci, *L'automatizzazione delle decisioni amministrative algoritmiche fra big data e machine learning. Verso l'algocratic governance?*, in *Dir. e proc. amm.*, 2, 2022, 265 ss. In chiave comparata, cfr. M. Finck, *Automated Decision-Making and Administrative Law*, in P. Cane - H.C.H. Hofmann - E.C. Ip - P.L. Lindseth (eds.), *The Oxford Handbook of Comparative Administrative Law*, *Oxford University Press*, Oxford, 2021, 657 ss.

garanzia di imparzialità della decisione automatizzata. Tuttavia, quest'ultima può essere ammessa solo nel caso di un procedimento amministrativo standardizzato; essa è da escludersi qualora vi siano margini di discrezionalità amministrativa: la valutazione degli interessi in gioco non può essere affidata ad un algoritmo. Ci si chiede allora come debba esser valutato il caso in cui l'attività nasca come discrezionale, ma, una volta esercitato il potere, l'amministrazione esaurisca il proprio margine di valutazione, circostanza che, in concreto, rende la decisione vincolata.

L'uso delle procedure automatizzate non può causare l'elusione dei principi che orientano l'attività amministrativa, in quanto la regola algoritmica alla base della procedura rimane pur sempre una regola ammnistrativa generale, definita dall'uomo. La regola algoritmica, acquisendo un valore giuridico pieno, deve rispettare i principi generali dell'attività amministrativa di pubblicità, trasparenza, ragionevolezza e proporzionalità. Per di più, la regola *de qua* deve prevedere una soluzione definita per tutti i casi possibili, senza alcun margine di discrezionalità, che invece spetta all'amministrazione nel momento dell'elaborazione dello strumento digitale. Specificamente, spetta all'amministrazione compiere la mediazione degli interessi coinvolti, anche per mediante *test* ed aggiornamenti continui dell'algoritmo. Mentre, il giudice è deputato a valutare in un secondo momento la correttezza del processo automatizzato in tutti i suoi elementi.

In virtù di quanto sin qui espresso, il Consiglio di Stato individua una serie di garanzie per tutelare il cittadino dinnanzi alla decisione automatizzata, identificando una forma di controllo *ex ante*, in sede di progettazione del *software*, momento in cui l'amministrazione è chiamata a svolgere *test* ed aggiornamenti continui. La fase inziale di individuazione dei dati e di definizione della regola algoritmica acquisisce rilievo fondamentale per garantire i diritti dei cittadini poiché la decisione automatizzata deriva dall'*output* finale dell'algoritmo, perciò da come è stato costruito, sulla base di quali dati, da come è stato addestrato. Proprio in tale momento deve essere tutelata la sfera di interessi e di diritti del cittadino.

Il Consiglio di Stato pare quindi anticipare al legislatore una possibile soluzione per regolare i rischi legati alle decisioni automatizzate, attraverso controlli procedimentali a valle della decisione automatizzata.

L'algoritmo può perciò essere ritenuto a tutti gli effetti quale "atto amministrativo informatico": deve essere conoscibile alla luce del principio di trasparenza: gli aspetti della formula tecnica devono essere tradotti nella regola giuridica ad essa sottesa, in modo da renderla comprensibile sia ai cittadini che al giudice. La conoscibilità consente di verificare che la procedura automatizzata sia conforme a quanto stabilito dalla legge o dalla stessa amministrazione, verificando per tale via le modalità e le regole poste alla base della decisione.

Il principio di conoscibilità è il presupposto fondamentale per poter indagare le motivazioni della decisione, garanzia fondamentale per il cittadino destinatario del provvedimento. La conoscibilità dell'algoritmo, peraltro, implica un ulteriore principio, ossia l'attribuzione della responsabilità della decisione non al *software*, bensì all'amministrazione che ha stabilito la regola posta alla base della decisione, che poi è stata automatizzata dall'algoritmo. Difatti, l'amministrazione non può abdicare al proprio ruolo affidando per intero la decisione ad un algoritmo, causando un'irreparabile violazione

del principio democratico.

Tuttavia, i principi di conoscibilità e di attribuibilità della decisione all'amministrazione potrebbero vacillare nel caso di uso delle tecnologie di *machine learning* e *deep learning*. Questi algoritmi sono in grado di definire in autonomia la regola alla base del risultato finale, così da diventar inesplicabile ed imprevedibile; inoltre paiono escludere la responsabilità dell'amministrazione per la decisione finale[37].

La regola algoritmica deve altresì poter essere sottoposta alla piena cognizione ed al sindacato del giudice, in modo da consentirgli di verificare con quali modalità sostanziali è stata assunta una decisione che si riverbera nella sfera giuridica del singolo. In tal modo il giudice può valutare la correttezza del processo informatico in tutte le sue componenti, dalla sua costruzione, all'inserimento dei dati, alla loro validità, alla loro gestione; nonché, vagliare la logicità e la ragionevolezza della decisione amministrativa robotizzata, ossia della "regola" che governa l'algoritmo[38]. La piena sindacabilità della decisione algoritmica[39] in tutti i suoi elementi involge un approccio necessariamente multidisciplinare – giuridico, informatico, ingegneristico – che richiede uno sforzo a tutto tondo per il giudice. Sorge così l'esigenza di definire le modalità per garantire un sindacato effettivo, che potranno essere gradatamente individuate nei diversi casi concreti successivi alla pronuncia *de qua* che segna l'apertura della giurisprudenza amministrativa nei confronti delle decisioni algoritmiche ed indica alcuni fondamentali princi-

[37] In una pronuncia successiva, Cons. Stato, sez. III, 25 novembre 2021, n. 7891 (di riforma della sentenza di primo grado, Tar Lombardia, sez. II, 31 marzo 2021, n. 843) i Giudici di Palazzo Spada, in un giudizio avente ad oggetto l'attribuzione dei punteggi alle offerte tecniche presentate dai concorrenti, nell'ambito di una procedura nazionale di gara per la fornitura di *pacemaker* di alta fascia ha formulato una nozione di algoritmo applicabile a sistemi tecnologici o a strumenti di alta fascia, offrendo un'interpretazione evolutiva della nozione di algoritmo, distinguendo gli algoritmi comuni da quelli tecnologicamente avanzati e dall'intelligenza artificiale.

Mentre i primi rappresenterebbero una mera sequenza finita di istruzioni, ben definite e non ambigue, tali da poter essere eseguite meccanicamente e produrre un determinato risultato, gli algoritmi tecnologici sarebbero caratterizzati da un efficiente grado di automazione, rappresentando sistemi di azione e controllo idonei a ridurre l'intervento umano nel processo.

L'intelligenza artificiale si configurerebbe quando l'algoritmo contempla meccanismi di *machine learning*, in un sistema che non si limita ad applicare le regole ed i parametri preimpostati, ma, altresì, elabora costantemente nuovi criteri di inferenza tra dati ed assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico.

Lo sforzo interpretativo del Consiglio di Stato appare certamente apprezzabile in considerazione dell'esigenza specifica di valorizzare le forniture di dispositivi con elevato grado di automazione anche in ragione della sensibilità del settore di richiesta della fornitura nonché della peculiarità del prodotto, trattandosi di *pacemaker* dotati di una funzione continuativa di "*sensing*" del ritmo cardiaco e di regolazione del medesimo.

Tuttavia, non pare attribuibile alla statuizione una portata definitoria generalizzata che travalica la specifica fattispecie esaminata in quanto la definizione di "algoritmo tecnologico" (o di "*alta fascia*") potrebbe risultare fuorviante, rispetto al concetto di processo decisionale automatizzato che presuppone la soluzione del problema in assenza dell'intervento umano, mediante un sistema in grado di accertare autonomamente la sussistenza delle condizioni per l'avvio delle operazioni e di risolvere il problema. Su tali aspetti, si v. *funditus* P. Clarizia, La nozione di algoritmo "tecnologico" secondo una recente decisione del Consiglio di Stato, in *irpa.eu,* 13 gennaio 2022.

[38] B. Spampinato, *Per un primo inquadramento teorico della decisione amministrativa algoritmica*, in *Rivista Giuridica AmbienteDiritto.it*, 3, 2021, 1 ss.

[39] S. Vernile, Verso la decisione amministrativa algoritmica*,* in questa *Rivista,* 2, 2020, 136 ss.; *,* in questa *Rivista,* 1, 2020, 18 ss.

pi per tutelare le garanzie dei cittadini, poi approfonditi in una sentenza successiva[40], la sentenza n. 881 del 4 febbraio 2020, in cui il Consiglio di Stato ha aperto alla possibilità di decisioni automatizzate anche nell'alveo della discrezionalità amministrativa[41], affermando che «Non vi sono ragioni di principio, ovvero concrete, per limitare l'utilizzo all'attività amministrativa vincolata piuttosto che discrezionale, entrambe espressione di attività autoritativa svolta nel perseguimento del pubblico interesse», puntualizzando che «se il ricorso agli strumenti informatici può apparire di più semplice utilizzo in relazione alla c.d. attività vincolata, nulla vieta che i medesimi fini predetti, perseguiti con il ricorso all'algoritmo informatico, possano perseguirsi anche in relazione ad attività connotata da ambiti di discrezionalità»[42]. Partendo dall'apertura che la giurisprudenza amministrativa offre, è possibile ipotizzare alcuni casi in cui l'utilizzo di algoritmi potrebbe venire impiegato in decisioni che sono il frutto dell'attività discrezionale della Pubblica Amministrazione. Come rilevato da una parte della dottrina[43], algoritmi decisionali potrebbero essere utilizzati quando l'Amministrazione predetermina i contenuti della decisione che scaturirà dalla macchina, limitando in tal modo le alternative possibili cui l'algoritmo può giungere. In questo modo il ricorso a decisioni algoritmiche potrebbe essere esteso a quei casi – caratterizzati dalla c.d. "bassa discrezionalità" – in cui l'esercizio discrezionale dell'attività amministrativa viene esercitato in un momento antecedente rispetto al momento decisionale vero e proprio[44]. Del resto, emerge *ictu oculi* che la predeterminazione dei criteri e delle soluzioni possibili ricompone l'attività discrezionale in una pressoché totale vincolatività, potendo la macchina unicamente scegliere tra alternative già previamente determinate.

L'analisi risulta più complessa quando invece residuino margini di discrezionalità in capo all'Amministrazione[45]. L'economia del presente contributo di ricerca non consente di addentrarsi ulteriormente nella trattazione *de qua*. Di certo, le prospettive di utilizzo delle tecnologie "intelligenti" nell'esercizio di attività connotate da ampi margini di discrezionalità impongono l'individuazione di principi applicativi che garantiscano, al contempo, il godimento delle moderne potenzialità informatiche e l'osservanza dei canoni generali di esercizio della funzione pubblica.

Tornando alla pronuncia in commento, i giudici riconoscono i vantaggi che la "rivoluzione digitale" può apportare alle Amministrazioni pubbliche in quanto una maggiore

[40] Consiglio di Stato, sez. VI, 4 febbraio 2020, n. 881, annotata, tra gli altri, da A. Valsecchi, Algoritmo, discrezionalità amministrativa e discrezionalità del giudice *(nota a Cons. Stato, sez. VI, 4 febbraio 2020, n. 881)*, in *iusinitinere.it,* 14 settembre 2020.

[41] G. Cavalcanti, Algoritmi e decisione amministrativa: la metamorfosi del procedimento nell'era della digitalizzazione 4.0, in *irpa.eu,* 2 novembre 2021.

[42] § 8 della sentenza in analisi.

[43] M.L. Maddalena, *La digitalizzazione della vita dell'amministrazione e del processo*, in *Foro Amministrativo*, 10, 2016, 2535 ss.

[44] M. Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi?*, in *Istituzioni del federalismo*, 2019, 3, 647.

[45] Parte della dottrina esclude l'automazione di decisioni amministrative discrezionali, come rileva P. Otranto, *Decisione amministrativa e digitalizzazione della p.a*, in *federalismi.it*, 17 gennaio 2018, 21, secondo cui tale esclusione deriverebbe dal fatto che «l'atto discrezionale, essendo fondato sulla ragionevolezza umana, sarebbe informato ad una logica "opaca" non riconducibile a percorsi predeterminati e predeterminabili».

digitalizzazione delle procedure pubbliche risponde a canoni di efficienza ed economicità dell'azione amministrativa, in applicazione del principio costituzionale del buon andamento dell'amministrazione *ex* art. 97, c. 2, Cost. ed è fondamentale per migliorare la qualità dei servizi per utenti e cittadini, specialmente con riferimento a «procedure … seriali o standardizzate, implicanti l'elaborazione di ingenti quantità di istanze e caratterizzate dall'acquisizione di dati certi ed oggettivamente comprovabili e dall'assenza di ogni apprezzamento discrezionale»[46]. I Giudici di Palazzo Spada, anche sulla base della normativa sovranazionale, elaborano allora un quadro di principi rilevanti nell'utilizzo di algoritmi e sistemi automatizzati:

il principio di conoscibilità, già accennato in altra precedente pronuncia, attiene al diritto di ciascuno sia di conoscere l'esistenza di processi automatizzati nei suoi confronti, sia di ottenere le informazioni sulla logica utilizzata nel procedimento amministrativo;

il principio di non esclusività della decisione algoritmica[47], *ex* art. 22 del regolamento (UE) 679/2016 (GDPR), per cui, come già riportato in apertura del presente paragrafo, «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»;

il principio di non discriminazione algoritmica è strettamente connesso al trattamento dei dati e richiede che il titolare del trattamento stesso utilizzi procedure statistiche appropriate e che metta in atto misure per correggere eventuali inesattezze ed errori, al fine di impedire «effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello *status* genetico, dello stato di salute o dell'orientamento sessuale»[48].

Certamente, rimangono ancora alcune questioni aperte poiché le decisioni amministrative algoritmiche costituiscono un fenomeno complesso ed eterogeneo, non suscettibile di essere regolamentato in modo definitivo e sistematico dalle pronunce giurisprudenziali. Pertanto, risulta indispensabile l'intervento del legislatore che sancisca un quadro normativo organico, fondato su principi che garantiscano un utilizzo degli algoritmi contraddistinto da etica ed affidabilità[49].

Tuttavia, il d.lgs. 7 marzo 2005, n. 82, recante il Codice dell'Amministrazione Digitale (C.A.D.) italiano, nonostante le sue reiterate modifiche[50], non ha ancora innestato la

[46] § 6 della sentenza in analisi.

[47] Tar Campania, sez. III, 14 novembre 2022, n. 7003, massima a cura di C. Della Giustina, in *AmbienteDiritto.it*: «il ricorso all'algoritmo, in funzione integrativa e servente della decisione umana, ovvero anche in funzione parzialmente decisionale nei procedimenti a basso tasso di discrezionalità, non può mai comportare un abbassamento del livello delle tutele garantite dalla legge sul procedimento amministrativo, ed in particolare di quelle sulla individuazione del responsabile del procedimento, sull'obbligo di motivazione, sulle garanzie partecipative, e sulla cd. non esclusività della decisione algoritmica».

[48] Il Consiglio di Stato ricava tale principio dal considerando 71 del GDPR.

[49] P. Falletta, *Alla ricerca di un paradigma giuridico della decisione amministrativa algoritmica*,in *Amministrazione in cammino - Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione*, 31 marzo 2022, 1 ss.

[50] Cfr. la sua versione più recente aggiornata alle ultime modifiche del 29 giugno 2022, consultabile in *normattiva.it*.

disciplina rispetto all'opportuna regolamentazione di tale pratica sempre più diffusa.
Ad ogni modo, anche alla luce dell'*excursus* giurisprudenziale, può ritenersi che non sussista radicale incompatibilità fra informatizzazione e discrezionalità amministrativa[51], avanzando l'idea che le nuove tecnologie determinino (*melius*: sollecitino), sia pure seguendo criteri prudenziali, "la ridefinizione e riallocazione del potere discrezionale"[52].
Certamente, Il processo di informatizzazione non può tuttavia degenerare nella violazione dei principi generali del diritto amministrativo, che rappresentano gli ineludibili parametri di adeguamento dei tradizionali moduli di esercizio della funzione pubblica alle nuove forme di automazione provvedimentale. Pertanto risulta indispensabile avviare un percorso di trasformazione che, pur non potendo prescindere da un ripensamento dei classici schemi di organizzazione delle pubbliche amministrazioni, deve ad ogni modo garantire la scelta di programmi informatici adeguati al perseguimento dei fini di pubblico interesse.
Ci si domanda allora se vi sia una possibilità sostanziale di assicurare la trasparenza[53] del funzionamento dei sistemi di Intelligenza Artificiale (IA)[54], a titolo esemplificativo attraverso l'introduzione di consone procedure di certificazione e di controllo in merito alla loro affidabilità.
E' opportuno sottolineare che l'IA non è mai citata *expressis verbis* nel GDPR, nonostante molti dei dati processati attraverso i meccanismi decisionali concernenti l'IA siano qualificabili come personali e riconducibili alla disciplina comunitaria. A tal proposito, pare utile evidenziare che non tutti i dati processati dalla IA in un'attività amministrativa sono personali*;* ad ogni modo, anche qualora non fossero dati personali sono – se trattasi di dati pubblici – sottoposti ad un regime normativo eurounitario.
Nell'ambito della Strategia europea per l'Intelligenza Artificiale, la Commissione europea ha pubblicato, il 21 aprile 2021, la proposta di Regolamento sull'approccio europeo

[51] V. Neri, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urbanistica e Appalti*, 5, 2021, 581 ss.

[52] A. Cassatella, *La discrezionalità amministrativa nell'età digitale*, in Aa. Vv., *Scritti per Franco Gaetano Scoca*, vol. I, Napoli, 2020, 675 ss.; tradizionalmente A. Police, *La predeterminazione delle decisioni amministrative. Gradualità e trasparenza nell'esercizio del potere discrezionale*, Napoli, 1997, 247 ss., offre spunti ricostruttivi *evergreen*, estremamente utili anche nell'ambito degli attuali profili evolutivi della tematica, secondo cui la predeterminazione dell'azione pubblica accrescerebbe anche il grado di prevedibilità delle decisioni amministrative, facendo sorgere, di conseguenza, in capo agli amministrati un legittimo affidamento in ordine all'esito dell'azione stessa. A tal riguardo, l'A. esprime un giudizio contrario all'utilizzo dei termini "autolimite" o "autovincolo", in quanto locuzioni che sembrano attribuire all'istituto una connotazione negativa, cioè di limite alla discrezionalità, per cui non valorizzerebbero la funzione propulsiva della futura azione discrezionale esercitata dal fenomeno in questione.

[53] F. De Leonardis, *Big data, decisioni amministrative e "povertà" di risorse della pubblica Amministrazione*, in E. Calzolaio (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Milano, 2020, 152-156.

[54] G. Marchianò, *Intelligenza Artificiale: IA specifiche e l'amministrazione provvedimentale – IA generali e i servizi pubblici*, in federalismi.it.; sulle questioni problematiche derivanti dall'applicazione della logica degli algoritmi all'attività vincolata piuttosto che a quella discrezionale della pubblica amministrazione, si v. *funditus* R. Cavallo Perin (a cura di), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Torino, 2021, 16 ss.; evidenzia la necessità di un algoritmo trasparente ed accessibile, specialmente quale condizione di correttezza della decisone assunta G.M. Esposito, *Al confine tra algoritmo e discrezionalità. Il pilota automatico tra procedimento e processo*, in *Diritto e processo amministrativo*, 2019, 62 ss.; sulle posizioni di dottrina e giurisprudenza in merito al carattere (o meno) "discrezionale" dell'informatizzazione dell'attività amministrativa, si v. E. Picozza, *Intelligenza artificiale e diritto - politica, diritto amministrativo and artificial intelligence*, in *Giurisprudenza italiana*, 2019, 1657 ss.

all'Intelligenza Artificiale[55], quale primo quadro giuridico europeo sull'IA[56]. La proposta normativa *de qua* pone divieto assoluto rispetto ad una serie di possibili usi di alcuni sistemi di IA, quali quelli che, al fine di distorcere in maniera sostanziale il comportamento di una persona, usano tecniche subliminali o che sfruttano una vulnerabilità legata all'età o ad una disabilità[57] di uno specifico gruppo. Inoltre essa stabilisce una puntuale disciplina rispetto ai sistemi di IA qualificati "ad alto rischio", ossia le tecnologie che causano rischi elevati per la salute, la sicurezza o i diritti fondamentali delle persone, come i sistemi di IA destinati ad essere utilizzati quali componenti di sicurezza di prodotti soggetti a valutazione di conformità secondo una disciplina europea: a titolo esemplificativo, i dispositivi medici. Tra le specifiche regole introdotte si segnalano, in particolare, l'obbligo di creare e mantenere attivo un sistema di *risk management*, l'obbligo di assicurarsi che i sistemi di IA possano essere sottoposti a supervisione da parte di persone fisiche, l'obbligo di garantire l'attendibilità, accuratezza e sicurezza degli obblighi di trasparenza verso gli utenti sul funzionamento dei sistemi di IA.

Alla luce di quanto sin qui enucleato, può ritenersi che il progressivo incremento del ruolo degli algoritmi[58] nella nostra società risulti di grande interesse nell'ambito sani-

[55] Cfr. Artificial Intelligence act

[56] Commissione europea, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, Bruxelles, 26.1.2022 COM(2022) 28 final, 1-7, spec. 4. Il Parlamento europeo, il Consiglio e la Commissione proclamano solennemente la dichiarazione *de qua*: il contributo della proposta della Dichiarazione dei diritti e principi digitali per la decade digitale europea apporta spunti di riflessione rilevanti, anche per altri aspetti di questo contributo di ricerca, analizzati nel prosieguo. In particolare, il Cap. III "Libertà di scelta", *Interazioni con algoritmi e sistemi di intelligenza artificiale*, prevede che: «Ogni persona dovrebbe essere messa nelle condizioni di godere dei benefici offerti dall'intelligenza artificiale facendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali». Ci si impegna a: – «garantire la trasparenza in merito all'uso degli algoritmi e dell'intelligenza artificiale e a fare in modo che le persone, quando interagiscono con essi, siano autonome, responsabili e informate; – garantire che i sistemi algoritmici siano basati su insiemi di dati adeguati al fine di evitare discriminazioni illecite e consentano la supervisione umana dei risultati che riguardano le persone; – garantire che le tecnologie come gli algoritmi e l'intelligenza artificiale non siano utilizzate per predeterminare le scelte delle persone, ad esempio per quanto riguarda la salute, l'istruzione, l'occupazione e la vita privata; – prevedere garanzie affinché i sistemi digitali e di intelligenza artificiale siano sicuri e vengano utilizzati nel pieno rispetto dei diritti fondamentali delle persone». Cfr. le chiare ed ancora attuali riflessioni di M. Bassini, (con A. Pajno - G. De Gregorio - M. Macchia - F.P. Patti - O. Pollicino - S. Quattroccolo - D. Simeoli - P. Sirena), *AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2019, *passim.*

[57] B. Rabai, *The role of technology and innovation in digital and social inclusion. The case of disability in a public perspective*, in questa *Rivista*, 1, 2022, 199 ss.; V. Tondi Della Mura, *La disabilità fra «sanità» e «assistenza» (ovvero fra le omissioni della politica e le innovazioni dell'amministrazione-sussidiaria)*, in *Non Profit*, 2, 2011, 5 ss.; anche in *federalismi.it*, 14, 2011, 1 ss., effettua, a tal proposito, considerazioni sistematiche interessanti, certamente ancora attuali, su cui è opportuno riflettere, anche sotto un profilo ricostruttivo: «La tutela dei diritti, sia pure nominalmente accresciuti in consistenza e quantità, non si è dimostrata efficace ed effettiva. La necessità di un approccio integrale e integrato alle problematiche della disabilità si è infranta innanzi alla frantumazione costituzionale delle competenze coinvolte. Gli effetti della scissione fra «sanità» e «assistenza», l'una condivisa fra Stato e regioni (art. 117, comma 3, Cost.), l'altra riservata alle regioni e demandata agli enti locali (art. 117, comma 4, Cost.), solo apparentemente è stata risolta dall'intervento trasversale dello Stato in tema di livelli essenziali delle prestazioni (art. 117, comma 2, sub m, Cost.). Divaricatesi le competenze, si sono frastagliati altresì i centri d'indirizzo e di spesa, originandosi un sistema multilivello casuale, disorganico e fonte d'inevitabile incertezza giuridica, clientela politica e corruzione amministrativa».

[58] P. Moro, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in questa *Rivista*, 3, 2019, 21 ss.

tario[59].

Esso, difatti, è strettamente connesso alla questione del decremento del ruolo del soggetto umano nell'assunzione di decisioni aventi conseguenze sostanziali per la salute del paziente destinatario, *quaestio* che, nella prospettiva della sicurezza dei dati concerne sia la circolazione/conservazione del dato sanitario, sia specialmente la sua formazione, la cui decisione deve essere il più possibile sicura, avendo rilievo per la salute del paziente.

Nell'ambito dell'analisi incentrata sull'art. 22 GDPR, basilare è l'interpretazione dell'inciso «decisione basata unicamente sul trattamento automatizzato»[60], avendo l'avverbio funzione di *discrimen* rispetto alle decisioni ammissibili e a quelle non ammissibili.

La riflessione svolta alla luce della citata giurisprudenza amministrativa[61] induce a considerare il ruolo che la dimensione umana mantiene anche in epoca applicativa di *smart technologies*[62]. Difatti, parte della dottrina[63] afferma che, in ogni caso, nella fattispecie di cui all'art. 22 GDPR debba manifestarsi un intervento umano concretamente funzionale al riesame degli esiti del processo automatizzato[64].

Attenta dottrina[65] ha sostenuto pure che «il sistema automatico tende, nel tempo, a catturare la decisione stessa». Tale assunto determina due conseguenze rilevanti: primariamente, la dimostrazione che una decisione lesiva sia fondata unicamente su di un processo automatizzato assume, in concreto, le caratteristiche di una «*probatio diaboli-*

[59] L'IA applicata alla medicina soffre di un grave difetto di trasparenza, al punto che, sovente, «non è dato comprendere, nemmeno ai programmatori, il percorso attraverso cui la macchina produce il risultato della propria attività». Evidenzia chiaramente tali aspetti critici P. Lombardi, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, cit., 68. Cfr. altresì A. Di Martino, *The relationship between Law and Technique in the construction of Administration by algorithms*, in *European Review of Digital Administration & Law - Erdal*, 2(1), 2021, 199 ss.

[60] Nel senso che la norma in effetti non è diretta a vietare la decisione automatizzata *tout court*, si esprime G. Finocchiaro, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 244-245.

[61] Cfr. ancora A. Valsecchi, *Algoritmo, discrezionalità amministrativa e discrezionalità del giudice (nota a Cons. Stato, sez. VI, 4 febbraio 2020, n. 881),* cit.; G. Pesce, *Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale*, in *giustizia-amministrativa.it*, 2020; A. Sola, *La giurisprudenza e la sfida dell'utilizzo di algoritmi nel procedimento amministrativo*, novembre 2020, in *Giustamm.it*; V. Canalini, *L'algoritmo come "atto amministrativo informatico" e il sindacato del giudice*, in *Giornale di Diritto Amministrativo*, 6, 2019, 781 ss.

[62] M. Tresca, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale*, in questa *Rivista*, 3, 2018, 240 ss.

[63] C. Napoli, *Algoritmi, intelligenza artificiale e formazione della volontà pubblica: la decisione amministrativa e quella giudiziaria*, in *Rivista AIC*, 3, 2020.

[64] L'art. 22 GDPR potrebbe essere "riletto" nel senso di configurare un diritto ad essere destinatari di decisioni che siano il risultato di un processo in cui sia presente la componente umana. Sussisterà però una differenza sostanziale tra «l'imbattersi in un medico che è contrario a priori a confermare una decisione algoritmica piuttosto che avere a che fare con un medico predisposto a scegliere l'opzione più idonea a supportare le scelte della macchina per l'assenza della disponibilità di informazioni che siano anche solo lontanamente paragonabili all'enorme massa di dati che ha costituito il presupposto per la decisione della macchina». Si esprime in tal senso P. Lombardi, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, cit., 69.

[65] A. Simoncini, *Diritto costituzionale e decisioni algoritmiche,* in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, 55. Più di recente, Id., *Lo «Stato digitale». L'agire provvedimentale dell'amministrazione e le sfide dell'innovazione tecnologica*, in *Riv. trim. dir. pubbl.*, 2, 2021, 529 ss.

ca»[66]; per di più, l'eccesivo affidamento che il medico riponga sui risultati derivanti da macchine intelligenti potrebbe contribuire a causare il c.d. "*deskilling* professionale", ossia la progressiva riduzione delle competenze professionali del sanitario[67].
Perciò, in sintesi, se la presenza del consenso esplicito dell'interessato innesta un'eccezione alla regola enunciata dall'art. 22, par. 1, GDPR, dovendo tuttavia il titolare del trattamento attuare misure consone di tutela – il cui livello minimo è costituito dal diritto di ottenere comunque un intervento umano –, la *quaestio* principale[68] sarà quella di enucleare i caratteri di tale intervento sotto l'aspetto della formazione tecnica. Ciò acquisirà un rilievo evidente nella transizione da tecnologie di semplice comprensione – la cui applicazione involga un mero accertamento tecnico – a tecnologie intelligenti di ultima generazione, le cui logiche complesse necessitano di una valutazione tecnica *tout court*, tuttavia controvertibile in *rerum natura*.
Si ritiene ad ogni modo auspicabile che le potenzialità espresse dalle tecnologie intelligenti vengano pienamente incorporate nelle professioni sanitarie in quanto numerosi sarebbero i benefici sostanziali. I medici potrebbero svolgere effettivamente il ruolo che il GDPR, specialmente attraverso l'art. 22, conferisce loro. Inoltre, accogliendo un'ottica di apertura alla digitalizzazione, essi potrebbero orientare quest'ultima anche in funzione delle esigenze e caratteristiche dell'*ars medica*.

4. Aspetti critici e profili evolutivi della valorizzazione dei dati sanitari nella prospettiva europea, tra informatizzazione e ridefinizione del potere discrezionale

A livello comunitario[69], negli ultimi anni, costanti sono stati gli *input* europei alla digitalizzazione del settore sanitario ed alla condivisione dei dati sanitari. Tra i basilari aspetti di innovazione vi sono: la condivisione di *best practices*, l'interoperabilità dei sistemi di informazione, la sicurezza dei dati e le tecnologie per il potenziamento della privacy, l'implementazione dell'infrastruttura di servizi digitali per la sanità elettronica, i registri e le piattaforme delle malattie comuni, gli strumenti per la ricerca sulle malattie rare, la prevenzione ed il controllo delle minacce sanitarie transfrontaliere, lo scambio transfrontaliero di dati sanitari, un utilizzo ottimale dei finanziamenti europei[70].

[66] P. Lombardi, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, cit., 56.

[67] Il sanitario corre il rischio di perdere la dimestichezza acquisita rispetto alla valutazione analitica delle informazioni disponibili. Come estrema *ratio*, potrebbe non essere più in grado di rilevare neanche gli errori grossolani. Rileva il rischio di tale deriva ivi, 70.

[68] P. Guarda - L. Petrucci, *Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati*, in *Bio-Law Journal*, 2020, 425 ss.

[69] Cfr. *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final, 2015.

[70] Commissione europea, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, cit., 4, in particolare il Cap. II *Solidarietà e inclusione*, specificamente la parte dedicata ai "Servizi pubblici digitali online": «Ogni persona dovrebbe avere accesso a tutti i servizi pubblici principali *online* in tutta l'Unione. A nessuno deve essere chiesto di fornire dati più spesso di quanto necessario durante l'accesso ai servizi pubblici digitali e il loro utilizzo». Ci si impegna a: «– garantire che a tutti gli europei sia offerta un'identità

I sistemi sanitari ed assistenziali necessitano *funditus* di riforme ed opzioni innovative per risultare accessibili ed efficaci nel prestare assistenza ai cittadini europei[71]. La condivisione del dato è un elemento essenziale ai fini del perseguimento di tali fini. Tuttavia i dati sono sovente disponibili in formati che non ne assicurano l'interoperabilità ed inoltre sono spesso sottoposti ad una gestione differente tra gli Stati membri. Per di più, all'interno dei sistemi sanitari nazionali si riscontrano difformità gestionali da Regione in Regione.

La perdurante fase emergenziale legata alla diffusione del Covid-19 ha fatto emergere *ictu oculi* il potenziale inesplorato, dando così avvio all'impiego diffuso di soluzioni innovative in ambito medico, specialmente mediante il ricorso alla telemedicina[72] ed all'assistenza da remoto. Le tecnologie digitali possono consentire ai cittadini un più agevole monitoraggio del proprio stato di salute, la prevenzione rispetto all'insorgenza di nuove patologie e l'efficientamento del funzionamento dei sistemi sanitari.

Tuttavia, la crisi sanitaria ha anche messo in evidenza "le vulnerabilità dello spazio digitale", la sua dipendenza da *critical infrastructures*[73], sovente non ubicate nei territori europei; essa ha evidenziato altresì la dipendenza da poche *big tech company*. Tale periodo di crisi pandemica è stato oltretutto caratterizzato da un incremento dell'afflusso di prodotti contraffatti, di furti informatici, nonché da un'amplificazione dell'impatto della disinformazione sulle società democratiche.

A tal proposito, la Commissione europea stima che la realizzazione di un'ulteriore integrazione dei servizi pubblici *online*, il miglioramento delle infrastrutture per la trasmissione elettronica e l'accesso ai dati potrebbe portare benefici annuali cospicui, fino a 120 miliardi di euro all'anno.

Tra le priorità che l'Unione europea ha individuato nel *Digital Compass 2030* vi sono: la costruzione di un'infrastruttura interconnessa paneuropea comune e polivalente ai fini dell'elaborazione dei dati, da utilizzare nel pieno rispetto dei diritti fondamentali[74]; lo sviluppo di capacità periferiche in *real time* per soddisfare le esigenze degli utenti finali vicino ai luoghi di generazione dei dati; la progettazione di piattaforme *middleware* sicure, a basso consumo ed interoperabili per usi settoriali, al fine di consentire un facile scambio e condivisione dei dati.

Tale prospettiva è stata delineata nell'ambito del Programma *EU4Health*[75] per il perio-

digitale accessibile, sicura e affidabile, che dia accesso a un'ampia gamma di servizi *online*; – garantire l'accessibilità e il riutilizzo su vasta scala delle informazioni della pubblica amministrazione; – agevolare e sostenere in tutta l'Unione un accesso fluido, sicuro e interoperabile ai servizi sanitari e assistenziali digitali concepiti per soddisfare le esigenze dei cittadini, comprese le cartelle cliniche».

[71] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana, COM(2018) 233 final.

[72] G. Delle Cave, La sanità "digitalizzata" nell'economia delle Smart City, in *irpa.eu,* 23 novembre 2022.

[73] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *2030 Digital Compass: the European way for the Digital Decade,* COM(2021) 118 final.

[74] G. De Minico, *Fundamental rights, European digital regulation and algorithmic challenge*, in questa *Rivista*, 1, 2021, 9 ss.

[75] Regolamento (UE) 2021/522 del Parlamento europeo e del Consiglio del 24 marzo 2021 che istituisce

do 2021-2027, orientato alla trasformazione digitale dei servizi sanitari, alla promozione dell'interoperabilità, allo sviluppo di uno spazio europeo dei dati sanitari.
Può ritenersi che *EU4Health* rappresenti la risposta dell'Unione europea alla diffusione del Covid-19. Si tratta in effetti del più grande programma per la salute finora approvato in termini di risorse finanziarie, a fronte di un investimento di 9,4 miliardi di euro, destinato a fornire finanziamenti agli Stati Membri, alle organizzazioni sanitarie e alle ONG. Il programma *de quo* finanzierà anche le azioni connesse alla creazione del c.d. *European Health Data Space*[76]. Difatti, la creazione di uno spazio europeo dei dati costituisce una delle priorità della Commissione europea per il periodo 2019-2025, anche nel settore sanitario. Certamente, uno spazio comune europeo dei dati sanitari apporterà, anche in un'ottica promozionale, un miglioramento nello scambio e nell'accesso a differenti tipi di dati sanitari, – tra cui quelli tratti da cartelle cliniche elettroniche, i dati genomici, i dati estrapolati dai registri dei pazienti – non soltanto per sostenere il c.d. uso primario dei dati, ossia la fornitura di assistenza sanitaria, bensì altresì per il *c.d. uso secondario dei dati*, ossia per la ricerca sanitaria e la definizione delle politiche sanitarie.
Lo Spazio Europeo dei Dati Sanitari dovrà fondarsi sul rispetto dei principi di trasparenza[77] e protezione dei dati personali dei pazienti nonché sul rafforzamento della *data portability* ai sensi dell'art. 20 del GDPR[78].
Ai fini dello sviluppo dell'*European Health Data Space*, la Commissione europea si adopererà assieme agli Stati membri, incentrandosi specificamente su tre pilastri: 1) un forte sistema di *data governance* dei dati ed un *framework* di regole per lo scambio di dati; 2) la qualità dei dati; 3) la creazione di una struttura in grado di abilitare l'interoperabilità.
A tal proposito, il *EDPB-EDPS Joint Opinion* 03/2022 *on the Proposal for a Regulation on the European Health Data Space*[79] ha messo in discussione alcuni degli aspetti della proposta *de qua*, specificamente in relazione alle sue ambizioni ed ai suoi strumenti. I Garanti europei sottolineano la necessità che lo "Spazio europeo dei dati sanitari" rispetti le norme sulla privacy ed altresì che i dati siano conservati unicamente all'interno dello Spazio economico europeo. In particolare, Il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (EDPS) raccomandano pieno rispetto delle norme poste a protezione dei dati dei pazienti europei, nel parere congiunto sulla proposta della Commissione europea per lo Spazio europeo dei dati sanitari (*Ehds-European Health Data Space*).
Come già accennato, la proposta è orientata a semplificare la creazione di un'unione sanitaria europea ed a consentire all'Ue di sfruttare pienamente il potenziale offerto

un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 («programma UE per la salute») (*EU4Health*) e che abroga il regolamento (UE) n. 282/2014.

[76] La proposta di regolamento della Commissione europea per istituire lo spazio europeo dei dati sanitari, del 3 maggio 2022, è visionabile in *health.ec.europa.eu*.

[77] Si v. *funditus* A.G. Orofino, *The Implementation of the Transparency Principle in the Development of Electronic Administration, in European Review of Digital Administration & Law – Erdal*, 1(1-2), June-December 2020, 123 ss.

[78] Per il diritto alla portabilità dei dati cfr. *privacy-regulation.eu*.

[79] European Data Protection Supervisor – European Data Protection Board, *EDPB-EDPS* Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, adopted on 12 July 2022, 1-32, in *edpb.europa.eu*.

dallo scambio, dall'uso e dal riutilizzo sicuro e protetto dei dati sanitari elettronici, sia per fornire una migliore assistenza sanitaria, anche transfrontaliera, al soggetto i cui i dati sono stati raccolti nel c.d. "uso primario", sia a fini di ricerca scientifica, medicina personalizzata, statistica, applicazioni digitali per la salute nel c.d. "uso secondario".
Nell'accogliere con entusiasmo l'impegno a rafforzare i diritti delle persone rispetto ai propri dati elettronici sanitari, l'EDPB e l'EDPS esprimono, tuttavia, una serie di timori e criticità di ordine generale. Innanzitutto, con riferimento al disallineamento tra le previsioni della proposta sui diritti degli interessati e il GDPR. Inoltre, pur riconoscendo che le previsioni della proposta orientate a facilitare l'uso secondario di dati sanitari elettronici possano generare benefici per il bene pubblico, il Comitato ed il Garante europeo mettono in rilievo i rischi per i diritti e le libertà delle persone interessate, derivanti da queste ulteriori attività di trattamento, rispetto alle quali, diversamente dall'"uso primario", non è garantito all'interessato il diritto di limitare l'accesso di terzi ai propri dati.
Pertanto, il Comitato ed il Garante europeo ritengono che le finalità dell'uso secondario dei dati sanitari elettronici non siano adeguatamente definite dalla proposta e chiedono ai co-legislatori di delimitare ulteriormente tali finalità, circoscrivendole a quelle collegate al perseguimento di un bene pubblico nel settore sanitario e/o previdenziale.
In relazione ai dati sanitari generati dalle *app* per il benessere e da altre applicazioni digitali per la salute, EDPB e EDPS chiedono che tali informazioni personali non vengano messe a disposizione per l'"uso secondario", perché producono un'enorme quantità di dati, che non sono della stessa qualità di quelli generati dai dispositivi medici e che possono essere trattati insieme ad ulteriori informazioni diverse da quelle sanitarie. Difatti, nonostante l'obiettivo dell'infrastruttura per lo scambio di dati sanitari elettronici prevista nella proposta sia quello di facilitare lo scambio dei dati sanitari, tuttavia la grande quantità di dati che verrebbero trattati, la loro natura altamente sensibile, il rischio di accesso illegale e la necessità di garantire un controllo efficace da parte di autorità indipendenti per la protezione dei dati richiedono, secondo il parere espresso dall'EDPB e l'EDPS, che Parlamento europeo e Consiglio impongano l'obbligo di conservare i dati sanitari elettronici esclusivamente all'interno dello Spazio economico europeo, fatti salvi ulteriori trasferimenti in conformità con le garanzie approntate dal GDPR.
Per quel che concerne il modello di *governance* introdotto dalla proposta, l'EDPB e l'EDPS sottolineano che le Autorità per la protezione dei dati sono le uniche autorità competenti per le questioni relative al trattamento dei dati personali e dovrebbero rimanere l'unico punto di contatto per le persone in merito a tali questioni. Perciò, dovrebbe essere evitata ogni sovrapposizione tra tali Autorità e i nuovi enti introdotti dalla proposta e dovrebbero essere specificate le rispettive competenze nonché previsti chiari obblighi di cooperazione[80].
La Commissione europea aveva già preannunciato, nell'ambito dell'*European Data Stra-*

[80] V. Di Felice, Servizio Studi del Senato, *Note su atti dell'Unione europea*, Nota n. 102, *Lo Spazio Europeo dei Dati Sanitari*, luglio 2022.

tegy[81] e nel più recente *Data Governance Act*[82], l'*intentio* di perseguire risultati sostanziali nel settore dei dati sanitari e di ottimizzare il potenziale originato dagli sviluppi delle tecnologie digitali ai fini dell'introduzione dell'innovazione in ambito sanitario.
La raccolta, l'accesso, la conservazione, l'uso ed il ri-uso dei dati sanitari pongono questioni che devono essere affrontate in un quadro normativo bilanciato, di contemperamento dei contrapposti interessi, che tenga ad ogni modo in debita considerazione gli interessi ed i diritti dei cittadini, specificamente per quel che concerne il trattamento dei dati relativi allo stato di salute, nell'ottica di una ponderata ridefinizione e redistribuzione del potere discrezionale.
La Direttiva sull'assistenza sanitaria transfrontaliera[83] ha prodotto un *framework* di collaborazione tra le autorità nazionali responsabili per la sanità elettronica: la c.d. rete *eHealth*; tuttavia gli accordi stipulati e gli strumenti sussistenti rispondono alle sfide in corso in maniera meramente parziale. Diverse sono le criticità emergenti.
In particolare, l'insufficiente scambio di dati sanitari ha un impatto negativo sulla fornitura di servizi sanitari e, perciò, sull'uso primario del dato sanitario.
Ancora, il livello di digitalizzazione varia notevolmente all'interno di ogni Stato Membro e l'interoperabilità tra i fornitori di servizi sanitari rimane limitata.
La rete *eHealth* e la connessa infrastruttura IT hanno potenziato lo scambio transfrontaliero di dati sanitari per l'assistenza sanitaria, specialmente in relazione alle cartelle cliniche dei pazienti ed alle prescrizioni elettroniche. Tuttavia, la sua natura giuridica volontaria – e perciò non vincolante – ne ha limitato l'impatto nonché influenzato l'adozione in senso restrittivo.
L'attività di esercizio dell'accesso ed il controllo sui propri dati sanitari risulta sovente estremamente complessa per i pazienti. Le cartelle cliniche elettroniche (*EHR*) non sono ancora diffuse uniformemente in tutta l'Unione europea e molti pazienti non possono agevolmente accedervi per utilizzare le informazioni in esse contenute, o trasferirle tra diversi operatori, specialmente in caso di trasferimento transfrontaliero.
Tutto ciò causa inefficienze, sforzi ulteriori, ritardi nelle cure e, *last but not least*, costi più elevati per i pazienti e per i sistemi sanitari.
Essendo limitata la condivisione delle cartelle cliniche elettroniche, le informazioni in esse contenute non possono essere facilmente scambiate nel trattamento dei pazienti.
Per quel che concerne l'uso secondario del dato sanitario, l'accesso e la condivisione di dati sanitari per la ricerca scientifica e l'innovazione, per la definizione di nuove politiche e per le attività di regolamentazione, rimangono ancora molto limitati all'interno dell'Unione europea.
Le sfide poste nell'ambito della raccolta, dell'accesso, della conservazione, dell'uso e del riutilizzo dei dati sanitari nell'assistenza sanitaria sono essenzialmente di carattere legale, specialmente giuspubblicistico, nonché tecnologico. Difatti, sotto un profilo

[81] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i dati*, COM(2020) 66 *final.*

[82] Proposta di regolamento del Parlamento europeo e del consiglio relativo alla *governance* europea dei dati, COM(2020) 767 final.

[83] Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera.

normativo, il GDPR sancisce un *framework* comune di regole a cui gli Stati membri hanno aggiunto ulteriori specifiche e restrizioni concernenti il trattamento e la condivisione di dati sanitari. Pertanto, il trattamento dei dati sanitari personali negli Stati membri risulta frammentario, causando ostacoli nonché un accesso limitato dei ricercatori e delle istituzioni pubbliche, riducendo in tal modo la competitività dell'Unione europea nonché la prospettiva di innovazione a livello globale.

Tra l'altro, gli Stati membri hanno approcci differenti rispetto all'accesso ed alla condivisione dei dati sanitari. In particolare, alcuni di essi hanno istituito organismi nazionali che semplificano l'accesso ai dati sanitari; tuttavia, tali organismi non esistono in tutti gli Stati membri. Emerge *ictu oculi* che una cooperazione, una *governance*[84] ed un'infrastruttura IT limitate e non interoperabili a livello comunitario, sostanzialmente ostacolano l'accesso ai dati sanitari da parte di ricercatori, organismi di regolamentazione ed istituzioni pubbliche.

Un numero crescente di strumenti digitali per la salute integra sistemi di intelligenza artificiale (AI). La Commissione europea sta perciò lavorando su un quadro orizzontale per l'IA che involge profili connessi alla sicurezza ed ai diritti fondamentali, che è destinato ad essere applicato in diversi settori, inclusi i prodotti sanitari[85].

Tuttavia, gli aspetti specifici relativi alla salute che si fondano sul quadro dell'IA, tra cui la formazione, i test e la convalida dei sistemi di IA, potrebbero necessitare di un'ulteriore analisi tecnico-giuridica interdisciplinare integrata.

L'utilizzo di strumenti di IA, nello specifico l'opacità di alcune applicazioni, può rendere difficile l'inquadramento dei profili di responsabilità o la garanzia di conformità. Perciò risulta fondamentale la previsione di adeguate garanzie sui diritti fondamentali ed in tema di risarcimento dei danni.

Tali questioni dovrebbero essere analizzate e risolte nell'ambito dell'*European Health Data Space*[86], il cui specifico programma è orientato a:

- assicurare l'accesso, la condivisione e l'uso ottimale dei dati sanitari ai fini della prestazione dell'assistenza sanitaria, nonché il loro riutilizzo per la ricerca e l'innovazione, l'elaborazione delle politiche e le attività di regolamentazione, in modo sicuro, tempestivo, trasparente ed affidabile nonché mediante un'opportuna *governance* istituzionale;
- promuovere un "mercato unico della salute digitale", che ricomprenda i servizi ed i prodotti sanitari, inclusa la telemedicina, il telemonitoraggio e la salute mobile (c.d. *mobile health*, *mHealth*);
- potenziare lo sviluppo, la diffusione e l'applicazione di prodotti e servizi sanitari digitali affidabili, inclusi quelli che incorporano l'intelligenza artificiale nel settore della salute;

[84] E. Sorrentino – A. F. Spagnuolo, *Dati sanitari: aperti, accessibili e riutilizzabili*, in questa *Rivista*, 1, 2022, 170 ss.

[85] C. Mannelli, *Etica e Intelligenza artificiale. Il caso sanitario*, Roma, 2022, coniugando attualità e analisi, offre degli spunti di riflessione per mettere a fuoco la realtà dell'IA, il suo straordinario potenziale, nonché i rischi e i limiti che la caratterizzano, al fine di incoraggiarne uno sviluppo inclusivo, sostenibile e responsabile.

[86] European Commission, *Proposal for a regulation of the European Parliament and of the Council on the European Health Data Space,* Strasbourg, 3.5.2022, COM (2022) 197 final 2022/0140 (COD).

- sancire un quadro giuridico e di *governance* appropriato per coprire l'accesso e lo scambio di dati sanitari per la fornitura di assistenza sanitaria, la ricerca, la definizione delle politiche e le attività di regolamentazione.

L'*European Health Data Space*, integrato in combinato disposto con profili del c.d. *Data Governance Act*, prevede la designazione di organismi nazionali per la salute digitale ed organismi settoriali competenti rispetto all'uso secondario dei dati sanitari. E' altresì previsto: il sostegno alle autorità pubbliche (a titolo esemplificativo, le agenzie di medicina, le istituzioni epidemiologiche, gli istituti sanitari nazionali) ai fini dell'accesso ai dati sanitari nel pieno ossequio delle disposizioni normative sulla protezione dei dati; l'accesso ai dati genetici ed il collegamento con i dati sanitari; il riutilizzo dei dati detenuti da soggetti privati; il sostegno alla formazione ed alla sperimentazione di applicazioni sanitarie di intelligenza artificiale.

Emerge a tal punto *ictu oculi* l'interazione di tali previsioni con il GDPR, specificamente per quel che concerne gli artt. 9 e 89 del GDPR, in relazione alla regolamentazione dei dati sanitari.

Risulta perciò opportuna l'eliminazione delle barriere tecniche che ostacolano l'utilizzo ed il ri-uso dei dati, in particolare quelle relative alle infrastrutture, all'interoperabilità, alla qualità dei dati ed agli *standard* nel settore sanitario. Appare altresì utile approfondire l'analisi tecnico-giuridica rispetto:

- alle opzioni relative alle infrastrutture per l'uso dei dati per l'assistenza sanitaria, con riferimento all'infrastruttura di servizi digitali per la sanità elettronica (*MyHealth@EU*) per lo scambio transfrontaliero dei dati dei pazienti quando viaggiano all'estero;
- alle opzioni riguardanti l'*enforcement* dell'interoperabilità[87] delle cartelle cliniche elettroniche, in linea con il formato europeo di scambio, nonché dell'interoperabilità semantica e tecnica dei diversi tipi di dati;
- alle opzioni concernenti i diversi modelli di infrastrutture interoperabili ai fini dell'accesso ai dati ed i connessi servizi per semplificare un sicuro stoccaggio transfrontaliero nonché per l'elaborazione e l'analisi dei dati sanitari a fini di ricerca, di elaborazione delle politiche e di regolamentazione, in un quadro rinnovato[88]

[87] F. Laus, *Preparedness e once only nella digitalizzazione della PA: focus sul settore sanitario*, in *European Review of Digital Administration & Law – Erdal*, 2(2), 2021, 163 ss.

[88] J. B. Auby, *Administrative Law Facing Digital Challenges*, in *European Review of Digital Administration & Law – Erdal*, 1(1-2), June - December 2020, 7 ss.

della discrezionalità amministrativa[89] *tout court*, essendosi riallocato, in via pretoria[90], nell'ambito delle nuove tecnologie, il potere sostanziale della Pubblica Amministrazione[91] di adottare una decisione effettuando, in base alla legge, una scelta fondata sulla ponderazione di un interesse pubblico primario con interessi secondari, pubblici, privati, o collettivi.

4.1 La concentrazione dei dati quale strumento di avanzamento nella ricerca e di progresso nelle cure sanitarie: considerazioni conclusive

La *chance* di aggregazione di informazioni in sistemi che ne consentano un accesso ed un riutilizzo semplificato e rapido, quali i c.d. *data lakes* o *data warehouse*, costituisce uno degli aspetti fondamentali per la ricerca e lo sviluppo di soluzioni fondate sull'analisi dei dati. Ciò emerge *ictu oculi* nel settore sanitario.

Il profilo *de quo* è stato ulteriormente rilevato nel corso della pandemia da Covid-19 che ha reso improcrastinabile l'implementazione di un'infrastruttura capace di facilitare la condivisione, l'accesso ed il ri-uso sicuro del dato sanitario.

L'aumento esponenziale dell'informazione disponibile segue un tasso di crescita molto elevato, mediante il cospicuo sviluppo e la consequenziale diffusione di dispositivi di acquisizione dati. Nonostante ciò, l'accesso ed il riutilizzo delle risorse informative risulta assai frenato.

I fattori che si frappongono ad una più ampia "democratizzazione" dell'informazione sanitaria, che risulti orientata ad incentivare la rapida concretizzazione di progetti di ricerca e sviluppo, sono di svariata natura: tra questi, la mancanza di una piattaforma *standard* per la condivisione sicura del dato sanitario nonché la natura sensibile del dato stesso[92].

---

[89] G. Gardini, *La discrezionalità amministrativa e tecnica*, in *Il diritto amministrativo nella giurisprudenza*, Rimini, 2022, 267 ss., si sofferma in maniera sistematica sugli istituti della discrezionalità amministrativa e tecnica, a partire da un commento delle sentenze del Consiglio di Stato, sez. III, 5 febbraio 2021, n. 1091 e sez. VI, 24 aprile 2019, n. 2625. Il dibattito dottrinale intorno al concetto di discrezionalità tecnica ha radici antiche e complesse, che in questa sede non può essere trattato in maniera compiuta. Non a caso la nozione di discrezionalità tecnica è tra le meno chiare nonché tra le più contestate sotto il profilo della sua autonomia, in quanto esistono solo accertamenti, apprezzamenti e giudizi tecnici che possono essere riferiti tanto ad atti discrezionali quanto ad atti vincolati. Per una completa analisi dell'evoluzione dottrinale si rinvia a F. Liguori, *Attività liberalizzate e compiti della amministrazione*, Napoli, 1999, 160 ss.; A Giusti, *Contributo allo studio di un concetto ancora indeterminato: la discrezionalità tecnica della pubblica amministrazione*, Napoli, 2007, 17 ss. Più di recente si v. A. Moliterni, *Le disavventure della discrezionalità tecnica tra dibattito dottrinario e concrete dinamiche dell'ordinamento*, in Id. (a cura di), *Le valutazioni tecnico-scientifiche tra amministrazione e giudice. Concrete dinamiche dell'ordinamento*, Napoli, 2021, 7 ss.

[90] Tar Campania, sez. III, 14 novembre 2022, n. 7003; Cons. Stato, sez. III, 25 novembre, 2021, n. 7891; Cons. Stato, sez. VI, 4 febbraio 2020, n. 881, in giustizia-amministrativa.it.

[91] F. F. Pagano, *Pubblica Amministrazione e innovazione tecnologica*, in *La Rivista "Gruppo di Pisa"*, 3, 2021, 84 ss.

[92] The *European Monitoring Tool* prevede che per il 2025 il mercato dei dati europei raggiungerà il valore di oltre 140 miliardi di Euro. Cfr. *First Report on Facts and Figures Updating the European Data Market Study Monitoring Tool By International Data Corporation (IDC) and the Lisbon Council,* European Data Market Study Updated SMART 2016/0063.

Risulta perciò chiara la necessità di un mutamento di paradigma tecnologico ai fini della valorizzazione dell'*asset* informativo. A tal proposito, diversi iniziative europee sono state avanzate al fine di rendere possibile l'accesso ed il riutilizzo del patrimonio informativo sanitario attraverso l'aggregazione in *data lake* o *data warehouses*[93].
La nascita di tali realtà in diversi Stati membri dimostra la rilevanza della tematica della condivisione del dato ed altresì quanto questa necessità sia avvertita in tutti gli Stati membri dell'Unione europea.
L'aggregazione di queste informazioni, attraverso piattaforme dedicate, svolge funzione incentivante rispetto alla ricerca, semplificando l'accesso al dato. Per di più, essa consente l'eliminazione di barriere geografiche, sostenendo l'originarsi di collaborazioni e sinergie internazionali orientate al progresso scientifico[94].
Certamente, al fine di conferire vigore e sostanza alle previsioni comunitarie del mercato dei dati, è indispensabile, in una prospettiva *de iure condendo*, un intervento organico del legislatore nazionale[95] fondato sui principi di legalità algoritmica[96], affinché le nuove tecnologie a disposizione dell'ambiente IT (I*nformation Technology*) e la ricerca di soluzioni innovative in tema di privacy dei dati si sviluppino[97] e vengano adottate con un metodo integrato[98], nonché alla luce del principio di contemperamento dei contrapposti interessi, ossia considerando che la "buona" Pubblica Amministrazione, nell'effettuare una scelta e quindi nell'applicare la propria riallocata discrezionalità nell'ambito delle *new technologies* nel c.d. *European Health Data Space*, dovrà sempre tenere in adeguata considerazione l'armonizzazione di tutti gli interessi coinvolti dall'azione amministrativa[99], ovvero interesse pubblico e interessi secondari pubblici o privati, ribadendo, in chiusura del presente lavoro, la necessità di un algoritmo trasparente ed accessibile[100],

---

93 A titolo esemplificativo, si fa riferimento all'*eHealth platform Belgium*, un servizio governativo belga, che offre la possibilità agli attori del panorama sanitario di scambiare in maniera sicura informazioni anche sensibili.
Si cita altresì *The Health Data Research Hubs* inglese che semplifica l'accesso ai dati del sistema sanitario nazionale per il settore pubblico, accademico e della ricerca industriale nel Regno Unito. Cfr. Aa. Vv., *e-Health Data Sharing*, *Best practices e soluzioni per la condivisione del dato*, *l'anonimizzazione e la creazione di data lake con dati sanitari*, cit., 30-31.

94 E. Carloni, *Le nuove tecnologie al servizio delle pubbliche amministrazioni*, in A.I.P.D.A., *Annuario 2019. Quali saperi servono alla pubblica amministrazione? Selezione, valorizzazione e tutela della professionalità pubblica. Atti del Convegno annuale,* Pisa, 10-12 ottobre 2019, Napoli, 2020, 31-32.

95 A. Pajno - F. Donati - A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Vol. I, *Diritti fondamentali, dati personali e regolazione*, Bologna, 2022.

96 F. Nassuato, Legalità algoritmica nell'azione amministrativa e regime dei vizi procedimentali, in *ceridap.eu,* 24 novembre 2022.

97 M.G. Losano, *La lunga marcia dell'informatica nelle istituzioni italiane*, in R. Cavallo Perin - D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, XXIV.

98 *European Commission Directorate General for Communications Networks, Content and Technology Directorate G — Data Unit G.1 — Data Policy & Innovation*, *Study to support an Impact Assessment on enhancing the use of data in Europe*, Brussels, febbraio 2022, 1-428: in linea con la comunicazione della Commissione europea sulla strategia europea per i dati del 2020 (COM(2020) 66 *final*), lo studio valuta i settori chiave che rientrano nelle questioni e nel potenziale ambito di azione dei *Data Governance Acts* e del *Data Act*.

99 A. M. Chiariello, *AI and Public Services: a Challenging Relationship Between Benefits, Risks and Compliance with Unavoidable Principles*, in *European Review of Digital Administration & Law – Erdal*, 2(2), 2021, 185 ss.

100 B. Marchetti, *The algorithmic administrative decision and The Human in the loop*, in *BioLaw Journal - Rivista di BioDiritto*, 2, 2021, 1 ss., esamina l'uso dell'intelligenza artificiale da parte delle Pubbliche Amministrazioni

specialmente quale condizione di correttezza della decisone amministrativa assunta.

in un contesto normativo caratterizzato dall'assenza di una regolamentazione generale ed incentrato sull'intervento *ex post* da parte della giurisprudenza in veste sostitutiva. Partendo da un caso basato su un algoritmo, l'attenta dottrina analizza l'efficacia del Regolamento Europeo sulla Protezione dei Dati e il ruolo effettivo del principio "*human in the loop*", considerando le diverse tipologie di algoritmo applicabili, la normativa *background* e le competenze dei pubblici ufficiali che operano con l'intelligenza artificiale.

European Media Freedom Act: la tutela europea della libertà dei media*

Giuseppe Muto

Abstract

La digitalizzazione ha rivoluzionato la stampa e il modo di informarsi dei cittadini, ciò impone una necessaria riflessione sulle nuove prospettive delle libertà e dei diritti connessi all'infosfera. Muovendo dalle fonti di rango costituzionale e dal differente approccio regolatorio adottato dagli USA e dall'Europa, il saggio si propone il fine di approfondire la Proposta di Regolamento del Parlamento e del Consiglio dell'UE (cd. *European Media Freedom Act*) e la sua integrazione nel nuovo *acquis communautaire* del digitale.

Digitalisation has revolutionised the press and the way citizens are informed, this requires a necessary reflection on the new perspectives of freedoms and rights connected to the infosphere. Moving from the constitutional rank sources and the different regulatory approach adopted by the US and Europe, the essay aims to examine the Proposal for a Regulation of the EU Parliament and Council (European Media Freedom Act) and its integration into the new digital *acquis communautaire*.

Sommario

1. Introduzione. – 2. L'informazione *point to multipoint*. – 3. La necessità di una regolamentazione europea. – 4. Le fonti del diritto dell'informazione. – 5. Il pluralismo delle fonti informative nell'era digitale. – 6. Il differente approccio regolatorio tra USA ed Europa. – 7. La regolamentazione della rete nell'UE e la tutela del pluralismo informativo. – 8. La legittimazione dell'UE ad adottare lo EMFA. – 9. Lo *European Media Freedom Act*. – 9.1. I *consideranda* della Proposta di Regolamento. – 9.2. I diritti degli attori dell'ecosistema editoriale e il rafforzamento della trasparenza. – 9.3. Il contrasto alla frammentazione normativa e l'implementazione della cooperazione tra le autorità nazionali competenti. – 9.4. L'implementazione del dialogo con le piattaforme più grandi (cd. *very large online platforms, VLOPs*). – 9.5. Le regole per il corretto funzionamento del mercato interno dei media – 9.6 La pubblicità di stato. – 10. Conclusione.

Keywords

stampa – pluralismo – *European Media Freedom Act* – Unione europea – digitalizzazione

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

1. Introduzione

Il 16 settembre 2022 la Commissione europea ha presentato lo *European Media Freedom Act*[1]. Un provvedimento nato per proteggere il pluralismo e l'indipendenza dei media nell'UE. Il regolamento proposto prevede, tra l'altro, l'introduzione di garanzie contro le interferenze politiche nelle decisioni editoriali e contro la sorveglianza dei giornalisti. Inoltre, pone l'accento sull'indipendenza e sul finanziamento stabile dei media da parte del servizio pubblico, nonché sulla trasparenza della loro proprietà e sull'allocazione della pubblicità di stato. Si stabiliscono misure per proteggere l'indipendenza dei redattori e per rendere noti i conflitti di interesse. Infine, si prevede la creazione di un nuovo indipendente Consiglio europeo per i Servizi dei Media, composto dalle autorità nazionali del settore[2].

In questo contributo si cercherà di affrontare le questioni di ordine pratico e costituzionale connesse all'accostamento tra la rivoluzione tecnologica e la società dell'informazione. In primo luogo, ci si interrogherà sull'opportunità di adottare uno specifico strumento regolatorio e se non fossero già sufficienti le norme all'uopo previste nelle fonti che regolano il mercato digitale (*i.e,* DSA, DMA e AVMSD). Sotto l'aspetto più strettamente costituzionale, si indagherà, dapprima, sulla legittimazione dell'UE ad adottare un provvedimento che influisce in maniera molto determinante sui valori costituzionali intrinseci alla tradizione di ogni stato e, successivamente, sulla possibilità di estendere ad internet le logiche proprie dello Stato di diritto, oppure, al contrario se sia necessario abbandonare i conosciuti schemi concettuali per rispondere all'esigenza di regolamentare il diritto all'informazione in rete.

2. L'informazione *point to multipoint*

Per comunicazioni di massa (in inglese *mass media*) ci si riferisce all'«insieme dei mezzi per far conoscere, diffondere e divulgare messaggi significativi, carichi di valori diversi, a un pubblico anonimo, indifferenziato e disperso, e anche le tecniche con le quali gruppi specializzati elaborano e diffondono informazioni, messaggi, segni e simboli, nonché le informazioni e i messaggi stessi»[3]. Lo sviluppo tecnologico ha determinato una forte mutazione ed innovazione degli strumenti di comunicazione di massa, determinando una radicale modifica dalla modalità *point to point* a quella *point to multipoint*[4], tipica di alcuni strumenti, quali la televisione ed oggi, soprattutto, internet. La modifica di questa prospettiva, da un lato, ha consentito di superare i limiti intrinseci ai media

[1] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno (legge europea per la libertà dei media) e modifica la direttiva 2010/13/UE*, COM(2022) 457 final. Di seguito anche EMFA, o la Proposta di Regolamento o la Proposta.

[2] Il breve riassunto della Proposta di Regolamento è del *Comunicato stampa della Commissione europea* del 16 settembre 2022, in *ec.europa.eu*.

[3] Treccani, *Comunicazioni di massa*, in *Enciclopedia Online*, in *treccani.it*.

[4] Così come definito da S. D'Alfonso, *Mezzi di comunicazione di massa*, in S. Cassese (diretto da) *Dizionario di diritto pubblico*, Milano, 2006, 3632.

tradizionali[5] (ad esempio, giornali fortemente partigiani o localizzati in una specifica area geografica)[6], dall'altra parte, si è scontrata con l'incapacità cognitiva dell'uomo di scegliere, valutare e approfondire una quantità così ingente di informazioni proveniente da diverse fonti (cd. infodemia[7]). Se da un punto di vista biologico l'infodemia costituisce un problema, sotto la lente del diritto costituzionale assicura il pieno compimento del pluralismo dell'informazione, a cui tende la norma contenuta nell'art. 21 Cost[8]. L'avvento delle nuove tecnologie nel campo dell'informazione permette di amplificare le più flebili voci dell'opposizione, soprattutto in contesti di regimi poco democratici; un'opposizione adeguatamente informata può scegliere di diffondere sui *social media* il contenuto ricevuto da una tradizionale fonte di informazione (la stampa). Tale caratteristica è sovente illustrata per mezzo della equazione secondo cui un'elevata diffusione di Internet è connessa a risultati più avanzati in materia di libertà di stampa[9].

Tuttavia, tale circostanza non esime il legislatore dall'occuparsi di trovare una regolamentazione che possa essere considerata idonea a garantire la neutralità dei *mass media* (in particolare, di internet) e dal configurare delle idonee ipotesi di responsabilità per gli intermediari (cd. *internet service provider*), in considerazione della natura aterritoriale e dell'accesso illimitato che caratterizza la rete[10].

3. La necessità di una regolamentazione europea

Il predominante ruolo impresso dalla tecnologia alla rete e, in particolare, alle piattaforme di condivisione ha consentito alle stesse di accumulare quantità sempre maggiori di ricchezza e di potere[11]. Tali piattaforme hanno assunto la capacità di influenzare i processi di formazione dell'opinione pubblica, modellare le convinzioni politiche e le intenzioni di voto dei cittadini, minando il corretto funzionamento della democrazia. Tuttavia, in considerazione del dichiarato ruolo di meri intermediari di servizi, le piat-

[5] La realtà dei fatti ci impone di considerare come le più autorevoli fonti di informazione non sono mutate nel passaggio alla digitalizzazione, è semplicemente cambiato lo strumento per mezzo del quale essi operano, così A. Koltay, *The Regulation of the Internet and its Gatekeepers in the Context of the Freedom of Speech*, in *New Media and Freedom of Expression: Rethinking the Constitutional Foundations of the Public Sphere*, Oxford, 2019, 75 ss.

[6] Sul tema A. Bhagwat, *Cacophony: speech and press in the internet era*, in *Our democratic First Amendment,* Cambridge, 2020, 106.

[7] «La situazione della Rete viene così a essere strutturalmente caratterizzata dall'impossibilità dell'essere umano di gestire la gran massa delle informazioni disponibili. Ricorrendo ai parametri tradizionali, si è parlato di una nuova forma di scarsità, la quale oggi non riguarderebbe più la natura e/o il costo dei mezzi usati per la diffusione (come l'etere), ma il tempo e l'attenzione degli utenti». Così, M. Manetti, *Regolare internet*, in questa *Rivista*, 2, 2020, 49 ss. Sul punto si consideri anche G. Pitruzzella, *La libertà di informazione nell'era di Internet*, ivi, 1, 2018, 39 ss.

[8] Sul tema M. Manetti, *Pluralismo dell'informazione e libertà di scelta*, in *Rivista AIC*, 1, 2012, 2.

[9] Sul tema K. Kocak – Ö. Kibris, *Social media and press freedom*, in *British Journal of Political Science*, New York, 2022.

[10] Ivi, 3641.

[11] S. Zuboff, *The age of surveillance capitalism: the fight for a human future at the new frontier of power*, in New York, 2019.

taforme di condivisione non sono titolari di una responsabilità editoriale e di tutti gli altri obblighi statuiti per gli organi di informazione.

Emerge, pertanto, l'urgenza di centralizzare a livello europeo i capisaldi della tutela del pluralismo dell'informazione. In questo senso la Commissione europea ha intrapreso un lungo percorso[12], che ha portato lo scorso settembre alla pubblicazione della proposta di European Media Freedom Act (EMFA)[13]. È da tempo che le istituzioni europee si erano interrogate sull'opportunità di offrire una risposta coesa a tale fenomeno: infatti, già la Risoluzione del Parlamento europeo del 10 marzo 2011 e la European Citizen Initiative for Media Pluralism[14] del 2015 si ponevano il fine di promuovere l'adozione di una legislazione europea, che potesse garantire l'indipendenza dei media da interessi economici e politici[15].

Più nello specifico, la necessità di una specifica regolamentazione viene anche evidenziata dall'emergere in maniera rilevante di nuove fonti informative non regolamentate e poco affidabili o, altre volte, artatamente create da autorità o soggetti privati stranieri per manipolare i processi elettorali e destabilizzare gli Stati[16]. L'opportunità di godere di un'informazione di qualità è risultata evidente durante la pandemia da Covid-19, dove l'Italia ha dato prova di essere una democrazia matura, dimostrando di essere capace di offrire «un'informazione libera, polifonica, autorevole e capace di illuminare il potere»[17], consentendo ai cittadini di conoscere effettivamente la realtà, sebbene drammatica[18]. Sono, infatti, altri gli Stati europei che hanno registrato e continuano a registrare costanti minacce alla propria libertà di stampa. La recente audizione al Parlamento europeo del vicedirettore del giornale polacco Polityka[19], Łukasz Lipiński, ha posto l'accento su come i media dell'Europa orientale siano stretti tra i giganti del tech e i poteri autoritari, che usano strumenti sempre più sofisticati per esautorare le opposizioni. Infatti, il giornalista ha evidenziato come nel suo Paese il governo stia estendendo il potere sui media indipendenti e sulla tv pubblica, rendendo i più piccoli

---

12 Si veda Commissione europea, *Safeguarding media freedom in the EU – new rules – Call for evidence for an impact assessment*, 2021, in *ec.europa.eu*, nonché Commissione europea, *Public consultation for a European Media Freedom Act*, in *ec.europa.eu.*

13 Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno (legge europea per la libertà dei media) e modifica la direttiva 2010/13/UE*, COM(2022) 457 final.

14 Disponibile al link *mediainitiative.eu/our-history*, che non ha mai visto alla luce, non avendo raggiunto il numero minimo di firmatari richiesto dal regolamento (UE) n. 211/2011.

15 R. Mastroianni, *Freedom and pluralism of the media: an European value waiting to be discovered?,* in questa *Rivista*, 1, 2022, 106.

16 Y. M. Citino, *Verso l'European Media Freedom Act: la strategia europea contro le minacce al pluralismo e all'indipendenza dei media da una prospettiva de iure condendo*, in questa *Rivista*, 2, 2022, 233.

17 G.E. Vigevani, *Sistema informativo e opinione pubblica nel tempo della pandemia*, in *Quaderni costituzionali*, 4, 2020, 783 ss. Sul tema anche Commissione europea, *Comunicazione congiunta al Parlamento Europeo, al Consiglio Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Contrastare la disinformazione sulla Covid-19 – Guardare ai fatti*, JOIN(2020) final.

18 L'intervento del potere politico sui media in situazioni di crisi al fine di impedire la diffusione di notizie che possano creare panico o abbattere il morale della popolazione è una tendenza comune non solo ai regimi autoritari.

19 A. Rogal, *Journalists call for EU policymakers to deliver 'robust' Media Freedom Act in face of increasing state-owned harassment*, in *The Parliament*, *theparliamentmagazine.eu.,* 14 luglio 2021.

organi di stampa e la stampa estera dei fari di libertà. Tuttavia, anche questi ultimi sono destinati all'estinzione, dal momento che, da un lato, la società petrolifera nazionale, Orlen, sta impiegando risorse per la loro acquisizione[20] e, dall'altro, la stampa estera è profondamente avversata dai recenti provvedimenti governativi[21]. È la stessa relazione sullo Stato di diritto dell'Unione europea per il 2021 che rileva la crescente intensità delle influenze esogene sui media: solo per citare due esempi, a Malta i due principali partiti politici posseggono emittenti televisive e radiofoniche e ciò ha provocato un sindacato di costituzionalità sull'autorità di regolamentazione dei media; in Slovenia si sospetta che le previste modifiche del *budget* dell'emittente pubblica siano dettate da motivazioni politiche[22]. Il settore dei media è parte del più ampio ecosistema dell'industria della cultura, che rappresenta uno dei 14 ecosistemi produttivi individuati per la transizione digitale e *green*. La garanzia di media indipendenti produce delle esternalità positive, non solo in ambito economico, ma consente anche di assicurare l'accesso al pluralismo informativo.

Inoltre, come emerso dalla Relazione Annuale sullo Stato di Diritto sopra citata, il modello attuale si caratterizza per una scarsa cooperazione tra le autorità regolatorie dei diversi Stati membri, rendendo concretamente inefficaci le strategie adottate dall'attuale autorità europea (*European Regulators Group for Audiovisual Media Services*, ERGA[23]). L'ERGA, inoltre, non dispone di sufficienti strumenti per scoraggiare l'utilizzo da parte dei cittadini di Internet Service Provider che siano finanziariamente o editorialmente controllati da alcuni Paesi terzi. A questo riguardo, le opacità connesse alla proprietà di alcuni fornitori di servizi multimediali producono una non chiara

[20] *Polish state-run oil company buys leading media group*, 21 agosto 2020, in *dw.com*.

[21] D. Tambini, *What the EU's Media Freedom Act could mean for journalism in Europe* in *LSE European Politics and Policy blog*, 2021.

[22] Commissione europea, *Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni, Relazione sullo Stato di diritto 2021, La situazione dello Stato di diritto nell'Unione europea*, COM(2021) 700 final, 19: «In Cechia il consiglio di vigilanza della televisione nazionale ha continuato a risentire di controversie politiche. A Malta, poiché i due principali partiti politici possiedono emittenti televisive e radiofoniche, la sezione pertinente della legge nazionale in materia di radiodiffusione è stata sottoposta a sindacato costituzionale, contestando il modo in cui l'autorità di regolamentazione dei media applica le norme. In Slovenia i portatori di interessi ritengono che i progettati cambiamenti del finanziamento dell'emittente di servizio pubblico e la pressione esercitata sull'agenzia di stampa nazionale siano dettati da motivazioni politiche. In Polonia la potenziale acquisizione di un grande gruppo editoriale privato da parte di una società petrolifera controllata dallo Stato ha sollevato dubbi in quanto potenziale minaccia per il pluralismo dei media. In Bulgaria l'influenza politica sui media continua a destare preoccupazione, anche a causa della mancanza di norme che impediscano ai politici e ai partiti politici di possedere mezzi di informazione. In Ungheria il Consiglio dei media ha adottato una serie di decisioni che hanno comportato l'interruzione delle trasmissioni di una delle ultime stazioni radiofoniche indipendenti del paese».

[23] L'ERGA «riunisce i direttori o i rappresentanti di alto livello degli organismi nazionali di regolamentazione indipendenti nel settore dei servizi audiovisivi, per consigliare la Commissione sull'attuazione della direttiva UE sui servizi di media audiovisivi (AVMSD)». Gli obiettivi che persegue sono: «consigliare e assistere la Commissione nel suo lavoro, per garantire un'attuazione coerente della direttiva AVMSD e per qualsiasi altra questione relativa ai servizi audiovisivi di competenza della Commissione.; facilitare la cooperazione tra gli organismi di regolamentazione dell'UE, come previsto dalla direttiva che disciplina i servizi di media audiovisivi; consentire uno scambio di esperienze e di buone pratiche». Così *European Regulators Group for Audiovisual Media Services*, *About ERGA*, in *erga-online.eu*. (trad. mia).

e ingiusta allocazione delle risorse economiche. In particolar modo, l'esternalità negativa si registra con riferimento all'utilizzo di fondi pubblici per scopi pubblicitari. Pertanto, come emerso dalla Conferenza sul Futuro dell'Europa[24], l'Unione è chiamata ad implementare l'indipendenza dei *media*, il pluralismo e la protezione dei giornalisti, attraverso l'introduzione di livelli minimi standard comuni a tutta l'Unione europea, nonché a fronteggiare la disinformazione e le interferenze straniere.

L'urgenza di adottare detto provvedimento legislativo è stata evidenziata, anche, al di fuori dei confini dell'Unione europea dall'Osservatorio Audiovisivo del Consiglio dell'Europa[25], il quale ha prodotto una relazione sul tema dell'indipendenza dei *media* pubblici. Inoltre, sono concordi sul tema anche le organizzazioni *no-profit* e gli emittenti del servizio pubblico, i quali sottolineano l'importanza di introdurre linee guida comuni per la salvaguardia di un giornalismo online di qualità, al fine di poter effettivamente assolvere ad un interesse generale. Infine, anche gli emittenti privati supportano l'adozione di principi comuni per la valutazione del grado di pluralismo dei *media* e la trasparenza interna alle loro strutture aziendali, nonché l'implementazione della tutela delle fonti giornalistiche.

Un approccio regolativo comune – così come previsto dalla proposta di un EMFA – potrebbe non solo centralizzare a livello europeo alcuni capisaldi in tema di indipendenza dei media, ma anche rispondere ad alcune ulteriori esigenze di ordine pratico. Infatti, l'attuale formulazione della AVMSD (*Audiovisual Media Services Directive*) risulta inidonea a garantire l'imparzialità e l'integrità del mercato europeo dei media, per questa ragione la Proposta di Regolamento prevede di introdurre specifiche norme sulla trasparenza degli assetti proprietari. Parimenti, in considerazione del crescente impatto che i contenuti resi disponibili e aggregati dalle piattaforme digitali svolgono sul dibattito pubblico, risulta assolutamente inadeguato che queste ultime siano regolate dalla *eCommerce Directive*, risalente al 2000. Tuttavia, anche laddove si prendesse in considerazione la normativa recentemente entrata in vigore in materia di regolamentazione del mercato interno digitale (*i.e.,* il *Digital Service Act*, DSA), la stessa risulterebbe parzialmente inidonea a garantire il pluralismo dei media: l'assenza di una definizione di "contenuto nocivo"[26] potrebbe produrre un quadro normativo gravemente disarmonico tra i diversi Stati Membri[27].

Alla luce di quanto appena descritto, è emersa[28] l'urgenza di dotare l'*acquis communautaire* di uno strumento normativo che sappia prevedere adeguati meccanismi di controllo

[24] Conferenza sul Futuro dell'Europa – *Report on the Final Outcome*, May 2022, in particolare Proposal 27 (1) and 37 (4).

[25] Sul tema F.J. Cabrera Blàzquez – M. Cappello – J. Talavera Milla – S. Valais, *Governance and independence of public service media*, IRIS Plus, European Audiovisual Observatory, Strasbourg, 2022.

[26] La connotazione di contenuto nocivo risulta essere di fondamentale rilevanza al fine di porre in essere le "adeguate misure di mitigazione del rischio" contro la disinformazione.

[27] M. Cantero Gamito, *Consistent regulatory and self-regulatory mechanisms for media freedom in the Digital Single Market: the European Media Freedom Act (EMFA) as meta-regulation*, Working Paper, in *Robert Schuman Centre for Advanced Studies – Centre for media pluralism and media freedom*, 42, 2022, 9.

[28] Sono diversi gli atti nei quali le istituzioni UE hanno evidenziato questa priorità, *inter alia*: Consiglio dell'Unione europea, *Conclusioni sulla salvaguardia di un sistema mediatico libero e pluralistico*, 2020/C 422/08, in *eur-lex.europa.eu*; Consiglio dell'Unione europea, *Conclusioni sui media europei nel decennio digitale: un piano d'azione per sostenere la ripresa e la trasformazione*, 8727/21, in *europarla.europa.eu*.

dei contenuti condivisi sui *social network* e definire le regole di comportamento per i *service provider*, affinché quest'ultimi adottino degli algoritmi che siano effettivamente neutrali (soprattutto durante le campagne elettorali[29]) e tendano alla realizzazione del pluralismo, nonché adottino delle politiche di lunga durata che favoriscano la circolazione di un'informazione di buona qualità[30].

La regolazione di un fenomeno tanto delicato quale la libertà di stampa e il diritto ad essere informati in un ecosistema, dove si confrontano diversi ordinamenti con differenti tradizioni costituzionali, pone inevitabilmente il legislatore nella situazione di dover adeguatamente analizzare le fonti, al fine di operare un corretto bilanciamento tra i diversi interessi in gioco[31].

4. Le fonti del diritto dell'informazione

La libertà di espressione può declinarsi in libertà di espressione "attiva" (intesa come diritto di ognuno di esprimere la propria opinione) e in libertà di espressione "passiva" (nel senso di essere titolari del diritto di essere adeguatamente informati). Quest'ultima accezione è strettamente connessa allo svolgimento della professione giornalistica, che oggi incontra sempre nuove sfide nell'era della digitalizzazione.

Già nella Dichiarazione Universale dei Diritti Umani, adottata dall'Assemblea generale delle Nazioni Unite il 10 dicembre 1948, si affermava che «Ogni individuo ha diritto alla libertà di opinione e di espressione incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere».

In ambito europeo, l'art. 10 della Convenzione europea dei Diritti dell'uomo dispone che «Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive». Questa norma è stata al centro di un'importante decisione della Corte EDU – *Autronic AG c. Svizzera*[32] – nella quale si chiarisce che l'applicabilità dell'art. 10 della Convezione non deve essere limi-

[29] Sull'effetto delle digital platforms durante le campagne elettorali si consideri M. Monti, *Le Internet platforms, il discorso pubblico e la democrazia*, in *Quaderni costituzionali*, 4, 2019, 816 ss.

[30] R. Montaldo, *La tutela del pluralismo informativo nelle piattaforme online*, in questa *Rivista*, 1, 2020, 229.

[31] La difficoltà di regolare in maniera compiuta questa fattispecie traspare chiaramente dalle parole di C. Esposito, *La libertà di manifestazione del pensiero*, in *Rivista italiana per le scienze giuridiche*, 2, 2011, 29. L'A., con riferimento all'ordinamento italiano, afferma: «In sostanza, dunque, la tesi che in Italia la garanzia costituzionale del diritto di manifestazione del pensiero si limiti a sancire la libertà dall'azione preventiva dei censori, della polizia, dei giudici o delle leggi, ma non la libertà dalla disciplina o dalle limitazioni sostantive del diritto è doppiamente inesatta: per ciò che afferma e per ciò che nega. Non è esatto che sia vietato alle leggi, in modo specifico, di impedire, le manifestazioni vietate, perché in via di principio quando una manifestazione è vietata, le leggi hanno questo potere. Non è esatto che la Costituzione attribuisca alle leggi potestà di discriminare pensiero da pensiero e di vietare le manifestazioni per il loro contenuto, perché in via di principio proprio questo potere è negato alle leggi».

[32] CEDU, *Autronic AG c. Svizzera,* ric. 175/231 (1989), § 15.

tato alla libertà di per sé, ma anche al mezzo che consente la piena fruibilità del diritto stesso, ossia la rete.[33]

Anche l'Unione europea ha recepito nel proprio *acquis* questo importante principio, così formulato nell'art. 11 della Carta di Nizza: «Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. La libertà dei media e il loro pluralismo sono rispettati».[34] Da queste parole emerge la strettissima relazione esistente tra la democrazia e la libertà di informazione, dal momento che godere di media liberi e di una pluralità di voci nella società costituisce «un'indispensabile precondizione e un'essenziale tutela per una democrazia in salute»[35]. Comprendiamo la centralità assoluta che viene assegnata dall'Unione europea a "la libertà dei media e al loro pluralismo" tanto dalla posizione enfatica con cui questa espressione è collocata nella disposizione, quanto dall'esplicito richiamo che viene operato, a differenza di quanto compiuto dell'art. 10 CEDU[36].

La rilevanza di tali principi si riscontra anche nell'art. 2 TUE. Quest'ultimo, infatti, nel richiamare i valori fondanti dello stato di diritto, considera il pluralismo, giustificando la rilevanza che la Commissione europea riserva alla libertà dell'informazione e all'indipendenza dei media nella Relazione annuale sullo Stato di diritto dell'Unione (come meglio illustrato *infra*)[37]. Sebbene la formulazione di questa disposizione non ponga in maniera esplicita un obbligo per gli Stati Membri, risulta inevitabile – come chiarito dalla Corte di giustizia[38] – che essi si adeguino ai principi fondanti e comuni dell'Unio-

[33] È di opinione differente il costituzionalista statunitense Eugene Volokh, secondo cui la stampa deve essere intesa come una tecnologia, il che significa che qualsiasi persona che parla attraverso i media ha diritto alla protezione completa garantita dalla libertà di parola, ma come impresa, la stampa non avrebbe diritto ad alcuna protezione aggiuntiva (così come riportata da A. Koltay, *The Regulation of the Internet and its Gatekeepers*, cit., 78).

[34] Sul punto si consideri, *inter alia*: R. Mastroianni – G. Strozzi, *Articolo 11*, in R. Mastroianni *et al.* (a cura di) *Carta dei diritti fondamentali dell'Unione Europea*, Milano, 2017, 217.

[35] R. Mastroianni, *Freedom and pluralism of the media: an European value waiting to be discovered*, cit., 103.

[36] Mastroianni (ivi, 107) si interroga largamente su quali possano essere gli strumenti utilizzabili dall'Unione europea per garantire l'implementazione dell'art. 11 della Carta di Nizza. L'A. immagina un modello tradizionale, secondo il quale gli Stati Membri sarebbe colpiti da procedure di infrazione, laddove le norme nazionali sulla proprietà dei media e il loro controllo – quindi a tutela del pluralismo informativo – non consentano (o concretamente ostacolino) l'entrata nel mercato nazionale di entità stabilite in altri Stati membri. Secondo l'approccio innovativo, invece, l'A. considera il pluralismo informativo come una precondizione necessaria per l'esercizio del diritto di voto. Infatti, dal momento che l'art. 39 della Carta stabilisce il diritto a votare e a candidarsi alle elezioni del Parlamento europeo e l'art. 14, par. 3, TUE afferma che i membri del Parlamento europeo sono eletti a suffragio universale diretto, libero e segreto, una violazione delle norme che sovraintendono alla tutela del pluralismo informativo e alla libertà dei media costituisce in concreto un'inosservanza delle norme deputate alla tutela del suffragio universale.

[37] Commissione europea, *Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni, Relazione sullo Stato di diritto 2021, La situazione dello Stato di diritto nell'Unione europea*, COM (2021) 700 final, 19: «Il pluralismo dei media e la libertà dei media sono elementi essenziali dello Stato di diritto, della responsabilità democratica e della lotta contro la corruzione».

[38] CGUE, C-791/19, *Commission v. Poland - Régime disciplinaire des juges*: «l'Unione europea è composta da Stati che si sono impegnati liberamente e volontariamente a rispettare i valori comuni di cui all'articolo

ne europea[39]. Pertanto, è possibile ritenere che il combinato disposto degli artt. 39, c. 2, e 11, c. 2, della Carta e dell'art. 2 TUE impone agli Stati Membri di dotarsi di adeguate procedure, affinché le elezioni dei membri del Parlamento europeo si realizzino in un ambiente nel quale gli elettori abbiano accesso ad un'informazione plurale[40].

Sotto questo aspetto, l'Italia, in particolare la sua Costituzione, condivide il valore intrinseco di questi principi. Infatti, l'art. 21 Cost., nei primi due commi, racchiude sia la declinazione attiva (diritto di informare) sia la declinazione passiva (diritto di essere informati) della libertà di espressione, che, secondo le più risalenti sentenze della Corte costituzionale, costituiscono «il presupposto per la corretta formazione dell'opinione pubblica su cui si fonda la democrazia»[41]. Infatti, la sopracitata norma afferma che: «Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. La stampa non può essere soggetta ad autorizzazioni o censure». La particolare formulazione della norma (*i.e.,* l'attribuzione del diritto a tutti e non solo ai cittadini e l'assenza di ogni riferimento al contesto sociale) e il suo posizionamento tra i rapporti civili fanno ritenere che non si tratti di un diritto funzionale, bensì di un diritto individuale[42]. Si giunge a tale tesi per mezzo del combinato disposto con l'art. 2 Cost., il quale, richiamando i diritti inviolabili dell'uomo, ipotizza l'esistenza di alcuni diritti che sono attribuiti allo stesso come tale, in virtù delle sue qualità universali e per il soddisfacimento dei suoi bisogni egoistici. La libertà di espressione, pertanto, non può che essere ritenuta incontrovertibilmente utile allo svolgimento di una vita democratica[43]. Non sarebbe ammissibile una differente interpretazione, poiché la stessa si porrebbe in contrasto con le ragioni storiche della rivendicazione del diritto individuale di manifestazione del pensiero. In questo senso, la Costituzione italiana non solo risulta essere pienamente conforme con i principi sovranazionali appena descritti, ma può porsi come esempio per il legislatore europeo. La modernità del "modello italiano" non è limitata al riconoscimento del diritto, ma si manifesta, soprattutto, con riferimento al riconoscimento del valore del pluralismo informativo. Infatti, risale al 1988 la sentenza con la quale la Corte costituzionale, con riferimento alle emittenti televisive, dopo aver evidenziato l'importanza del pluralismo informativo, ne proponeva una definizione[44] che tutt'oggi appare essere moderna. Infatti, dal momento che nella maggior parte dei casi il "monopolista"

2 del TUE, che li osservano e che si impegnano a promuoverli» (trad. mia).

39 Il pluralismo dei media è un principio ampiamente affermato dalla Corte di Giustizia dell'UE, che, a varie riprese, lo ha considerato preminente rispetto alla tutela della libera prestazione di servizi. Si considerino, inter alia, le sentenze: CGUE, C-555/19, *Fussl Modestraße Mayr* (2021); C-283/11, *Sky Österreich* (2013); C-719/18, *Vivendi* (2020).

40 R. Mastroianni, *Freedom and pluralism of the media: an European value waiting to be discovered*, cit., 109.

41 F. Donati, *L'art. 21 della Costituzione settanta anni dopo*, in *RDM*, 1, 2018, 95.

42 C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano,* cit., 21.

43 Ivi, 23.

44 Corte cost., 14 luglio 1988, n. 826, Il pluralismo consiste nella «possibilità di ingresso, nell'ambito della emittenza pubblica e di quella privata, di quante più voci consentano i mezzi tecnici, con la concreta possibilità [...] che i soggetti portatori di opinioni diverse possano esprimersi senza pericolo di essere emarginati a causa di processi di concentrazione delle risorse tecniche ed economiche nelle mani di uno o di pochi».

assume la funzione di supremo controllore del pensiero da manifestare, sulla base di ragioni economiche, tecniche o ideologiche, la Costituzione, «riconoscendo a tutti il diritto di diffondere il proprio pensiero con ogni mezzo di diffusione, […] ha escluso la costituzionalità di ogni legge che consenta o istituisca o non ostacoli qualsiasi forma di monopolio»[45]. Pertanto, è possibile concludere che le cautele immaginate 75 anni fa dalla nostra Costituzione risultano essere ancora efficaci nella realtà digitale, dove la concentrazione in poche di mani dei mezzi di comunicazione di massa può produrre conseguenze gravemente pregiudizievoli per il corretto dibattito democratico [46].

5. Il pluralismo delle fonti informative nell'era digitale

È indubbio che l'avvento della rete ha consentito agli utenti di ricevere ed inviare informazioni facilmente e gratuitamente in tutto il mondo. Ci si potrebbe spingere fino a ritenere che la digitalizzazione ha effettivamente eliminato la tradizionale distinzione tra libertà di parola e libertà di stampa, in considerazione della possibilità per le masse di poter comunicare con un numero potenzialmente infinito di individui[47]. Infatti, la rete ha eliminato gli ostacoli esistenti tra i giornalisti professionisti e gli opinionisti indipendenti ed ha contribuito a favorire la democratizzazione della sfera pubblica, producendo benefici per la libertà di espressione.

Tuttavia, sarebbe scorretto ritenere che «con l'avvento di internet, il problema della libertà di informazione nel suo profilo attivo (libertà di informare) e passivo (libertà di essere informato) possa considerarsi ormai sostanzialmente superato»[48]; basta volgere lo sguardo alla Cina, per verificare empiricamente lo sfruttamento di tecniche di controllo, di filtraggio dei dati e di censura delle informazioni disponibili in rete. Ancora, emergono notevoli difficoltà per la mente umana nel riuscire a tenere distinte le informazioni dalle opinioni (meritevoli di scarso credito), in considerazione della moltitudine di contenuti in cui essa si imbatte (si tratta della cd. "Cyberascades"[49], secondo cui i fatti e le opinioni possono diffondersi rapidamente senza un preventivo controllo o una serie riflessione sulle stesse). Inoltre, l'avvento di servizi informativi disponibili online (e in particolare sui *social network*) ha sostanzialmente modificato le abitudini dei fruitori degli stessi e ha prodotto, come conseguenza, la possibilità per i cd. *news aggregator* di trarre profitti dal lavoro dei giornalisti professionisti, a fronte di un impegno alquanto scarso[50].

«Ci sono ragioni per sospettare che il cambiamento dei modelli economici degli organi di stampa rappresenti una sfida molto seria per il libero flusso di informazioni, anche (o forse soprattutto) nei Paesi con una libertà di stampa apparentemente elevata».[51] Per

[45] C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano,* cit., 31.

[46] M. Manetti, *Regolare internet*, cit., 46.

[47] A. Koltay, *The Regulation of the Internet and its Gatekeepers*, cit.,105.

[48] F. Donati, *Internet*, in *Enciclopedia del diritto*, Annuali VII, Milano, 2014, 542.

[49] C. R. Sunstein, *#republic: divided democracy in the age of social media*, Princeton, 2017.

[50] Koltay, *The Regulation of the Internet and its Gatekeepers,* cit., 74.

[51] D. Hiaeshutter-Rice – S. Soroka – C. Wlezien, *Freedom of the press and public responsiveness.* in *Perspectives*

questa ragione, il legislatore europeo, partendo dal presupposto che la rete è essenziale per l'esercizio pratico della libertà di espressione e l'accesso all'informazione[52], ha intrapreso un lungo percorso di regolazione del settore digitale, muovendo dal presupposto che qualsiasi restrizione necessaria ai diritti coinvolti (*in primis* il diritto di essere informato) sia effettuata nel pieno rispetto della Convenzione europea dei diritti dell'uomo e del principio di proporzionalità. Inoltre, la moltitudine dei canali informativi disponibili in rete non esclude che possono determinarsi delle posizioni dominanti potenzialmente lesive del principio pluralistico[53]. Le ordinarie regole che sovraintendono a questo fine non sono suscettibili di trasposizione nell'ambito digitale per diverse ragioni, tra cui la difficoltà di individuare il mercato rilevante. Pertanto, gli interventi finora intrapresi dal legislatore, in particolare europeo, si concentravano su tre direttrici principali: favorire l'accesso ad internet al maggior numero possibile di individui[54], limitare il più possibile le pratiche di controllo e blocco dei dati e graduare la responsabilità degli Internet Service Provider.

La necessità di continuare ad indugiare nel senso della regolamentazione del diritto di informarsi in ambito digitale è stata chiaramente evidenziata dalla Presidente della Commissione europea von der Leyen nella Relazione Annuale sullo Stato di Diritto dell'Unione[55].

Dunque, tra i quattro pilastri da tenere in considerazione per operare la valutazione sullo Stato di Diritto dell'Unione si richiama esplicitamente il "*media pluralism and media freedom*". Più nello specifico, gli ambiti oggetto di scrutinio devono essere: (i) le autorità regolatorie dei media, (ii) la trasparenza nella proprietà dei media e le interferenze governative (*i.e.* la trasparente allocazione dei fondi pubblici per la pubblicità di interesse pubblico), e (iii) il quadro di riferimento normativo per la protezione dei giornalisti.

Emerge, pertanto, la chiara volontà delle istituzioni dell'Unione europea di impegnarsi al fine di rafforzare l'*acquis* europeo nel senso del rafforzamento della protezione, del pluralismo dei media e della loro indipendenza.

6. Il differente approccio regolatorio tra USA ed Europa

Tutti gli esperti di politiche sociali, in particolare i giuristi, appaiono concordare sulla necessità di costruire un nuovo quadro normativo di riferimento per gli Internet *inter-*

on politics, 2021, 481.

52 Direttiva (UE) 2009/140, considerando 4. Sul tema anche M. Manetti, *Pluralismo dell'informazione e libertà di scelta*, cit., 6

53 *Amplius* F. Donati, *Internet*, cit., 543.

54 Si pensi alla proposta di Stefano Rodotà di introdurre l'art. 21-*bis* Cost., avente ad oggetto il diritto di accesso ad Internet ed alla più moderne proposte di inserire l'art. 34-*bis* Cost.

55 «Il Meccanismo europeo dello Stato di Diritto monitora gli sviluppi significativi relativi allo Stato di Diritto negli Stati membri. La Relazione Annuale sullo Stato di Diritto fornisce una sintesi degli sviluppi più significativi negli Stati membri e a livello dell'UE, sia positivi che negativi. […] L'approccio al monitoraggio è lo stesso in tutti gli Stati membri, si basa su informazioni comparabili […] in un dialogo aperto con gli Stati membri». European Commission, *European Rule of Law mechanism: Methodology for the preparation of the Annual Rule of Law Report*, in *ec.europa.eu*.

mediaries. Costoro si sono spinti fino a ritenere opportuno la stipulazione di un nuovo contratto sociale[56], in considerazione della rinnovata responsabilità sociale[57] di cui i nuovi *communication gatekeepers* sono titolari.

Tuttavia, l'approccio regolatorio adottato dai due principali "legislatori" del tema (*i.e.* l'Unione europea e gli Stati Uniti d'America) appare essere estremamente diverso, se non contradditorio sotto alcuni aspetti. È proprio la comparabilità tra i due sistemi per grandezza e condivisione di valori democratici che evidenzia l'opportunità di realizzare un simile confronto. Già nel 1988 si evidenziava la distanza tra i due giganti[58], che veniva ricondotta non tanto ad una diversa visione del mondo, quanto ad un atteggiamento di ottimismo liberale che si scontrava con un sentimento di pessimismo liberale[59]. Nel mondo globalizzato nel quale viviamo emerge più che mai l'urgenza di operare un raffronto tra i diversi modelli regolatori adottati, al fine di consentire alle imprese europee di tenere testa agli altri attori globali sotto l'aspetto degli obblighi di trasparenza e delle regole antitrust[60].

In particolare, gli USA hanno adottato un orientamento di diritto negativo sulla libertà dei media, secondo cui essi dovrebbero essere considerati come oratori al pari di tutti gli altri e la libertà di parola dei media dovrebbe essere tutelata dall'aggressione dello Stato[61]; diversamente, l'approccio dell'Unione europea (e condiviso con il Consiglio d'Europa, Consiglio per i diritti umani delle Nazioni Unite, il Relatore Speciale delle Nazioni Unite) evidenzia non solo l'opportunità di tutelare la libertà dei media dalle interferenze dello Stato, ma anche la necessità di interventi regolatori positivi volti alla promozione dei diritti di espressione dei singoli individui attraverso i *media* in un ecosistema socialmente vantaggioso[62].

L'approccio statunitense alla tutela dei diritti digitali come diritti negativi si è affermato grazie alla giurisprudenza della Corte Suprema. La *ratio* a tale peculiare interpretazione deve ritrovarsi nelle radici storiche del paese: la libertà di stampa è nata durante la Rivoluzione Americana alla fine del XVIII secolo, periodo nel quale gli americani avevano un atteggiamento molto sospettoso nei confronti del potere – l'impero britannico – poiché questi controllavano i media, la libertà di parola e il dibattito attraverso la censura e l'imposizione di nuove tasse. Tale approccio è stato direttamente recepito dal Primo Emendamento, nella formulazione di una positiva affermazione del diritto,

---

[56] V. Pickard, *America's battle for media memocracy: the Triumph of corporate libertarianism and the future of media reform. communication*, in *Society and Politics*, New York, 2014.

[57] Hutchens Commission, *Report of the commission on freedom of the press*, Chicago, 1947.

[58] M. Manetti, *Regolare internet*, cit. 36.

[59] A. Di Giovine, *I confini della libertà di manifestazione del pensiero*, Milano, 1988.

[60] Y.M. Citino, *Verso l'European Media Freedom Act: la strategia europea contro le minacce al pluralismo e all'indipendenza dei media da una prospettiva de iure condendo*, cit., 251.

[61] D. Tambini, *Reconceptualizing Media Freedom*, in M. Moore – D. Tambini (eds.), *Regulating Big Tech: Policy Responses to Digital Dominance*, New York, 2021, 299: «*First, a negative rights approach to media freedom which proposes that media should be considered speakers like any others and that media and speech freedom exists through constraint on state incursion into the speech field*».

[62] *Ibid.*. «*Second, an international human rights approach according to which media freedom requires not only protection against state capture but also positive state intervention to promote expression rights of individuals through media, and special privileges to promote democratic media as a socially beneficial form of speech*».

accompagnato da un divieto di intervento dello Stato[63]: «Il Congresso non promulgherà leggi per il riconoscimento ufficiale di una religione, o che ne proibiscano la libera professione; o che limitino la libertà di parola, o della stampa; o il diritto delle persone di riunirsi pacificamente in assemblea e di fare petizioni al governo per la riparazione dei torti».[64] Nell'era della digitalizzazione, tale principio è stato applicato dalle Corti, adottando un atteggiamento remissivo verso la tutela della libertà di parola, al fine di assicurare una rapida crescita ed un rafforzamento economico delle imprese del web. Queste ultime, pertanto, godono di una quasi completa immunità: «È interessante notare che i fornitori di servizi considererebbero qualsiasi interferenza con l'attuale *status quo* come una limitazione della loro libertà, anche se […] [tali fornitori] non hanno nulla a che fare con i contenuti [asseritamente] viola[ti] e che non si tratta della loro "opinione"".[65] Questa posizione è stata chiarita anche dal costituzionalista americano Eugene Volokh, secondo il quale «se Internet viene considerato principalmente come una tecnologia, la libertà delle imprese che operano nel settore può essere limitato in base agli standard generali della libertà di parola»[66]. In dottrina, detta forma di limitazione è definita "censura per procura" ("*proxy censorship*"), dal momento che si determinerebbe una limitazione *de facto* della libertà di parola, nei casi nei quali un'autorità governativa dovesse chiedere ad un fornitore di servizi internet di valutare la legalità dei contenuti caricati, senza la previsione di alcuna garanzia procedurale[67]. A tal fine, la sezione 230 del *Communications Decency Act* (CDA) del 1996 introduce la cd. *Good Samaritan Clause*, che prevede delle ipotesi di immunità da ogni tipo di responsabilità derivante dall'esecuzione delle attività connesse alla decisione circa quali contenuti rimuovere[68]. Questa tesi è corroborata da diversi casi giurisprudenziali, tra tutti *Zeran c. America Online, Inc*[69], nei quali il giudice ha affermato che la pubblicazione, la modifica e la rimozione dei contenuti ricade nella discrezione del *service provider* e non esclude la sua immunità. Successivamente, il Primo Emendamento, oltre che essere applicato in sede giudiziale, è stato recepito dalle diverse piattaforme digitali quale *policy* interna[70]. Pertanto, è inevitabile che un atteggiamento particolarmente liberale nei confronti di queste società abbia rappresentato un importante fattore di sviluppo per le stesse. Inoltre, il radicamento delle sedi legali sul territorio americano ha reso, spesso, difficile

63 Ivi, 301.

64 Costituzione degli Stati Uniti d'America, I emendamento.

65 A. Koltay, *The Regulation of the Internet and its Gatekeepers*, cit., 98. «*The service providers would consider any interference with the current status quo to be a limitation of their freedom, even though their immunity is based on the theory that they have nothing to do with any infringing content and it is not their 'opinion'*».

66 Ivi, 78.

67 Sul tema S. F. Kreimer, *Censorship by proxy: the first amendment, internet intermediaries, and the problem of the weakest link*, in *University of Pennsylvania Law Review*, 2006.

68 R. Tushnet, *Power without Responsibility: Intermediaries and the First Amendment*, in *George Washington Law Review*, 76, 2008.

69 *Zeran c. America Online*, Inc 129 F3d 327 4th Cir 1997.

70 Si pensi al riguardo la scambio di tweet tra Thierry Breton, Commissario al Mercato Interno dell'Unione europea, ed Elon Musk, in occasione dell'acquisizione da parte di quest'ultimo di Twitter Inc. Elon Musk affermava «*the bird is freed*», il Commissario rispondeva «*In Europe, the bird will fly by our European rules*».

la loro chiamata in giudizio dinnanzi a giurisdizioni differenti[71].

Diversamente, l'approccio adottato dalle organizzazioni internazionali (e *in primis* dall'Unione europea) si pone all'estremo apposto, prevedendo una regolamentazione pubblica del fenomeno. Anche in questo caso, il differente metodo è determinato dalla storia che ha caratterizzato l'Europa alla metà del XXI secolo: i regimi antidemocratici avevano assunto il monopolio dei media e della democrazia e, conseguentemente, i cittadini trovarono nelle Carte costituzionali conforto per la tutela dei propri diritti fondamentali.

La diversità negli approcci regolatori trova il maggior punto di distanza nel fatto che negli USA la libertà di parola e la libertà di stampa, considerata come mezzo per la prima, sono indistinte. In Europa, al contrario, la libertà dei media è più importante della libertà di parola, in considerazione del ruolo di amplificazione che i media giocano nella democrazia e, sotto diversi aspetti, la parola è meno rilevante visto il mero ruolo di intermediazione[72].

«La prima tappa per una regolamentazione efficace è una sintesi teorica che metta insieme queste due condizioni e formi un nuovo approccio basato sui vantaggi di entrambe e su una valutazione realistica delle loro debolezze. Se la visione negativa dei diritti è stata utile agli Stati Uniti e al mondo nel periodo del dopoguerra, in cui la radiodiffusione ha dominato la comunicazione democratica, non riuscirà a conciliare la prossima fase dello sviluppo globale dei media con la democrazia. Finché non si faranno progressi teorici, il dibattito politico sarà un dialogo tra sordi, tra protagonisti per i quali gli stessi termini – come libertà di parola, stampa e media – hanno significati e implicazioni profondamente diversi».[73]

7. La regolamentazione della rete nell'UE e la tutela del pluralismo informativo

L'approccio regolatorio dell'UE, finalizzato al riaffermare la centralità dell'individualità umana nell'ecosistema digitale, sottraendolo alle piattaforme, si è mosso su due direttrici: la regolamentazione dei singoli servizi digitali e l'adozione di regole comuni per tutti i servizi digitali, che possono essere integrate da una normativa più restrittiva prevista dagli Stati membri. Il testo legislativo di base è la Direttiva sui servizi di media audiovisivi[74] (*Audiovisual Media Services Directive,* AVMS), la quale, oggetto di diverse modifiche resesi necessarie dallo sviluppo tecnologico, ha il fine di: «nell'ambito della strategia per il mercato unico digitale […] creare e garantire il corretto funzionamento di un mercato unico dell'Unione europea per i servizi di media audiovisivi, contri-

[71] A. Koltay, *The Regulation of the Internet and its Gatekeepers*, cit., 66.

[72] Così D. Tambini, *Reconceptualizing Media Freedom*, cit., 303.

[73] Ivi, 300.

[74] Direttiva (UE) 2018/1808 del Parlamento Europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.

buendo nel contempo alla promozione della diversità culturale e fornendo un livello adeguato di protezione dei consumatori e dei minori».[75]

Dunque, tale direttiva si rivolge a tutti i fornitori di servizi media audiovisivi e di radiofonia e ai servizi di piattaforma per la condivisione di video (tra questi si devono considerare tutti i soggetti che concorrono alla produzione di programmi televisivi, le piattaforme di intermediazione pubblicitaria online, i motori di ricerca, i *social network*, le piattaforme di *video sharing* e *video streaming* e le testate online)[76].

Concorrono alla costituzione di un ambiente mediatico libero, diversificato e dinamico i due regolamenti entrati recentemente in vigore: il *Digital Services Act* (DSA) e *Digital Markets Act* (DMA).

In particolare, il DSA intende «contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione ed in cui i diritti fondamentali sanciti dalla Carta, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo»[77]. Tale regolamento, sebbene si propone di modificare la E-Commerce Directive[78] – ritenuta oramai obsoleta in considerazione dello sviluppo tecnologico – ne mantiene l'impianto generale: si è preferito l'adozione dello strumento del regolamento, in luogo di quello della direttiva, si mantiene l'esenzione di responsabilità per i *provider* esercenti attività di *mere conduit*, *catching* e *hosting* (combinato disposto artt. 1, c. 2, e 3, c. 1) e si conserva l'assenza di obblighi generali di sorveglianza o di accertamento attivo dei fatti per i prestatori di servizi intermediari (art. 8).

Tuttavia, il regolamento (UE) 2022/2065 introduce degli elementi di novità, tra i quali: l'introduzione della cd. *Good Samaritarian Clause*, secondo la quale lo svolgimento di indagini volontarie, promosse di propria iniziativa da parte dei servizi intermediari, consente il godimento della esenzione dalla responsabilità prevista agli artt. 4, 5 e 6 (art. 7); la creazione di autorità nazionali incaricate della vigilanza dei fornitori di servizi intermediari, con poteri investigativi e sanzionatori, e il coordinamento tra le autorità competenti e gli Stati in materia di servizi digitali (artt. 49 ss.); e

l'adozione di un *risk-based approach*, prevedendo una differenziazione degli obblighi

---

[75] Dunque, «la nuova direttiva apre la strada a un contesto normativo più equo per l'intero settore audiovisivo, compresi i servizi a richiesta e le piattaforme per la condivisione di video. Le nuove norme rafforzano la tutela dei minori e la lotta contro l'incitamento all'odio in tutti i contenuti audiovisivi, promuovono le produzioni audiovisive europee e garantiscono l'indipendenza delle autorità di regolamentazione del settore audiovisivo». (Ministero dello Sviluppo Economico, *Relazione Air - Analisi di impatto della regolamentazione (AIR) relativamente allo schema di decreto legislativo di attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva (UE) 2010/13, relativa alla fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato*, con riferimento allo *Schema di decreto legislativo di attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio*).

[76] *Ibid.* L'avvento delle nuove tecnologie ha evidenziato, infatti, la necessità di ampliare il numero di soggetti che sono tenuti ad osservare l'Informativa Economica di Sistema (IES). Essa consente all'AGCOM di raccogliere le informazioni necessarie (si tratta, in particolare, dei dati anagrafici ed economici, che vengono dichiarati dagli stessi operatori annualmente) per monitorare i settori dei media e adempiere ai precisi obblighi di legge.

[77] Regolamento (UE) 2022/2065, art. 1, par. 1, così come pubblicato nella Gazzetta Ufficiale dell'Unione europea del 27 ottobre 2022.

[78] Direttiva 2000/31/CE.

di trasparenze e supervisione in relazione all'influenza giocata dal singolo servizio intermediario. Al riguardo, è possibile distinguere tra: *intermediary services, hosting services, online platforms e very large platforms* (*inter alia*, artt. 15 e 42).

Diversamente, il DMA[79] si pone il fine di «contribuire al corretto funzionamento del mercato interno stabilendo norme armonizzate volte a garantire, per tutte le imprese, che i mercati nel settore digitale nei quali sono presenti *gatekeeper* (controllori dell'accesso) siano equi e contendibili in tutta l'Unione, a vantaggio degli utenti commerciali e degli utenti finali»[80]. Ai sensi dell'art. 2, par. 1, dello stesso regolamento, per *gatekeeper* si intende «un'impresa che fornisce servizi di piattaforma di base, designata a norma dell'articolo 3», mentre i destinatari del regolamento sono i soggetti di cui all'art. 2, par. 2 (a titolo esemplificativo, servizi di intermediazione online, motori di ricerca online, servizi di social network online, servizi di piattaforma per la condivisione di video). In particolare, i *gatekeepers* saranno titolari di una serie di obblighi volti a tutelare l'effettiva concorrenza nei servizi digitali, così da prevenire condizioni inique per il mercato (artt. 5 ss.). Il testo di legge, inoltre, prevede un sistema sanzionatorio percentuale in relazione al fatturato totale realizzato a livello mondiale su base annua dal fornitore nell'esercizio precedente (art. 74 ss.).

La regolamentazione fornita dal DMA si pone in stretta connessione con la tutela del diritto di espressione in rete, dal momento che la posizione dominante di alcuni *gatekeepers* conferisce loro il potere di influenzare l'utente, scegliendo il contenuto da mostrare in relazione ai propri interessi (pensiamo ai contenuti che vengono mostrati sul *feed* dei maggiori social network). Infatti, «sebbene la nuova direttiva AVMS sottolinei che i "*video-sharing platform services*" non hanno alcuna "responsabilità editoriale", essi possono comunque essere soggetti a obblighi relativi ai contenuti […]. La direttiva riconosce che tali piattaforme organizzano ("visualizzano", "etichettano", "mettono in sequenza") i contenuti degli utenti e, se accompagnate dall'obbligo di intervenire contro i contenuti illeciti, il loro ruolo è chiaramente simile a quello di un editore».[81] La rilevanza del ruolo giocato da tali operatori digitali nel mondo della libertà di espressione delle idee è evidenziato dalla Raccomandazione sulla libertà di internet del 2016[82], nella quale, evidenziando l'importante ruolo degli attori privati, si illustra che, ai sensi dell'art. 10 della Convenzione europea dei diritti dell'uomo, tali attori digitali devono osservare i requisiti di legalità, legittimità e proporzionalità nell'espletamento della loro funzione di blocco, filtraggio e rimozione dei contenuti. Nella maggior parte dei casi, tale attività non è operata da persone fisiche ma da parte di algoritmi, il quale algoritmo può essere considerato come «una sorta di "*editor*", che presenta all'utente contenuti in base alle decisioni del suo creatore e utilizzando i dati raccolti sull'utente durante l'utilizzo del servizio o di altri servizi coevi»[83]. Inoltre, l'attività degli algoritmi non si limita alla mera trasmissione di informazioni, bensì propone un flusso di notizie

[79] Regolamento (UE) 2022/1925, così così come pubblicato nella Gazzetta Ufficiale dell'Unione europea del 12 ottobre 2022.

[80] Regolamento (UE) 2022/1925, art. 1, par. 1.

[81] A. Koltay, *The Regulation of the Internet and its Gatekeepers*, cit., 92.

[82] Recommendation CM/Rec(2016)5[1] *of the Committee of Ministers to member States on Internet freedom.*

[83] S. Halpern, *Mind control & the internet*, in *New York Review of Books*, 2011.

personalizzato per l'utente. Questa circostanza, inevitabilmente, produce delle conseguenze negative sulla polarizzazione del dibattito[84]. Infatti, gli utenti, naturalmente, sono portati a leggere e cercare i contenuti più simili alle proprie convinzioni, escludendo la lettura di coloro i quali hanno opinioni opposte alle proprie. Tale fenomeno è amplificato dai social network[85], i cui algoritmi tendono a mostrare contenuti pubblicati dagli amici o comunque da individui con le stesse opinioni e convinzioni dell'utente[86]. La conseguenza è quella di aumentare la distanza tra gli individui con opinioni confliggenti, indebolendo la coesione sociale e rafforzando gli estremismi[87]. Pertanto, da quanto fin qui esposto, emerge l'opportunità di considerare gli algoritmi come dei mezzi attraverso i quali si realizza la libertà di parola; ciò consente pure a questi servizi di indicizzazione automatica l'applicabilità delle più stringenti garanzie costituzionali e normative per la tutela della libertà di espressione.

8. La legittimazione dell'UE a adottare lo EMFA

Ad una prima visione disattenta, si potrebbe ritenere che i Trattati che definiscono le competenze dell'UE - sia esclusive, sia concorrenti – non comprendano l'adozione di strumenti volti a regolare il pluralismo dei media[88]. Tale posizione, tuttavia, non appare condivisibile, poiché risulta evidente come il possesso dei media da parte di individui che ricoprono cariche pubbliche e la creazione di posizione dominanti nel mercato producono un effetto negativo sul corretto funzionamento del mercato interno[89].
Appare curioso come l'UE radichi la propria competenza a legiferare in materia di libertà dei media nell'art. 114 TFUE, dando, dunque, primaria rilevanza al corretto funzionamento del mercato interno, in luogo della tutela dei diritti. Del resto, non potrebbe essere altrimenti: la tutela delle libertà coinvolge i più intimi aspetti costituzionali di ogni Stato, rispetto ai quali, non solo è precluso l'accesso all'UE, ma, soprattutto, è impossibile adottare un testo legislativo uniforme tra tutti i 27 Paesi[90]. Dunque, emerge chiaramente come il principio del mercato concorrenziale assume il valore di *Grundnorm* di ogni

[84] Sul tema si consideri C.R. Sunstein, *Republic.com Cittadini informati o consumatori di informazioni?*, trad. it, Bologna, 2003, secondo cui si arriverà al momento nel quale il cittadino sarà interessato ad ascoltare esclusivamente opinioni concordi con le proprie. Gli algoritmi tendono proprio a tale risultato. Anche R. Montaldo, *La tutela del pluralismo informativo nelle piattaforme online*, cit., 227.

[85] Nei media tradizionali, gli utenti non possono scegliere i contenuti da leggere o guardare, con l'inevitabile conseguenza di scontrarsi con opinioni differenti e rafforzare il pensiero critico.

[86] Sul tema si veda anche A. Bhagwat, *Cacophony: speech and press in the internet era,* cit., 106 secondo cui «*On social media, people simply are not confronted with serious challenges to their own beliefs and worldviews but rather tend to have their preexisting prejudices confirmed by the speech that they do encounter. It is these tendencies that have, I would argue, degraded political dialogue in the Internet era*».

[87] C.R. Sunstein, *#republic: divided democracy in the age of social media,* cit.

[88] A. Garcia Pires, *Media Pluralism and Competition*, in *Eur. J. Law Econ.*, 2017, 255.

[89] *Inter alia*, R. Mastroianni, *Promoting information pluralism through EU law: regulation of competition law in the Audiovisual Sector?*, in B. Cortese (ed.), *EU competition law*, Zuidpoolsingel, 2013, 33.

[90] Y.M. Citino, *Verso l'European Media Freedom Act: la strategia europea contro le minacce al pluralismo e all'indipendenza dei media da una prospettiva de iure condendo*, cit., 250.

iniziativa legislativa[91].

Tuttavia, tale accostamento operato dal legislatore europeo non appare essere nemmeno eccessivamente artificioso[92]: la creazione *ad hoc* di monopoli o di posizioni dominanti nel mercato dell'informazione, che assegnino ruoli di primaria rilevanza a certi leader politici o ad alcuni partiti, inevitabilmente, interferisce con il corretto esercizio del diritto di voto[93].

La necessità di adottare un approccio comune europeo è evidenziata dall'incapacità dei singoli Stati membri di proporre un'adeguata risposta individualmente. Infatti, la produzione e il consumo di contenuti multimediali, tra cui le notizie, ha carattere sovranazionale; per questa ragione, l'adozione di un approccio comune europeo consente di garantire la certezza del diritto (in considerazione delle differenze sussistenti tra i diversi ordinamenti degli Stati membri), la concorrenza leale tra i diversi fornitori di servizi multimediali e l'opportunità di realizzare investimenti transnazionali per il consolidamento del settore. Pertanto, sebbene una risposta comune europea sia resa necessaria dalle caratteristiche proprie del fenomeno, la proposta di regolamento deve comunque rispettare il principio di proporzionalità[94], che, nel caso di specie, si declina in una ben equilibrata ed armonizzata disciplina, che non ecceda quanto necessario per il raggiungimento di un comune quadro di riferimento normativo per il corretto funzionamento del mercato interno dei servizi multimediali. In particolare, ci si riferisce[95] al divieto di interferire, sfruttando la competenza propria degli Stati membri, nell'erogazione dei fondi pubblici per l'editoria e nello svolgimento di attività di interesse pubblico (così come previsto, dal Protocollo di Amsterdam e dall'art. 4, par. 2, TUE). Infine, sotto il profilo della sussidiarietà, l'intervento del legislatore europeo risulta essere necessario in considerazione dell'assenza di diversi strumenti regolatori, che consentano di godere di media liberi ed indipendenti e, conseguentemente, di un sano sistema democratico[96].

---

91 G.E. Vigevani, *I media di servizio pubblico nell'età della rete: verso un nuovo fondamento costituzionale, tra autonomia e pluralismo*, Torino, 2018, 2.

92 Di opinione contraria, M. Manetti, *Pluralismo dell'informazione e libertà di scelta*, cit., 8; la quale affermava che «La verità è che – come ha ribadito la Commissione europea – non è compito delle Comunità, ma degli Stati membri promuovere tale principio o valore [il pluralismo dei media]».

93 R. Mastroianni, *Freedom and pluralism of the media: an European value waiting to be discovered?,* cit., 109.

94 Puntualmente, la valutazione di proporzionalità viene superata dalla circostanza che differenti normative sui servizi multimediali possono: (i) porre barriere al mercato interno; (ii) creare indebite concentrazioni nel mercato interno; e (iii) determinare un'incoerente implementazione dell'AVMSD, così come successivamente modificata. (così Cantero Gamito, *Consistent regulatory and self-regulatory mechanisms for media freedom in the Digital Single Market: the European Media Freedom Act (EMFA) as meta-regulation*, cit. 12).

95 *Explanatory memorandum, Commissione europea*, *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno (legge europea per la libertà dei media) e modifica la direttiva 2010/13/UE*, COM(2022) 457 final.

96 M. Cantero Gamito, *Consistent regulatory and self-regulatory mechanisms for media freedom in the Digital Single Market: the European Media Freedom Act (EMFA) as meta-regulation*, cit. 14.

9. Lo *European Media Freedom Act* [97]

Alla luce delle considerazioni fin qui esposte, occorre ora indugiare in maniera più metodica sulla Proposta di Regolamento, al fine di individuarne i punti di forza e di debolezza. In questa analisi, ci serviremo della lente privilegiata che ci viene offerta da ERGA[98].

L'EMFA adotta un generale approccio flessibile basato sui principi, che consente, da una parte, una buona integrazione con le fonti che solo parzialmente regolano il fenomeno (*i.e.,* AVMSD, DSA e DMA), dall'altra parte, di proporre un livello minimo di armonizzazione tra le legislazioni dei diversi Stati Membri, a cui dovranno seguire ulteriori norme di implementazione e trasposizione. Risulta apprezzabile l'intenzione del legislatore di estendere in maniera orizzontale l'ambito di applicazione della proposta a tutte le azioni che possano danneggiare la libertà dei media e a tutte le tipologie di servizi multimediali, sia online che offline. La proposta, pertanto, adotta un approccio dinamico che le consentirà di regolare anche fenomeni nuovi, al momento non prevedibili, scongiurando l'eventualità che possano rinvenirsi nuove lacune nell'ordinamento[99]. Tuttavia, l'ERGA evidenzia l'opportunità di chiarire l'esclusione della carta stampata, al fine di evitare possibili conflitti con le specificità, anche di rango costituzionale, proprie di ogni Paese. Inoltre, è opportuno evidenziare il fatto che una tutela effettiva dei media non può non estendersi a tutti gli elementi coevi agli stessi; in questo senso, il legislatore europeo ha inteso prevedere, *inter alia*, un'adeguata protezione dei giornalisti e regolare le situazioni di monopolio informativo e la misurazione dell'audience. Così come già emerso nel dibattito prodromico al DSA, è di grande rilevanza l'interessamento ai servizi multimediali offerti da Paesi terzi e al trattamento offerto dalle cd. *very large online platforms* (VLOPs), che oggi costituiscono per i cittadini il principale strumento di informazione. La Commissione è ben consapevole che non sarà facile implementare un sistema legislativo così complesso in 27 Stati diversi; per questa ragione ipotizza la creazione (o per meglio dire l'implementazione) di un *European Board for Media Services*, il quale, a partire dall'attuale ERGA, dovrà essere dotato di nuove funzioni e responsabilità. Le principali caratteristiche di questo nuovo organo saranno la sua capacità decisoria e l'indipendenza funzionale dalla Commissione.

---

[97] Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno (legge europea per la libertà dei media) e modifica la direttiva 2010/13/UE*, COM(2022) 457 final.

[98] European Regulators Group for Audiovisual Media Services, *Proposal of the Commission for a European Media Freedom Act (EMFA)*, in *erga-online.eu,* novembre 2022; European Regulators Group for Audiovisual Media Services, *European Media Freedom Act (EMFA), ERGA position paper for the Open Public Consultation*, *in erga-online.eu*.

[99] M. Cantero Gamito, *Consistent regulatory and self-regulatory mechanisms for media freedom in the Digital Single Market: the European Media Freedom Act (EMFA) as meta-regulation*, cit., 16. In considerazione di tale circostanza l'A. assegna all'EMFA la definizione di meta-regolamento.

9.1. I *considerandа* della Proposta di Regolamento

Nell'era della digitalizzazione, i servizi mediatici indipendenti mutano rapidamente e costituiscono, da un lato, un settore di primaria rilevanza economica e, dall'altro, realizzano l'essenziale funzione di "cane da guardia" della democrazia. Infatti, de Tocqueville proponeva che la stampa fosse "il principale strumento democratico di libertà", per proteggere gli americani dai pericoli del dispotismo burocratico[100]. Si nota, dunque, che «nei Paesi nei quali la libertà di stampa è più elevata, si riscontra una maggiore reattività pubblica; nei Paesi in cui la libertà di stampa è bassa, i cittadini sembrano meno in grado di notare e reagire alla politica del governo»[101], pertanto si può ritenere che i *mass media* favoriscano *l'accountability* dei governanti[102].

Per questa ragione, la protezione della libertà dei media e la loro indipendenza è essenziale per il buon funzionamento del mercato interno dei servizi, oggi internazionale e digitalizzato. Infatti, le piattaforme digitali, facilmente raggiungibili da tutti i dispositivi personali, rappresentano per la maggior parte dei cittadini i principali punti d'accesso informativo; esse, spesso, escludono l'intermediazione delle cd. fonti tradizionali ed amplificano la polarizzazione dei contenuti, partecipando alla sagomatura dell'opinione pubblica nell'ambito del processo democratico.

Nondimeno, il mercato interno dei servizi d'informazione non è sufficiente integrato, in considerazione delle divergenze che si registrano negli approcci delle diverse autorità nazionali, le quali, perfino, generano delle restrizioni alla libertà di movimento nel mercato interno. Tale ecosistema appare essere in contrasto con il dettato dell'art. 11 della Carta di Nizza, dal quale è possibile ricavare il diritto per ciascun cittadino di poter usufruire di servizi informativi liberi e pluralistici; all'uopo occorre provvedere alla armonizzazione delle discipline nazionali. Per giunta, la necessaria integrazione all'interno dell'Unione appare essere necessaria al fine di garantire la certezza del diritto per tutti i creatori di contenuti, i quali, inevitabilmente, si riferiscono ad un pubblico internazionale.

Non è possibile immaginare un sistema informativo che sia in grado di svolgere effettivamente il proprio ruolo di "cane da guardia" della democrazia in un ambiente in cui non sia presente l'indipendenza editoriale. Non sono tollerabili, quindi, le crescenti interferenze con le scelte editoriali da parte di soggetti pubblici e privati, al fine di ottenere vantaggi personali, (in particolare, politici); si tratta di operare un necessario bilanciamento, da un lato, tra la libertà di espressione e di essere informati e, dall'altro, la libertà editoriale. Al fine di costituire opinioni ben informate e, conseguentemente, partecipare attivamente al dibattito democratico, è essenziale che i fruitori di servizi informativi siano consapevoli di chi abbia la proprietà degli stessi, cosicché essi possano indentificare e comprendere i potenziali conflitti di interesse. Pertanto, l'indipendenza

[100] A. de Tocqueville, *Democracy in America*, II, New York, 1835.

[101] D. Hiaeshutter-Rice – S. Soroka – C. Wlezien, *Freedom of the press and public responsiveness*, cit., 480.

[102] Si veda sul tema anche J. Whitten-Woodring, *Watchdog or Lapdog? Media freedom, regime type, and government respect for human rights*, in *International Studies Quarterly*, 53, 3, 2009, 595 secondo cui «*one of the main justifications for freedom of the news media is that a lack of censorship will enable the news media to act as a watchdog over the government and thereby render the government more responsible and responsive*».

editoriale richiede l'adozione di un approccio proattivo da parte delle organizzazioni che controllano i mezzi di informazione, le quali dovrebbero introdurre misure proporzionate ed adeguate allo scopo (sarebbe opportuno prevedere delle esimenti da tali obblighi regolatori in favore delle microimprese). Tuttavia, non si ritiene siano esenti da tali obblighi di trasparenza le emittenti pubbliche, le quali dovrebbero adottare strumenti ancora più vigorosi per combattere le interferenze esterne, in primo luogo quelle delle istituzioni politiche. In deroga alla normativa antitrust sugli aiuti di stato, deve essere consentito il finanziamento, su base pluriennale, da parte degli Stati membri in misura sufficiente a fornire ai cittadini l'accesso a notizie di qualità ed imparziali.
Inoltre, le regole che proteggono e sovraintendono la professione del giornalista sono profondamente diverse tra i vari Stati membri; tali differenze producono effetti negativi con riferimento alla tutela delle fonti, all'incertezza del diritto connessa alla loro responsabilità legale ed amministrativa. Si pensi, ad esempio, all'impiego di tecnologie di sorveglianza e captazione delle comunicazioni che possono impattare sulla possibilità per il giornalista di raccogliere, verificare ed analizzare le informazioni, che giungono, talvolta, anche da fonti confidenziali. La causa di tale diversità nella regolamentazione deve essere ritrovata nella forte eterogeneità presente tra le diverse autorità nazionali regolatorie; per questa ragione ed al fine di consentire una coerente applicazione di questa Proposta di Regolamento con le altre norme dell'Unione connesse al diritto dei media (*i.e.* direttiva (UE) 2010/13 cd. AVMS), si propone la costituzione del Consiglio Europeo per i Servizi Multimediali (*European Board for Media Services*)[103]. In tale organo, dovrebbero sedere i rappresentanti delle autorità regolatorie nazionali per implementare la cooperazione, al fine di consentire un corretto funzionamento del mercato interno per i servizi multimediali, in stretta connessione con le attività della Commissione. Pertanto, l'obiettivo è la creazione di un quadro di riferimento normativo chiaro e legalmente vincolante, che permetta una cooperazione effettiva ed efficace.
Infine, nell'era della digitalizzazione assumono primaria rilevanza i *providers* di piattaforme digitali più grandi, i quali, al pari degli Stati membri, dovrebbero ingaggiare un dialogo strutturato con il Consiglio Europeo per i Servizi Multimediali. In questo senso, la Proposta di Regolamento si impegna ad assicurare a tutti gli utenti la possibilità di usufruire dei contenuti digitali sulla base delle proprie preferenze, differentemente da quanto l'ordinario funzionamento degli algoritmi sarebbe portato a fare. Viene attribuita particolare rilevanza ai meccanismi di autoregolamentazione credibili e trasparenti, i quali, coerentemente con il dettato di questa nuova fonte del diritto europea, dovrebbero portare alla nascita di codici di condotta, linee guida, standard etici, gestione delle segnalazioni e correzione degli errori.

9.2. I diritti degli attori dell'ecosistema editoriale e il rafforzamento della trasparenza

L'art. 3 della Proposta di Regolamento afferma che «i destinatari dei servizi multimediali nell'Unione hanno il diritto di ricevere una pluralità di notizie e contenuti di attua-

[103] Di seguito, il Board.

lità, prodotti nel rispetto della libertà editoriale dei fornitori di servizi multimediali, a beneficio del dibattito pubblico».
Specularmente, l'art. 4 sancisce il diritto dei fornitori di servizi multimediali di svolgere pienamente le attività economiche senza limitazione alcuna diversa da quelle imposte dal diritto dell'Unione. Infatti, gli Stati membri devono rispettare la libertà di stampa, pertanto, essi non devono interferire in alcun modo con le decisioni editoriali e non devono porre in essere alcuna attività di sorveglianza o captazione dei giornalisti e dei fornitori di servizi multimediali e degli individui ad essi vicini, ad eccezione dei casi nei quali sussiste un pubblico interesse. Al fine di rendere effettiva tale tutela, gli Stati membri devono nominare autorità indipendenti competenti a decidere sulle denunce presentate dai fornitori di servizi multimediali. L'ERGA, pur condividendo l'opportunità di offrire un'adeguata tutela all'indipendenza dei media e un'opportuna riservatezza alle fonti informative – anche al cospetto delle autorità nazionali – evidenzia, da un lato, l'opportunità di estendere tali garanzie anche ai cd. giornalisti *freelancer*, dall'altro lato, la sopracitata indipendenza dei media incontra un limite rispetto alla necessità di perseguire obiettivi di interesse generale (ad esempio, la diffusione di messaggi dell'autorità pubblica su questioni di sanità pubblica).
L'informazione (soprattutto quella finanziata con risorse pubbliche) al fine di realizzare il ruolo di "cane da guardia" della democrazia deve garantire che i cittadini possano accedere ad un'offerta quanto più ampia e plurale di fonti informative. Si tratta di un tema estremamente sensibile, rispetto al quale il legislatore ha una limitatissima potestà legislativa, in considerazione dei limiti stabiliti dal Protocollo 29[104]. Non è possibile, pertanto, spingersi ad una regolazione che vada oltre la definizione di principi, che nel caso di specie appaiono ragionevoli e proporzionati[105]. Infatti, l'art. 5 dispone che «i fornitori di servizi multimediali pubblici devono fornire in modo imparziale una pluralità di informazioni e opinioni al loro pubblico, in conformità con la loro missione di servizio pubblico». Questo obiettivo è raggiunto a partire da modalità di nomina trasparenti (pubbliche e non discriminatorie) e dalla durata dell'incarico del *management*, adeguato e sufficientemente lungo a garantire l'effettiva indipendenza; inoltre, gli Stati membri devono assicurare adeguate risorse economiche per lo svolgimento dell'incarico.
Infine, la Proposta di Regolamento ritiene che i media di informazione, sebbene privati, devono osservare dei doveri di trasparenza, in considerazione del ruolo d'interesse pubblico che svolgono: essi hanno ad oggetto l'opportunità di rendere pubblico e facilmente accessibile le informazioni riguardanti l'impresa e la proprietà, diretta o indiretta, della stessa. Parimenti a quanto sopra espresso, anche questi fornitori di servizi multimediali devono godere di libertà nella determinazione delle decisioni editoriali[106]

[104] *Protocollo sul sistema di radiodiffusione pubblica negli Stati membri allegato al Trattato di Amsterdam*, Protocollo 29, 1997.

[105] European Regulators Group for Audiovisual Media Services, *Proposal of the Commission for a European Media Freedom Act (EMFA)*, in *erga-online.eu,* 4 novembre 2022.

[106] Al riguardo l'ERGA (*ibid.*) evidenzia l'opportunità di distinguere tra "decisioni editoriali individuali" e "linea editoriale". La prima, infatti, rientra nella libertà del singolo giornalista e deve essere preservata da ogni indebita influenza, mentre la seconda si tratta di un elemento strategico sotto l'aspetto economico e, pertanto, può essere oggetto di accordo tra il giornalista e l'editore.

e rivelare potenziali conflitti d'interesse.
La rilevanza che la Proposta di Regolamento riserva al pluralismo dell'informazione è determinata dal fatto che quest'ultimo deve essere considerato come un corollario della libertà dei media[107]. Infatti, la storia europea ha evidenziato come i media devono essere indipendenti dalle istituzioni più potenti (*in primis* dallo Stato), altrimenti essi perdono la propria legittimazione nel processo democratico, fino a poter cagionare grave danno alla democrazia, in considerazione della forte influenza che producono sull'opinione pubblica. In tale contesto, l'attività dei *gatekeepers* pone dei dubbi circa la possibile diretta interferenza che questi hanno con la libertà di parola ed il pluralismo dei media.
«Si noti lo strano paradosso: all'inizio, internet è stato immaginato come la soluzione definitiva alla scarsità di contenuti e prometteva di rendere non più necessarie le precedenti forme di regolamentazione dei media, mentre ora ci troviamo di fronte a problemi già noti al mercato dei media, ma su scala molto più ampia. Ciononostante, la libertà di parola rimane principalmente un "diritto negativo" che protegge il contenuto delle opinioni da fonti esterne di interferenza, ma non garantisce il diritto di utilizzare piattaforme che facilitino l'esercizio effettivo di questa libertà.[108]»
Nonostante, il differente approccio della dottrina europea e della dottrina italiana sul tema della libertà di espressione dei media (illustrato nel paragrafo 6), entrambe concordano sull'opportunità di tutelare il pluralismo dei media. Parimenti a quanto già esposto in ambito europeo, la diversità dei media (come è chiamato il fenomeno oltreoceano, *media diversity*) è tutelata dalla Federal Communication Commission (FCC), la quale, insieme con le altre norme in materia antitrust, si propone di evitare situazioni nelle quali gli operatori del settore dei media diventino talmente dominanti da possedere un potere addirittura superiore a quello degli attori statali[109].

9.3. Il contrasto alla frammentazione normativa e l'implementazione della cooperazione tra le autorità nazionali competenti

Ai sensi dell'art. 8, si istituisce il Consiglio Europeo per i Servizi Multimediali (*European Board for Media Services*), il quale, sostituendo *European Regulators Group for Audiovisual Media Services* (cd. ERGA), godrà di piena indipendenza nell'esercizio delle proprie attribuzioni (con le finalità descritte *supra*). In tale Consiglio siederanno i rappresentanti delle autorità regolatorie nazionali, le quali dovranno essere sostenute dagli Stati membri, anche economicamente. Per esplicita dichiarazione del legislatore, tale organo pone le sue radici nell'art. 30 AVMSD, il quale è stato oggetto di recepimento in quasi ogni Stato dell'Unione. Tuttavia, l'ERGA evidenzia l'opportunità che nella versione finale del regolamento siano presenti delle norme più stringenti che impongano agli Stati Membri di fornire a tali autorità regolatorie nazionali le idonee risorse finanziarie

[107] D. Tambini, *Reconceptualizing Media Freedom*, cit., 308.

[108] A. Koltay, *The Regulation of the Internet and its Gatekeepers*, cit., 90.

[109] D. Tambini, *Reconceptualizing Media Freedom*, cit., 308.

e umane per adempiere ai nuovi compiti loro assegnati.
Inoltre, la piena indipendenza dello stesso Board costituisce un prerequisito necessario per l'implementazione di tale proposta. Per questa ragione, l'ERGA, in risposta alla consultazione pubblica promossa dalla Commissione nei primi mesi del 2022 sul tema dell'EMFA[110], aveva sottolineato come questa autorità dovesse godere di (i) piena autonomia da ogni ente o istituzione (compresa la Commissione europea), (ii) adeguate risorse economiche e umane e (iii) idonee regole di *goverance*, in considerazione delle nuove funzioni assegnate. Sotto tale aspetto, occorre registrare che la Proposta non recepisce le indicazioni suggerite dal Gruppo[111]: sebbene sia astrattamente implementata la struttura del Board (art. 10) ed il suo segretariato generale (art. 11), tali norme sono di impossibile attuazione, in considerazione dell'inefficace e parziale indipendenza che gli viene riconosciuta. Infatti, sarebbe opportuno che tale organo di controllo potesse decidere autonomamente le proprie regole di funzionamento interno, senza alcun preventivo accordo con la Commissione (ad esempio, la durata dell'incarico del Presidente, che l'art. 10 fissa in due anni) e che le relazioni periodiche del segretariato generale fossero inviate al presidente del Gruppo stesso e non alla Commissione.
Tali perplessità si concretizzano nell'art. 12, il quale stabilisce che la principale attribuzione del Consiglio è quella di promuovere l'effettiva e coerente applicazione della Proposta di Regolamento e, in particolare, (tra le diverse funzioni):
supportare e consigliare la Commissione nella corretta e coerente applicazione della Proposta di Regolamento con le altre fonti del diritto;
promuovere la cooperazione e l'effettivo scambio di informazioni, esperienze, *best practices* e standard tecnici tra le diverse autorità regolatorie nazionali;
fornire pareri su questioni tecniche e fattuali connesse all'implementazione del mercato interno dei servizi multimediali, al pluralismo dei media e all'indipendenza delle scelte editoriali, su richiesta della Commissione e delle autorità regolatorie nazionali;
coordinare le misure regolatorie nazionali con riferimento all'accesso ai contenuti resi disponibili dai *media service providers* stabiliti fuori dall'Unione, laddove questi possano costituire seri e gravi pregiudizi per la difesa e la sicurezza pubblica;
favorire un dialogo strutturato tra i *providers* delle piattaforme digitali più grandi, tra i rappresentanti dei fornitori dei servizi multimediali e la società civile.
Se il Consiglio fosse un organo effettivamente indipendente, come espresso nell'art. 9, allora sarebbe controintuitivo inserire tra le sue funzioni e attività un continuo riferimento alla Commissione; non è accettabile che certe autorità nazionali, che sono pienamente autonome in patria, siano soggette "alla direzione e coordinamento" di un'istituzione sovranazionale[112].
Da un punto di vista più strettamente operativo, gli artt. 13 e successivi regolano i principi e le modalità attraverso i quali si dovrà realizzare la cooperazione tra le diverse autorità nazionali. Infatti, «un'autorità di regolamentazione nazionale può richiedere

[110] European Regulators Group for Audiovisual Media Services, *European Media Freedom Act (EMFA), ERGA position paper for the Open Public Consultation*, in *erga-online.eu.*

[111] European Regulators Group for Audiovisual Media Services, *Proposal of the Commission for a European Media Freedom Act (EMFA)*, in *erga-online.eu,* 5 novembre 2022.

[112] *Ibid.*

in qualsiasi momento la cooperazione o l'assistenza reciproca da parte di una o più autorità o organismo di regolamentazione nazionale ai fini dello scambio di informazioni o dell'adozione di misure proprie per la coerenza e l'applicazione del presente regolamento». L'autorità nazionale che riceve la richiesta non può esimersi dal dare corso alla stessa, salvo il caso in cui non sia competente o la sua esecuzione violerebbe il regolamento (in ogni caso, è richiesta un'adeguata motivazione).
Più nello specifico l'art. 16 statuisce che il Board coordina le misure adottate, anche dalle autorità nazionali, nei confronti dei fornitori di servizi multimediali stabiliti in un paese terzo, laddove «tali servizi di media pregiudichino o presentino un rischio serio e grave di pregiudicare la sicurezza pubblica e la difesa». La formulazione di tale norma risulta, però, essere eccessivamente generica, poiché potrebbe condurre alla circostanza di coinvolgere il Board per ogni decisione assunta da ciascuna autorità nazionale. Inoltre, la denunciata vaghezza può essere riscontrata anche nelle espressioni "rischio serio" e "pregiudicare la sicurezza pubblica e la difesa", che potrebbe condurre alla circostanza di limitare inopinatamente l'attività di taluni media, laddove tale possibilità dovrebbe essere riservata esclusivamente ai casi strettamente necessari. Infine, la pretesa di poter applicare lo stesso strumento regolatorio a tutti gli strumenti informativi, nonostante l'estrema eterogeneità interna a questa categoria, non consente di prevedere delle soluzioni concrete e specifiche alle diverse fattispecie: è evidente che verso un emittente televisivo via satellite stabilito in un paese terzo non possono essere adottate le stesse misure che sono utilizzate verso una piccola piattaforma informativa online. Sarebbe, pertanto, opportuno far sì che gli Stati Membri dotino le autorità nazionali delle necessarie competenze per irrogare sanzioni nei confronti di tali enti e, ai fini di assicurare l'uniformità del diritto, si adoperino al fine di individuare criteri comuni di valutazione[113].

9.4. L'implementazione del dialogo con le piattaforme più grandi (cd. *very large online platforms, VLOPs*)

Ai sensi dell'art. 17 della Proposta di Regolamento, le piattaforme digitali più grandi[114] devono rendere una dichiarazione nella quale, oltre ad affermare la sussistenza delle caratteristiche e dei requisiti di cui all'art. 2, attestano di essere editorialmente indipendenti da qualsiasi Stato (sia membro che terzo all'Unione europea) e di operare conformemente ai meccanismi co-regolatori ed auto-regolatori. Sempre ai fini di trasparenza, esse sono tenute, su base annuale, a rendere pubblico il numero delle circostanze nelle quali hanno imposto una qualche forma di restrizione o sospensione sulle proprie piattaforme a danno dei contenuti proposti dai fornitori di servizi multimediali ed a illustrare le ragioni sulla base delle quali hanno imposto tali restrizioni. Si vuole, dunque, instaurare un dialogo stabile tra i fornitori delle piattaforme più grandi, i rappresentanti dei servizi informativi e i rappresentanti della società civile, sotto gli auspici del Board. Le principali preoccupazioni dell'ERGA riguardo a tale disposizione hanno ad oggetto

[113] *Ibid.*

[114] In maniera complementare con quanto stabilito dal DSA.

l'asserita discrezionalità di cui tali VLOPs godrebbero nella valutazione di integrità ed affidabilità del fornitore di servizi informativi e l'opportunità di estendere l'ambito di applicazione di tali norme anche ai principali motori di ricerca informativi (ad esempio, Google News), e a piattaforme che localmente sono di primario rilievo, prevedendo delle soglie di utenti in rapporto alla popolazione totale di quel Paese. Inoltre, il principale *vulnus* deve essere ritrovato nell'assenza di una regolamentazione in caso di violazione da parte delle VLOPs degli obblighi[115] ivi previsti[116].
Inoltre, l'art. 19 statuisce il diritto per gli utenti di modificare facilmente le impostazioni di *default* dei propri *device* che monitorano gli accessi alla piattaforma e personalizzano sulla base degli interessi e delle preferenze l'offerta di media audiovisivi. Anche in questo caso, risulterebbe opportuno una chiarificazione di cosa si intenda per "impostazioni di default"[117].

9.5. Le regole per il corretto funzionamento del mercato interno dei media

L'art. 20 dispone che ogni intervento adottato da uno Stato membro con riferimento al mercato interno dei media deve essere proporzionato e adeguatamente giustificato, nonché definito in tempi certi. Inoltre, si prevede la possibilità per i fornitori di servizi multimediali di proporre appello contro ogni nuova previsione regolamentare, dinnanzi ad un organo indipendente, fermo restando i rimedi giurisdizionali previsti dalla legge.
L'art. 21 consente agli Stati membri di inserire nei propri ordinamenti norme sostanziali e procedurali che definiscano i criteri di apprezzamento delle concentrazioni nel mercato dei media. Dette norme devono essere trasparenti, oggettive, proporzionate e non discriminatorie e possono:
prevedere obblighi di notifica per gli operatori che costituiscono concentrazioni nel mercato dei media;
incaricare le autorità regolatorie nazionali della valutazione delle concentrazioni e dell'indipendenza dei media, previa determinazione di criteri oggettivi, non discriminatori e proporzionati.
Anche in queste due norme sarebbe opportuno meglio definire alcuni aspetti, al fine di garantire la certezza del diritto ed il corretto funzionamento del sistema ipotizzato dalla Proposta di EMFA. Ad esempio, sarebbe conveniente prevedere delle soglie quantitative al di sopra delle quali si attiverebbe l'art. 21, c. 1, oppure meglio regolamentare le circostanze in cui sia possibile un dialogo tra l'autorità nazionale e il Board, al fine di evitare che questa possa divenire una prassi, con la conseguenza di intasare il sistema,

[115] A tale riguardo, in un'ottica di cooperazione e trasparenza, potrebbe apparire opportuno che le VLOPs forniscano al Board, su sua giustificata richiesta, le informazioni e i dati derivanti dai monitoraggi realizzati ai fini delle norme in commento. (European Regulators Group for Audiovisual Media Services, *Proposal of the Commission for a European Media Freedom Act (EMFA)*, in *erga-online.eu*, novembre 2022, 9).

[116] *Ibid.*

[117] *Ibid.*

a discapito dell'effettività dell'attività di controllo[118].
In ultimo, ai sensi dell'art. 22 della Proposta di Regolamento, il Board esercita una funzione sussidiaria nell'apprezzamento del pluralismo esistente nel mercato dei media e nella valutazione di indipendenza degli stessi per mezzo dell'emissione di pareri. Sarebbe utile chiarire che tali pareri possano essere resi, anche senza una preventiva richiesta da parte della Commissione e, al contrario, il Board non sarebbe obbligato a renderli, laddove, pur in costanza di una richiesta della Commissione, non ne ravvisasse la necessità. Infatti, la valutazione del rischio di una determinata operazione di concentrazione per il pluralismo o l'indipendenza dovrebbe essere effettuata da organismi di regolamentazione indipendenti[119].

9.6. La pubblicità di stato

L'art. 24 dispone che le somme di denaro elargite dagli stati (o altre autorità pubbliche) in favore di fornitori di servizi informativi a fini pubblicitari siano assegnate secondo criteri trasparenti, oggettivi, proporzionati e non discriminatori e attraverso procedure aperte. In questo senso, devono essere resi noti i nomi di tali fornitori, nonché l'ammontare annuo speso per tale attività, distinto per ciascun fornitore. Le autorità di regolamentazione nazionale monitorano la corretta allocazione delle risorse e l'osservanza di tali obblighi. È evidente come tale ulteriore attività possa costituire un grosso aggravio, sarebbe auspicabile non solo chiarire che tipologia di analisi è richiesta, ma anche restringere l'ambito di applicazione dell'ampia definizione di "pubblicità di stato"[120].

10. Conclusione

L'emergere di un ruolo dominante delle piattaforme digitali nella distribuzione delle notizie ai cittadini europei, insieme con l'affacciarsi di nuove sfide connesse ad un'informazione poco professionale ed un progressivo perimento dei sistemi informativi nella parte orientale dell'Unione ha indotto il legislatore europeo a porre in atto delle azioni concrete a tutela del pluralismo informativo e la libertà dei media. Si tratta di principi affermati e tutelati sia dalla Carta di Nizza, sia dai Trattati fondanti dell'Unione, sia da molte costituzioni nazionali (ad esempio, art. 21 Cost.).
Dopo aver analizzato il nuovo e predominante ruolo che deve essere riconosciuto al pluralismo informativo in rete e avere considerato l'esperienza d'oltreoceano per evidenziare il differente approccio regolatorio, si è indugiato su un'analisi dello stato dell'arte, dalla quale è emersa l'impossibilità/incapacità di regolare adeguatamente il fenomeno sfruttando, in via incidentale, i più recenti regolamenti entrati in vigore (DSA, DMA) e le altre fonti efficaci già da qualche anno (AVMSD).

118 Ivi, 11

119 *Ibid.*

120 Ivi,12.

Il regolatore europeo ha, quindi, dovuto affrontare l'importante sfida di trovare la propria legittimazione a regolare un fenomeno così delicato e intrinsecamente connesso con i valori costituzionali di ogni Stato Membro; a questo fine, ha sfruttato la base regolatoria su cui ha la più solida competenza: l'adozione di misure relative al ravvicinamento delle disposizioni legislative per il corretto funzionamento del mercato interno. Tutto ciò costituisce la base per un'innovativa proposta di regolamento: l'*European Media Freedom Act*. Nonostante le limitate osservazioni mosse dall'ERGA concernenti l'opportunità di meglio definire alcuni concetti e riconoscere maggiore autonomia al cd. Board, la Proposta presenta un modello regolatorio ben ponderato, che offre una tutela orizzontale verso tutte quelle azioni che potrebbero minare la libertà di tutti i media. La principale forza è costituita dall'uniformità regolatoria offerta da tale Proposta di Regolamento: è fondamentale, che tutti gli Stati Membri condividano una stessa base regolatoria dei servizi informativi, al fine di abbattere le barriere interne al mercato comune e di evitare derive antidemocratiche. Assume particolare centralità il ruolo assegnato all'autorità regolatoria europea e alle autorità nazionali per la vigilanza e l'implementazione di misure volte a tutelare il pluralismo e l'indipendenza dei media. In questo modo, il legislatore stabilisce anche un *framework* comune per la sorveglianza (e l'eventuale intervento) sulle procedure interne messe in atto da alcune piattaforme (ad esempio, *Facebook Oversight Board*). Si estendono, dunque, i diritti degli utenti che possono "indirizzare" l'algoritmo verso il pluralismo informativo.

In conclusione, è possibile ritenere che il digitale – nella sua accezione connessa all'ambito informativo – sebbene presenti importanti novità e grandi sfide per il costituzionalista, sia riconducibile all'interno dei "vecchi" schemi concettuali dello Stato di diritto, sottoponendolo – per mezzo di adeguate norme di rango primario – alle regole di garanzia delle nostre libertà.

A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)*

Chiara Gallese

Abstract

The essay aims at examining the proposal for a new Regulation on fair access and use of data (Data Act), recently published by the European Commission. It examines the new legal framework in light of the European digital strategy, in particular the Strategy for Data, and describing how the proposal was conceived and inserted in the historical context. It also explores the newly introduced definitions, the scope of application, and the subjects of the proposal, identifying the most important legislative novelties and their consequences on different stakeholders. Lastly, it analyzes the normative gaps and the limitations of the current draft of the act.

Summary

1. Introduction – 2. The European Digital Strategy and the background of the proposal – 3. Scope of application, definitions, and subjects of the Data Act – 4. Data accessibility by design and by default and the right of access – 5. Data Portability, Fairness, Reasonableness, and Non-discrimination – 6. Making data available in case of exceptional need – 7. Transparency – 8. Regulating Smart Contracts – 9. Provision regarding Data Processing Services – 10. Provisions regarding unilaterally imposed unfair clauses – 11. Conclusion

Keywords

Data Act - European Digital Strategy - Digital Regulation - Data Access - Data Processing Services

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco". Funded by the REMIDE project, Carlo Cattaneo University - LIUC and by the UNI 4 JUSTICE Project

1. Introduction

The essay aims at examining the recent proposal for a new Regulation on fair access and use of data (Data Act), published by the European Commission on the 24th of February 2022. The proposal creates a new legal framework for the access and use of data, as depicted in Figure 1.

Firstly, we will focus on the European digital strategy, in particular the Strategy for Data, and on how the new proposal was conceived and inserted in the historical context. Secondly, we will explore the relevant definitions, scope of application, and subjects involved in the new legal framework. Thirdly, we will proceed to identify the most important legislative novelties introduced by the proposal and their consequences on different stakeholders. Lastly, we will examine the normative gaps left out of the proposal and the limitations of the current draft. Enacting this law will create new challenges and legal issues: to what legal cases will it be applicable? Who are the subjects that will be affected the most? What will be the consequences of the new legal framework? How is it harmonized with the existing legislation? What aspects is it failing to address?

We will answer these questions by analyzing the current text of the proposal, including the explanatory memorandum and the recitals, the related legislation (such as GDPR, which is complemented by this act), and the European Commission's working documents. We will also consider the current trends of the IoT market and the most common commercial practices in this field.

The analysis of the Data Act cannot be carried out only from a legal perspective, but business and technical point of views need to be taken into consideration as well, due to the fact that the object of the proposal is related to data generated by IoT devices, cloud computing and smart contacts are regulated, and interoperability requirements are a key element of the new legal framework.

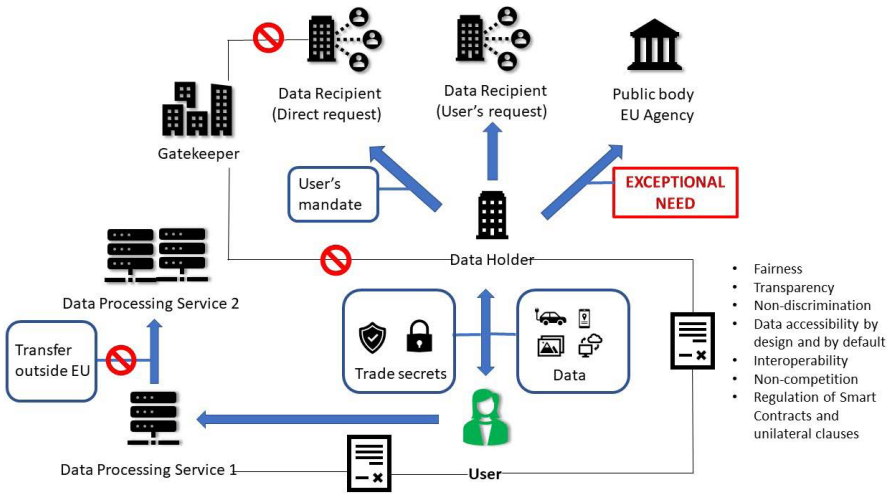


Figure 1: The framework of the Data Act

2. The European Digital Strategy and the background of the proposal

The proposal came into life as part of a broader European Digital Strategy regarding the movement of data in Europe. The interest of the EU in data, both from a perspective of protecting personal data and enhancing and harmonizing the sharing of data within the Union, began right after the Maastricht Treaty. As early as the 1995, the Database directive[1] was enacted, followed by the Data Protection Directive[2] the same year.

In 1997, with the development of the internet and the digital market, the EU started to regulate data protection in the telecommunications sector[3], and, in 2000, the field of electronic commerce[4]. 2002 has been a prolific year for the regulator, as five directives building the regulatory framework for electronic communications networks and services, together referred to as "the Framework Directive and the Specific Directives", were enacted[5].

In 2003, the Directive on the re-use of public sector information[6], now replaced by the Open Data Directive[7], was then enacted, following the desire of the European Commission to develop the potential of public sector data since the end of the 1980s[8].

In order to monitor the adoption, development and impact of electronic business practices, the European Commission launched the "e-Business W@tch" project in 2001. The project highlighted the need to create a suitable environment for companies

[1] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

[2] Directive 95/46/EC, now replaced by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).

[3] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, replaced, in 2002, by the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[4] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[5] That is Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), Directive 2002/21/EC of the European Parliament and the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), Directive 2002/22/EC (Universal Service Directive), and the above mentioned Directive on privacy and electronic communications. They were regularly updated in the light of technological and market developments, e.g., by Directive 2006/24/EC and by Directive 2009/136/EC, but also sometimes temporarily derogated, e.g., by Regulation (EU) 2021/1232.

[6] Directive 2003/98/EC on the re-use of public sector information, known as the PSI Directive.

[7] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

[8] K. Janssen, *The influence of the PSI directive on open government data: An overview of recent developments*, in *Government Information Quarterly*, 28(4), 2011, 446 ss.

within the EU in order to ensure they are able to compete at a global level, including «cutting 'red tape', fostering innovation and – more specifically with regard to ICT – counteracting shortages in e-skills and promoting systems inter-operability»[9], as a response to the issues created by globalization and a growing international competition. These action points were included in the 2005 Action Plan and a new industrial policy was launched by the Commission in the same year.

In 2010, the Digital Agenda for Europe was announced as one of the seven flagship initiatives of the Europe 2020 Strategy. The aim was to create a digital single market, taking into consideration the need for interoperability[10], to tackle the fact that the EU was «falling behind in markets such as media services, both in terms of what consumers can access, and in terms of business models that can create jobs in Europe. Most of the recent successful internet businesses (such as Google, eBay, Amazon and Facebook) originate outside of Europe»[11].The European Commission was starting to wake up about the growing power of foreign giants, and since then it has finally being working to keep pace with international competitors. To enhance the digital market, the e-money Directive was created[12]. Key Directives supporting the digital single market, such as the Services Directive, Unfair Commercial Practices Directive, the Telecoms Framework, the e-Commerce Directive, the eSignature Directive, and the VAT Directive, contributed to the Digital Agenda.

In 2011, a comprehensive open data package was presented by the European Commission, following the route of the PSI Directive and working towards making available its documents in machine-readable format. In 2012, the EU Open Data Portal was launched, to promote the accessibility and reuse of information. The EU endorsed the G8 Open Data Charter in 2013, and committed to implementing open data activities.

The economic and financial crisis of 2008, the increasing surges of migrants and refugees, and the terrorist attacks starting in 2015, however, posed new challenges for the EU. Better communication across the Union become not only a goal to promote the single market and competitiveness[13], boosting and modernizing the economy, but also a crucial factor in fighting traditional and cyber terrorism, and other criminal acts[14]. The Directorate-General for Communication Networks, Content and Technology noted in 2012 that «in today's technological environment, any structural change must necessarily include a strong dose of digitisation. Europe's companies cannot remain

[9] European Commission, *The European e-Business Report 2006/07 edition - A portrait of e-business in 10 sectors of the EU economy - 5th Synthesis Report of the e-Business W@tch*, 2007.

[10] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A Digital Agenda for Europe*, 2010; European Commission, *Digital agenda for Europe- Rebooting Europe's economy*, 2014.

[11] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A Digital Agenda for Europe.*

[12] Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institution.

[13] European Commission, *Digital agenda for Europe- Rebooting Europe's economy.*

[14] European Parliament, *A new Digital Agenda for Europe: 2015.eu European Parliament resolution of 5 May 2010 on a new Digital Agenda for Europe*, 2010.

competitive, nor can public services remain first-class, if they do not make extensive use of information and communication technology (ICT). Virtually all newly created jobs require good ICT skills, and so do most existing jobs, too. Promoting ICT is promoting a job-rich recovery»[15].

The 2012 e-commerce action plan was aimed at doubling the volume of e-commerce in Europe by 2015 by optimizing postal delivery, enhancing electronic and mobile payments, promoting online shopping, improving Internet security and implementing measures to fight cyberattacks[16]. In 2014, the European Commission had completed 72 of 101 actions in the context of the Digital Agenda[17] and promoted the use of high-speed broadband «by bringing forward new rules on cost reduction, a recommendation on next generation access networks, revised state aid guidelines for broadband and a proposal to complete the telecoms single market»[18]. In the same years, the Commission started the works for a revision of the personal data protection regulatory framework, that were aimed at enacting the General Data Protection Regulation and the the ePrivacy Regulation.

However, despite these regulatory efforts, during the 2005-2015 decade the EU has not been able to defend its digital sovereignty from foreign Big Techs, which managed to enact a series of anti-competitive and tax-elusive practices, and to exploit personal data of European citizens. As noted by Gueham, «The time has come for a digital offensive – while the European Union resigned itself to American hegemony for several years, it never promoted the rise of a national champion capable of taking on Google or Amazon on equal terms, as China did with Alibaba or Russia with Yandex. The penalties imposed by Brussels on Microsoft and Intel for abuse of a dominant position stick in people's minds. Since 2010, and particularly since the new Commission took office in 2014, Europe has defied US imperialism, a permanent slight to its sovereignty, especially since the Snowden scandal which placed the spotlight on the US administration's use of European citizens' data. However, initiatives against American giants are still too rare to inspire fear»[19] . These circumstanced led the European Commission to focus its energies in defending fundamental rights against powerful foreign actors. In 2016-2018, in fact, GDPR largely transformed the privacy framework and posed the basis for an efficient defense of EU citizens'.

The data protection legislation reform that was initiated with GDPR was expanded in 2016 with the Law Enforcement Directive[20], applied from 2018.

In the same year the Regulation regarding the processing of personal data by the Un-

[15] European Commission, *Digital Agenda for Europe Scoreboard 2012*, 2012.

[16] European Commission, *Digital agenda for Europe- Rebooting Europe's economy*, 2014.

[17] *Ibid.*

[18] *Ibid.*

[19] F. Gueham, *Digital sovereignty – steps towards a new system of internet governance*, in *fondapol.org*, 2017.

[20] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

ion institutions[21], together with the Regulation regarding non-personal data[22], was enforced. This was the first seed that lead to the Data Act and the beginning of a novel regulatory effort aimed at enhancing the EU Digital Strategy.

In 2020, in fact, three other proposals were published: the proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act), the proposal for a Regulation on a Single Market for Digital Services (Digital Services Act)[23] and amending Directive 2000/31/EC, and the proposal for a Regulation on European data governance (Data Governance Act), which the Data Act complements.

Finally, in 2021, the proposal for a Regulation on Artificial Intelligence (AI Act) was published, providing strict rules regarding data sets employed in developing high-risk AI models.

The need for such an extensive regulatory framework has arisen since the volume of data produced in the world has increased from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025[24]. The EU aims at becoming a leading role model by building «on a strong legal framework – in terms of data protection, fundamental rights, safety and cybersecurity – and its internal market with competitive companies of all sizes and varied industrial base»[25] .

In light of the above, it must be noted that big data is a crucial concept in the current era: processing such a large, complex and diverse amount of information enables data analysts to make accurate predictions in many areas and business sectors, such as health care, finance, marketing, and even environment, tackling major challenges, e.g., the climate change, as well as having a better understanding of social phenomena. It is also extremely important in the context of Artificial Intelligence, since machine learning models need a large amount of data to be trained[26]. It can be said, then, that a large part of the technological progress depends on the availability of data.

Having access to data is thus a powerful way to gain a business advantage over competitors. Because only large platforms now have access to a significant amount of data, there is a situation of oligopoly, in which the larger actors gain control over big data, and by analyzing it they are able to create more services and gain even more data, in a vicious circle. The European Commission pointed out that «The high degree of market power resulting from the 'data advantage' can enable large players to set the rules on the platform and unilaterally impose conditions for access and use of data

[21] Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

[22] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

[23] G. De Minico, *Fundamental rights, European digital regulation and algorithmic challenge*, in *Rivista di diritto dei media*, 1, 2021, 9 ss.

[24] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European Strategy For Data*, 2020.

[25] *Ibid.*

[26] Regarding the use of data to train AI models, the new proposal for a Regulation on Artificial Intelligence (AI Act) has drawn a new framework with the aim of removing biases in data sets whenever the system is considered as "high risk".

or, indeed, allow leveraging of such 'power advantage' when developing new services and expanding towards new markets. Imbalances may also arise in other situations, such as with regard to access to co-generated IoT data from industrial and consumer devices»[27].

Of all this data, a research from International Data Corporation (IDC 2019) has estimated that a large part (79.4 zettabytes) will be generated by connected devices (IoT) by 2025. Those devices will then become more and more important in the data economy. However, because the data generated by them are hosted in proprietary platforms and cloud solutions, only the producers have access to that information. The proposal of the Data Act aims at changing this situation by giving control back to users, who are the subjects of the data generating process, by rebalancing the contractual power for SMEs through the provision of fair clauses in data sharing contracts, and by allowing public sector bodies to access and use data held by private companies in exceptional circumstances.

The background of the new regulation is well explained in Recital 1 and 2, which explain that, while the digitization of economy is growing and electronic data are valuable elements of new technologies[28], data processing activities are hindered by data localization requirements and lock-in practices[29]. To exploit the data value chains of IoT systems and to cope with new legal issues[30], a legislative intervention has been necessary.

In addition, the Data Act reviews part of the Database Directive, in order to prevent the copyright protection of IoT data which could be used as an excuse to limit the right of access: «In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to

[27] European Commission, *Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - A European Strategy For Data*, cit.

[28] Recital 1: «The digitisation of the economy is accelerating. Information and Communications Technology is no longer a specific sector, but the foundation of all modern innovative economic systems and societies. Electronic data are at the centre of those systems and can generate great value when analysed or combined with services and products».

[29] Recital 2: «Data value chains are built on different data activities: data creation and collection; data aggregation and organisation; data processing; data analysis, marketing and distribution; use and re-use of data. The effective and efficient functioning of data processing is a fundamental building block in any data value chain. However, the effective and efficient functioning of data processing, and the development of the data economy in the Union, are hampered, in particular, by two types of obstacles to data mobility and to the internal market: data localisation requirements put in place by Member States' authorities and vendor lock-in practices in the private sector».

[30] As noted by the second part of Recital 1: «At the same time, the rapid development of the data economy and emerging technologies such as Artificial Intelligence, Internet of Things products and services, autonomous systems, and 5G are raising novel legal issues surrounding questions of access to and reuse of data, liability, ethics and solidarity. Work should be considered on the issue of liability, in particular through the implementation of selfregulatory codes and other best practices, taking into account recommendations, decisions and actions taken without human interaction along the entire value chain of data processing. Such work might also include appropriate mechanisms for determining liability, for transferring responsibility among cooperating services, for insurance and for auditing».

databases containing data obtained from or generated by the use of a product or a related service».

3. Scope of application, definitions, and subjects of the Data Act

Article 1 of the proposal defines its scope of application and subject matter: it is aimed at harmonizing the rules about data generated by the use of "a product or related service", in order to make it available from "data holders" to:
the User (natural or legal person who generates the data);
Data Recipients (natural or legal person who receives the data in the context of their business or professional activity);
public sector bodies or Union institutions, agencies or bodies, in case of exceptional need and for the performance of a task carried out in the public interest.
The definition of the term "data"[31] is borrowed from the Data Governance Act: «Any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording». Although it is rather broad, its relevance is specified by the definition of "product", i.e. «a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data» and by that of "related service", that is a «digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions».
In this context, it is clear that the proposal intends to restrict the definition to data generated by all connected devices[32], including robots, with the exception of those devices that have a mere accessory function (such as hard drives, dock stations, decoders, modems, WiFi bridges, etc.). Interestingly, Recital 15 excludes some of the most common IoT devices: «Certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners. They require human input to produce var-

[31] While the OECD defines it as «data can be described as the unordered and unprocessed representation of any types of observations that are quantified and stored in symbols» in *Introduction to Data and Analytics (Module 1): Taxonomy, Data Governance Issues, and Implications for further Work*, OECD 2013.

[32] Recital 14 makes reference to IoT devices: «Physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things) should be covered by this Regulation. Electronic communications services include land-based telephone networks, television cable networks, satellite-based networks and near-field communication networks. Such products may include vehicles, home equipment and consumer goods, medical and health devices or agricultural and industrial machinery».

ious forms of content, such as text documents, sound files, video files, games, digital maps». The exclusion of smart phones, tablets, notebooks, and cameras, which are known to generate a large amount of data and metadata of great value, significantly reduces the scope of this proposal. For example, smart phones are commonly used as tools for delivering tele-health services[33], to control other IoT devices,[34] etc. Modern smarthpones are not just telephones anymore, they can become specific devices through mobile apps (e.g., controlling heating, lighting, and doors of the house). In many cases, there is little difference between a smartphone and a different IoT device, therefore this exclusion seems incongruous.

On the other hand, the definition is to some degree extended by the inclusion of data generated by digital services, such as proprietary software running in IoT devices. It is unclear, however, what software is exactly included in the definition of "digital service". The article specifies that a piece of software is included if «its absence would prevent the product from performing one of its functions», but it does not define what is a "function". For example, are third-parties proprietary apps such as Google Maps, installed on smart devices, included? One of the function of modern IoT devices (e.g., smart watches) is to enable their owner to navigate on the web, use social media, send messages, make calls through internet, take pictures, etc. Some of them have built-in and pre-installed apps, which cannot be uninstalled by the User.

Article 7[35] further extend the concept to "virtual assistants", defined as «software that can process demands, tasks or questions including based on audio, written input, gestures or motions, and based on those demands, tasks or questions provides access their own and third party services or control their own and third party devices». The reference is clearly to popular systems such as Siri, Alexa, and Google Assistant, which are used by millions of people worldwide, for example to search for information, control smart devices in the house, listen to music, do shopping, etc.[36]

Recital 22 contains an explanation about the scope of the Regulation regarding virtual assistants and it also gives a hint about the relevance of apps: «Virtual assistants play an increasing role in digitising consumer environments and serve as an easy-to-use interface to play content, obtain information, or activate physical objects connected to the Internet of Things. Virtual assistants can act as a single gateway in, for example, a smart home environment and record significant amounts of relevant data on how users interact with products connected to the Internet of Things, including those manufactured by other parties and can replace the use of manufacturer-provided in-

[33] S. D. Burdette – T. E. Herchline – R. Oehler, *Practicing medicine in a technological age: using smartphones in clinical practice*, in *Clinical infectious diseases*, 47(1), 2008, 117 ss.; D.C. Baumgart, *Smartphones in clinical practice, medical education, and research*, in *Archives of internal medicine*, 171(14), 2011, 1294 ss.; W. J. Gordon et al., *Beyond validation: getting health apps into clinical practice*, in *NPJ digital medicine*, 3(1), 2020, 1 ss.

[34] X. Mao et al., *Design and implementation of a new smart home control system based on internet of things*,. in *2017 international smart cities conference (ISC2)*, IEEE, 2017, 1 ss.

[35] «Where this Regulation refers to products or related services, such reference shall also be understood to include virtual assistants, insofar as they are used to access or control a product or related service».

[36] M. B. Hoy, *Alexa, Siri, Cortana, and more: an introduction to voice assistants*, in *Medical reference services quarterly*, 37(1), 2018, 81 ss.; I. Lopatovska et al., *Talk to me: Exploring user interactions with the Amazon Alexa*, in *Journal of Librarianship and Information Science*, 51(4), 2019, 984 ss.

terfaces such as touchscreens or smart phone apps. The user may wish to make available such data with third party manufacturers and enable novel smart home services. Such virtual assistants should be covered by the data access right provided for in this Regulation also regarding data recorded before the virtual assistant's activation by the wake word and data generated when a user interacts with a product via a virtual assistant provided by an entity other than the manufacturer of the product. However, only the data stemming from the interaction between the user and product through the virtual assistant falls within the scope of this Regulation. Data produced by the virtual assistant unrelated to the use of a product is not the object of this Regulation». Data gathered from apps seems thus included in the scope of the regulation insofar they are related to the interaction between the User and the product.

In addition, Recital 16 makes reference to software as a service (SaS), including in the scope also third-party services which are part of the original contract: «Such related services can be part of the sale, rent or lease agreement, or such services are normally provided for products of the same type and the user could reasonably expect them to be provided given the nature of the product and taking into account any public statement made by or on behalf of the seller, renter, lessor or other persons in previous links of the chain of transactions, including the manufacturer. These related services may themselves generate data of value to the user independently of the data collection capabilities of the product with which they are interconnected. This Regulation should also apply to a related service that is not supplied by the seller, renter or lessor itself, but is supplied, under the sales, rental or lease contract, by a third party. In the event of doubt as to whether the supply of service forms part of the sale, rent or lease contract, this Regulation should apply». Therefore, third-parties apps may be included in the definition of "related services", although it seems that not all data generated by those apps are subject to the Data Act.

In fact, Recital 17 clarifies that Users' recordings that were made on purpose are within the scope of the Regulation, together with data generated by Users' actions: «Data generated by the use of a product or related service include data recorded intentionally by the user. Such data include also data generated as a by-product of the user's action, such as diagnostics data, and without any action by the user, such as when the product is in 'standby mode', and data recorded during periods when the product is switched off. Such data should include data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights», while Recital 14 excludes the results of data analysis from the scope of the proposal[37].

[37] «The data represent the digitalisation of user actions and events and should accordingly be accessible to the user, while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation».

3.1 Subjects of the proposal

After defining the relevant terms, the subjects to whom the proposal is aimed are identified:

- manufacturers of products and suppliers of related services and their users in the European market;
- Data Holders that make data available to Data Recipients located in the Union, and to public sector bodies and Union institutions, agencies or bodies;
- Data Recipients located in the Union;
- Data Holders that provide data in cases of exceptional need;
- Providers of Data Processing Services (DPS) targeting customers in the Union.

The focus of the proposal is to extend the legal protection to all products that are available to European consumers, regardless of the subject who is putting them into the market. In this way, foreign companies targeting EU customers need to comply as well.

However, Article 7 restrict the scope of the proposal to medium and big enterprises, explicitly excluding micro and small enterprises[38], provided that they are not partnered or linked to larger enterprises[39]. This provision intends to avoid to impose additional burdens to companies that have lesser means to comply, while at the same time preventing bigger companies to circumvent the regulation by establishing smaller new branches or controlled entities.

Three subjects are introduced by this provision, namely the "Data Holder", the "Data Recipient", and the "User". The first one can be considered the equivalent of the "Data Controller" in GDPR, while the last one is correspondent to the "Data Subject", although it is not restricted to natural person, but it includes legal persons as well. The Data Recipient, which is sometimes referred to as "Third Party", on the other hand, corresponds to the "Third Party" concept in GDPR (including Data Processors).

3.2 Relationship with GDPR

The concept of data is not restricted to non-personal data, although personal data are already covered by GDPR, which prevails over the provisions of the Data Act[40].

The novelty of this proposal is that it covers also *anonymized data*, that is, information that was originally classified as personal data, but then put through a number of technical operations to remove the elements that could lead back to identification of the data subject. In doing so, the legislator intends to regulate and curb the habit of large

[38] As defined in Article 2 of the Annex to Recommendation 2003/361/EC: less than 50 employees and a turnover and/or balance sheet that does not exceed 10 million EUR.

[39] Also as defined in Article 3 of the Annex to Recommendation 2003/361/EC.

[40] In fact, the regulation itself reminds multiple times that GDPR should be respected: «Where the user is not a data subject, any personal data generated by the use of a product or related service shall only be made available where there is a valid legal basis under Article 6(1) of Regulation (EU) 2016/679 and where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 are fulfilled».

companies to take advantage of users' personal data by claiming that they were "fully anonymized"[41] and thus not subject to GDPR obligations, such as the right of access and right to portability.

Personal data protection interrelates with the Data Act when Users' data are personal data or the data set is mixed (personal and non personal data). In fact, in this case Data Holders are also Data Controllers and Users are Data Subjects (see Recital 24), and all GDPR provisions must be respected (see Recital 30), including the rights of access and portability. This proposal confer to Data Subjects the right to receive not only their personal data, but also non personal ones.

The data portability right is, in fact, expanded by the proposal, providing that data generated by the use of a product or related service can be made available to a third party at the request of the user.

While Article 20 provides for a right of Data Subjects to receive the personal data they provided to the Data Controller «in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided», when the legal basis for the processing is consent or a contract and it is carried out by automated means. According to the same article, in addition, Data Subjects have the right to «have the personal data transmitted directly from one controller to another, where technically feasible» This right does not apply to «processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller».

Recital 31 notes that «Article 20 specifies that it pertains to data provided by the data subject but does not specify whether this necessitates active behaviour on the side of the data subject or whether it also applies to situations where a product or related service by its design observes the behaviour of a data subject or other information in relation to a data subject in a passive manner». The wording of the article is not dirimment at this regard, but it seems to suggest at least the will to share the data.

Recital 31 further specifies that the Data Act intends to complement the right to portability, but in a broader way, as it «grants users the right to access and make available to a third party to any data generated by the use of a product or related service, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing. Unlike the technical obligations provided for in Article 20 of Regulation (EU) 2016/679, this Regulation mandates and ensures the technical feasibility of third party access for all types of data coming within its scope, whether personal or non-personal. It also allows the data holder to set reasonable compensation to be met by third parties, but not by the user, for any cost incurred in providing direct access to the data generated by the user's product. If a data holder and third party are unable to agree terms for such direct access, the data subject should be in no way prevented from exercising the rights contained in Regulation (EU) 2016/679». Therefore, it is explained that the right enshrined in GDPR prevails over that contained in the Data Act.

[41] Very often, the process of anonymization is not even carried out according to the Working Party 29's Opinion on Anonymization Techniques of 2014.

Users may also be Data Controllers themselves, for example in the case of IoT devices used by employees of a company. By filing a data access request, the company may acquire its employees' (or a different person's) personal data, becoming a Controller. When Users assume the role of Controllers, they must have a valid legal basis according to GDPR for requesting personal data generated by the use of a product or related service. For example, in case of a company wanting to get access to their employees data, a legitimate interest might be present. Clearly, in this case the User-Controller must ensure that the Data Subjects concerned are informed pursuant to Article 14 of GDPR.

It might also happen that the Data Holder and the User are qualified as Joint Controllers, pursuant to Article 26 of GDPR. In this case, a contractual agreement is needed to determine their respective responsibilities, in particular as regards the exercising of the rights of the data subject and in providing the privacy notices according to Articles 13 and 14.

As highlighted by Recital 30, once data has been made available, the User might as well become a Data Holder, thus acquiring the obligations to make data available under the Data Act.

4. Data accessibility by design and by default and the right of access

Article 3 introduces for the first time a principle of "data accessibility by design and by default", meaning that systems need to be designed and set in such a way that Users can easily - and, if possible, directly - have access to the information generated by the device[42]. The provision is complementing the right of access enshrined in GDPR.

The main novelty of the regulation is in fact the provision of the right of access to users' data, contained in the first paragraph of Article 4: «Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible».

[42] In fact, the Article states the following: «Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user», and recital 20 further specifies that «In case several persons or entities own a product or are party to a lease or rent agreement and benefit from access to a related service, reasonable efforts should be made in the design of the product or related service or the relevant interface so that all persons can have access to data they generate. Users of products that generate data typically require a user account to be set up. This allows for identification of the user by the manufacturer as well as a means to communicate to exercise and process data access requests. Manufacturers or designers of a product that is typically used by several persons should put in place the necessary mechanism that allow separate user accounts for individual persons, where relevant, or the possibility for several persons to use the same user account. Access should be granted to the user upon simple request mechanisms granting automatic execution, not requiring examination or clearance by the manufacturer or data holder. This means that data should only be made available when the user actually wants this. Where automated execution of the data access request is not possible, for instance, via a user account or accompanying mobile application provided with the product or service, the manufacturer should inform the user how the data may be accessed».

The key concept of this provision is that all data generated by an IoT system, which is not already in the control of the User, can now be accessed by the same User at no cost and without undue delay. This means that, whenever the data generated by the system is not under the direct control of the User and it is not possible to download it directly, the User has the right to receive a copy and is now able to process it independently from the Data Holder.

Some example of data that can be requested are, for example, travel routes, gasoline consumption, speed fluctuation, breaking and accelerating frequency, travel time and frequency, tire pressure, motor oil level and consumption, maintenance frequency, regarding a connected car; time of switching on and off, duration, frequency of usage, and intensity levels of a smart light bulb; usage, charge and status of battery, time of switching on and off and connection to the internet, maintenance data, related to smart glasses.

The proposal puts an accent on the benefits of this provision for individuals and companies, especially because of the fact that it will allow them to switch to a different enterprise to perform maintenance activities. In fact, a common problem is that many IoT products (e.g., cars, industrial machinery) can be repaired and updated only by their producers or by authorized retailers, as the relevant data, that would allow to understand how the system works, is not disclosed by the manufacturer. Producers often hide under the "trade secret" excuse, claiming that disclosing maintenance data would imply sharing protected information. The proposal puts a full stop to this practice.

In fact, regarding trade secrets[43], the proposal prescribes at par. 3 of Article 4 a legitimate basis for the disclosure according to article 3, par 1, lett. d), of the Trade Secret Directive, but it imposes a condition to be fulfilled: it is possible to request the disclosure of trade secrets «provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties». Those measures can be agreed between the Data Holder and the User. However, par. 6 of Article 8 provides that this regulation does not impose an obligation to disclose such information [44]. Therefore, although producers are now obliged to share the relevant data, they can do it without disclosing trade secrets, and they cannot hide the data claiming that it constitutes a secret. As an additional reassurance for Data Holders, a non-compete provision has been inserted to prevent unfair use of data obtained thanks to this regulation, providing that «The user shall not use the data obtained pursuant to a request referred to in paragraph 1 to develop a product that competes with the product from which the data originate».

This provision is counterbalanced by paragraph 6, which set a symmetrical limit to the use of data generated by the User: «The data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user. The data holder shall not use such data generated by the

[43] The concept is defined by the Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Trade Secret Directive).

[44] «Unless otherwise provided by Union law, including Article 6 of this Regulation, or by national legislation implementing Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets within the meaning of Directive (EU) 2016/943».

use of the product or related service to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active».

On one hand, then, the User cannot exploit the data to become a competitor of the Data Holder, as this would be an unfair practice and the proposal intend to prevent the right of access to be used as an excuse to steal trade secrets and business information to gain a commercial advantage. On the other hand, paragraph 6 conversely makes sure that data generated by the User is regulated by a contract between the two parties, and prevents the Data Holder to exploit the User's data in an unfair way that would undermine the User's position in the market. This is also to prevent larger companies to exploit data obtained by SMEs.

The introduction of the right of access will have an impact on both large companies and SMEs, as well as on citizens. Natural persons will be able to have a better insight on data they generate, being able to analyze it and having a more complete picture of their IoT systems, for example by learning what profile has been built, what preferences are tracked by the Data Holder, enabling them to make informed choices regarding consent and device settings. They will also be able to transfer the data into different systems and to store them as they prefer. This will facilitate maintenance operations, as they will be able to provide to repair services all relevant information. The difference with the right of access pursuant to GDPR is that Users are now able to obtain also the information derived from personal data, which previously was excluded because it was classified as anonymized data, and which enables non-SME enterprises to sell data to advertisers without complying to GDPR.

SMEs will benefit even more from this provision, as they will be able to analyze their own data to perform gap analysis and improve their internal procedures and products (e.g., in the transportation industry, by improving management of trucks and travel route, monitoring compliance with road rules, improving shifts of drivers). According to McKinsey, through the analysis of IoT data for predictive maintenance, maintenance costs and equipment downtime can be significantly reduced, and in the factories setting, it is possible to achieve a «10 to 20 percent energy savings and a 10 to 25 percent potential improvement in labor efficiency»[45].

However, there are still some obstacles to the possibility of data exploitation. One is the fact that in some sectors there is an oligopoly of manufacturers, so that Users have difficulties in finding alternatives and their control over the data is limited[46]. To overcome part of this issue, the proposal tries to empower Users by giving a better control over their data and by providing non-competition obligation, preventing Data

[45] McKinsey Global Institute, *The Internet of Things: Mapping the value beyond the hype,* in *mckinsey.com*, June 2015.

[46] Recital 25 highlights this problem: «In sectors characterised by the concentration of a small number of manufacturers supplying end users, there are only limited options available to users with regard to sharing data with those manufacturers. In such circumstances, contractual agreements may be insufficient to achieve the objective of user empowerment. The data tends to remain under the control of the manufacturers, making it difficult for users to obtain value from the data generated by the equipment they purchase or lease. Consequently, there is limited potential for innovative smaller businesses to offer data-based solutions in a competitive manner and for a diverse data economy in Europe».

Holders to exploit the data to undermine the economic position of the User on the market[47]. Recital 25 also suggests to rely on sectoral legislation and Codes of Conduct[48], as its 2018 predecessor Regulation regarding Non-Personal Data[49].
Another issue is the fact that lock-in practices are still very common, and not every data is shared. Manufacturers often retain their data sets in proprietary format, so that it is impossible to port them in a different environment[50].
For this reason, the proposal introduced the right of Data Portability and some interoperability requirements, excluding micro and small enterprises by the envisaged obligations[51].

5. Data Portability, Fairness, Reasonableness, and Non-discrimination

Article 5 provides for the "Right to share data with third parties", that is, the Data Portability principle: «Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the

[47] Recital 25 reminds that « [...] the data holder should not use any data generated by the use of the product or related service in order to derive insights about the economic situation of the user or its assets or production methods or the use in any other way that could undermine the commercial position of the user on the markets it is active on. This would, for instance, involve using knowledge about the overall performance of a business or a farm in contractual negotiations with the user on potential acquisition of the user's products or agricultural produce to the user's detriment, or for instance, using such information to feed in larger databases on certain markets in the aggregate (e.g. databases on crop yields for the upcoming harvesting season) as such use could affect the user negatively in an indirect manner. The user should be given the necessary technical interface to manage permissions, preferably with granular permission options (such as "allow once" or "allow while using this app or service"), including the option to withdraw permission».

[48] «This Regulation should therefore build on recent developments in specific sectors, such as the Code of Conduct on agricultural data sharing by contractual agreement. Sectoral legislation may be brought forward to address sector-specific needs and objectives».

[49] At Article 6: «The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards [...]».

[50] Recital 19 notes that «In practice, not all data generated by products or related services are easily accessible to their users, and there are often limited possibilities for the portability of data generated by products connected to the Internet of Things. Users are unable to obtain data necessary to make use of providers of repair and other services, and businesses are unable to launch innovative, more efficient and convenient services. In many sectors, manufacturers are often able to determine, through their control of the technical design of the product or related services, what data are generated and how they can be accessed, even though they have no legal right to the data. It is therefore necessary to ensure that products are designed and manufactured and related services are provided in such a manner that data generated by their use are always easily accessible to the user».

[51] As mentioned before, Article 7 explicitly states that «The obligations of this Chapter shall not apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as micro or small enterprises, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as a micro or small enterprise».

same quality as is available to the data holder and, where applicable, continuously and in real-time». The User can now file a request to the Data Holder and force them to send their data to a Third Party, without having to incur in additional costs or wait a long time. Data Holder cannot use the data portability principle as an excuse to charge Users with transfer fees (which, for example, was often the case with telecommunication companies), nor they can speciously delay the transfer.

In addition, instead of making a request on their own name, Users, by law, can now give a power of attorney[52] to a third party, which acts in force of a contract of mandate. This provision is introduced for legal systems that do not have an existing discipline regarding mandate, and, in legal systems where this contract already exists, to force by law Data Holder to promptly comply with that mandate. In fact, even in legal systems in which special mandate is defined by a legal provision [53], it is not uncommon that large companies refuse to accept it in order to stonewall the User's request and avoid to comply with it. Thanks to this new provision, the possibility to use a mandate and the obligation to comply are clearly laid out by law.

Specularly to paragraph 6 of Article 4, paragraphs 6 and 7 coordinate the right to portability with that provided by GDPR, stressing the prevalence of the latter.

Paragraph 2 builds a bridge to the proposal for a Digital Markets Act of 2020, providing that "gatekeepers"[54] are not eligible to be considered "Third Parties" in this context. It also forbids them to:

- solicit or incentivize Users to make data, which has been obtained using the right of access, available to their services;
- solicit or incentivize Users to transfer data through to the right of portability;
- receive from Users the data obtained through the right of access.

This provision is intended to avoid giving gatekeepers (such as Google) even more

[52] By power of attorney we mean the unilateral act by which one person empowers another to represent him/her/them.

[53] E.g., the Civil Code, such as in Italy, Article 1703: «The mandate is the contract by which one party commits to perform one or more legal acts on behalf of the other».

[54] Gatekeepers are defined by the Digital Markets Act as providers of core platform services such as: «(a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communication services; (f) operating systems; (g) cloud computing services; (h) advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services listed in points (a) to (g)»; provided that «(a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future». In addition, it has to meet the following thresholds: «(a) the requirement in paragraph 1 point (a) where the undertaking to which it belongs achieves an annual EEA turnover equal to or above EUR 6.5 billion in the last three financial years, or where the average market capitalisation or the equivalent fair market value of the undertaking to which it belongs amounted to at least EUR 65 billion in the last financial year, and it provides a core platform service in at least three Member States; (b) the requirement in paragraph 1 point (b) where it provides a core platform service that has more than 45 million monthly active end users established or located in the Union and more than 10 000 yearly active business users established in the Union in the last financial year; for the purpose of the first subparagraph, monthly active end users shall refer to the average number of monthly active end users throughout the largest part of the last financial year; (c) the requirement in paragraph 1 point (c) where the thresholds in point (b) were met in each of the last three financial years».

business power than they already have, so that their economic position is not made stronger by a provision originally intended to help SMEs and consumers. The explicit exclusions also make sure that the User is not "tricked" into giving consent to the gatekeeper to re-use the data accessed according to the proposal. It is very common that Users do not read full texts of Terms and Conditions[55], therefore it is necessary to prevent exploitative practices that would allow them to easily gain access to an increased amount of User's data from third parties just by inserting a related clause in their Terms. Also, it prevents gatekeepers from obtaining data from Users through a compensation (monetary or not). This legal framework is complementing that of the Digital Markets Act to stem the bargaining and economic power of Big Techs by returning the control over data to consumers and by limiting their room for manoeuvre. If they wish to obtain the data, they cannot do this thanks to the Data Act.

Other provisions aimed at facilitating the right to portability require Data Holder to refrain from requesting «any information beyond what is necessary to verify the quality as user or as third party», and from keeping any information on the third party's requests beyond what is necessary to execute the request and «for the security and the maintenance of the data infrastructure».

In addition, exactly as provided for the right to access, a provision aimed at protecting trade secrets has been laid down: «the data holder shall not use any non-personal data generated by the use of the product or related service to derive insights about the economic situation, assets and production methods of or use by the third party that could undermine the commercial position of the third party on the markets in which the third party is active». However, a loophole also has been unwisely inserted: «Unless the third party has consented to such use and has the technical possibility to withdraw that consent at any time", enabling Data Holder to hide the consent form, as is often the case, under the general Terms and Conditions button. Is it any wonder why the Third Party would consent to let Data Holder derive information that potentially "could undermine the commercial position [...] on the markets».

Paragraph 8 protects the Data Holder specifying that trade secrets may only be disclosed to Third Parties insofar as they are strictly necessary to achieve the purpose agreed between the User and the Third Party (that is, in the context of the right to portability). The Third Party is required to adopt all necessary specific measures agreed upon to preserve the confidentiality of that information. The provision also requires that the Data Holder and the Third Party specify the nature of the data as trade secrets, and the security and organizational measures to preserve their confidentiality, in an agreement (which may well be inserted in the above-mentioned Terms and Conditions). This asymmetry of protection between Third Parties (which, according to this proposal, can only be non-gatekeepers) and Data Holders (which, at the contrary, generally are Big Techs) is out of tune with the purpose of the regulation.

On the other hand, interestingly, the provision forbid the Third Party to «deploy coercive means or abuse evident gaps in the technical infrastructure of the data holder designed to protect the data in order to obtain access to data», which in many coun-

[55] N. Steinfeld, *I agree to the terms and conditions:(How) do users read privacy policies online? An eye-tracking experiment*, in *Computers in human behavior*, 55, 2016, 992 ss.

tries would already *per se* constitute a criminal offense.

Article 6 imposes additional obligations to Third Parties, in order to protect Users from unfair use of the transferred data. First, similarly to GDPR, it introduces the principles of purpose and storage limitation, requiring Third Parties to limit the processing only to the purposes and under the conditions agreed with the User (also taking into account GDPR whenever personal data are involved), and it also requires them to delete the data as soon as they are no longer necessary to fulfil those purposes. In addition, according to the principle of fairness, it prohibits Third Parties to:

- coerce, deceive or manipulate the User in any way[56];
- use the received data to profile natural persons, unless it is necessary to provide the requested service;
- make the received data available to another third party, unless this is necessary to provide the requested service;
- make the received data available to gatekeepers;
- use, alone or through another party, the received data to develop a product that competes with the Data Holder's products;
- prevent the User to exercise the right to portability towards other parties.

The first paragraph of Article 8 forces Data Holders to abide to the principle of fairness, transparency, reasonableness, and non-discrimination[57], extending its scope not only to the sharing of data under this regulation, but also to any «other Union law or national legislation implementing Union law» that require them to share the data. Of course, fairness, reasonableness, and non-discrimination principles are fundamental principles of Union Law, therefore Data Holders are generally forced to apply them to natural persons. This provision, however, extends them, together with the transparency principle, to the general framework of data sharing, forcing Data Holders to comply with Chapters III and IV, and therefore to be subjected to the administrative fines provided by Article 33, even when they are making data available under a different piece of legislation. This is an interesting implication of the proposal, considering the upcoming set of legislation implementing the EU Digital Strategy.

To prevent situations of uncertainty and to attract the protection laid down by contractual law, paragraph 2 requires both Data Holders and Users to enter into a contract to regulate the terms of data availability (and are not obliged to provide more information than that strictly necessary to demonstrate compliance to the agreed contractual clauses[58]). It also states that clauses regarding the access to and use of the data or the liability and remedies for the breach or the termination of data-related obligations,

[56] The article specifies «by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user».

[57] «Where a data holder is obliged to make data available to a data recipient under Article 5 or under other Union law or national legislation implementing Union law, it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner in accordance with the provisions of this Chapter and Chapter IV».

[58] See para. 5: «Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or their obligations under this Regulation or other applicable Union law or national legislation implementing Union law».

which are deemed to be unfair (according to Article 13) or in breach of User's rights under Chapter II, are nonbiding. It is unclear why the legislator has chosen the expression "non-binding" instead of "void", since it is referring to clauses that are contrary to mandatory provisions, which are non-derogable. In this context, it is reasonable to assume that the meaning is equal to "void", that is non-enforceable, non-remediable, and *ab origine* without any effect. Because of the aim of this provision, it is also presumed that the whole contract will be valid even without those void clauses.

With regards to the non-discrimination principle, it is forbidden to Data Holders to discriminate between "comparable categories"[59] of Data Recipients, including their partner enterprises or linked enterprises. In this context, the burden of proof is inverted: the Article provides that the Data Holder needs to demonstrate that no discrimination occurred. In addition to this provision, it is also forbidden to form a monopoly, making data available on an exclusive basis, unless explicitly requested by the User.

Article 9, following the principle of reasonableness, prescribes that any agreed compensation for making data available shall be reasonable, and in cases where the Data Recipient is a micro, small or medium enterprise, such compensation cannot exceed direct costs to comply with the request; however, the Article states that subsequent law may regulate its amount.

In the last paragraph, according to the principle of transparency, it is provided that Data Holders must provide in sufficient detail the criteria on which the calculation is based, in order to allow the Data Recipient to verify the reasonableness of the amount and where the direct costs originate.

The legislator provides for a dispute settlement mechanism to settle disputes in relation to the determination of fair, reasonable and non-discriminatory terms for and the transparent manner of making data available (Article 30), by establishing independent and certified bodies in each Member State.

6. Making data available in case of exceptional need

The right to access is not the only way in which the proposal requires Data Holders to share the data in their possession (as before, excluding small and micro enterprises). In fact, another important novelty of the Data Act is Article 14, which introduces the obligation to make data available to public bodies and authorities based on exceptional need circumstances, following a simple request. The concept of exceptional need is identified by Article 15 in

- the necessity to respond to a public emergency;
- the necessity to prevent a public emergency or to assist the recovery from a public emergency, when the data request is limited in time and scope;
- the necessity to fulfill a specific task in the public interest that has been explicitly provided by law, that is hindered by the lack of available data;

[59] The proposal does not draw any example or criteria to determine if a Data Recipient is deemed comparable. It could be presumed that reference should be made to size, sector, turnover.

- the impossibility for public sector body or Union institution, agency or body, to obtain such data by alternative means[60].

This provision may be seen as laying down a form of expropriation. The difference between the obligation to make data available towards Users and towards public bodies is that in the first case the data is generated by Users and consequently it can be argued that they are the legitimate owners, while in the latter case the obligation is towards a third party, who has no role in the generation of the data itself. In principle, third parties have no right over the data, and they are not part of the contract between Data Holders and Users. Only User can authorize Data Holders to share the data with Third Parties, conferring a power of attorney. In this case, not only the permission of the Users is bypassed, but they even have no possibility of challenging the request.
The value of data is now recognized worldwide and even became the core of many business models. For some companies, data is the only resource they have. In this context, it is clear that a sharing obligation means a transfer of assets from the company to the public authority, even if it is done for the public interest and in a situation of public emergency. Data can be considered as goods protected by international investment law,[61] but because of their nature, which allows to make copies, it is unlikely that the mandatory sharing obligation can be considered as direct expropriation. It is, however, possible to consider it as indirect expropriation.
On the other hand, it could be argued that the burden on companies is limited, as they are forced to share only a *copy* of their asset, thus continuing to exploit data for their own purposes. In addition, it has to be noted that the obligation only arises in limited cases, for example when it has not been possible to obtain the same data at market price. The company, in principle, could avoid the expropriation by preparing their data in advance to sell it to public authorities (when feasible and allowed by law).
According to article 17 of the EU Charter of Fundamental Rights[62], the rule of law must be respected when expropriating property in cases of public interest and a fair compensation must be paid.
However, Data Holders are not always compensated for the data sharing towards public entities, as in the case of public emergency they are required to make data available for free.
There are some guarantees for a fair and transparent request by public bodies. In fact, the request must abide some mandatory conditions. First, it must be specified what

[60] As some examples of unsuccessful attempts to obtain such data in other ways, the Article list the impossibility of purchasing the data on the market at market rates; the impossibility of obtaining the data by relying on existing obligations; and the fact that adopting new legislative measures would be too lengthy and could not ensure the timely availability of the data; it also mentions the circumstance that obtaining the data through the procedure laid down in the Data Act would substantively reduce the administrative burden for Data Holders or other enterprises.

[61] T. Peramatukorn, *Potential Expropriation Claims Against Data Sharing Requirements*, in *NYU Journal of International Law and Politics*, 54(1), 2021, 249 ss.

[62] «1. Everyone has the right to own, use, dispose of and bequeath his or her lawfully acquired possessions. No one may be deprived of his or her possessions, except in the public interest and in the cases and under the conditions provided for by law, subject to fair compensation being paid in good time for their loss. The use of property may be regulated by law in so far as is necessary for the general interest. 2. Intellectual property shall be protected».

data are required, the legal basis that allows the request, the deadline for complying to it or to challenge it. Article 18 provides that the Data Holder may decline or seek the modification of the request within 5 working days fin case of public emergency grounds and within 15 working days in other cases of exceptional need, if the data is unavailable, if the request does not meet the conditions laid down in Article 17 of the proposal, or if the requested data has already been provided in response to previously submitted request for the same purpose by another public body. In case of controversy, the case will be brought before the competent authority (Article 31).
Secondly, the public body cannot simply file a request, but it must demonstrate the exceptional need for which the data are requested, and it need to be proportionate to that exceptional need, in terms of the granularity and volume of the data requested and frequency of access of the data requested. The proposal requires that the legitimate aims of the Data Holder, the protection of trade secrets, and the cost and effort required to make the data available must be taken into account.
In addition, the purpose of the request, the intended use of the data requested, and the duration of that use must be specified.
Lastly, following the principle of data minimization, the request must concern non-personal data as much as possible. When personal data are needed, the Data Holder must take reasonable efforts to pseudonymise the data, if the request can be fulfilled with pseudonymised data. Regarding trade secrets, they can only be requested if the disclosure is strictly necessary to achieve the purpose of the request.
The public body must also inform the Data Holder of the penalties that will occur in the event of non-compliance with the request.
Additional guarantees are provided by Article 19, according to which the public body must respect the purpose limitation principle, implement technical and organisational measures that safeguard the rights and freedoms of data subjects whenever personal data are received, and follow the principle of storage limitation, destroying the data as soon as they are no longer necessary and informing the data holder that the data have been destroyed.

7. Transparency

Transparency is an overarching principle throughout the proposal, following the example of many legal instruments that are part of the EU Digital Strategy.
First, Article 3 introduces the right of information, stating that the subject that enter in a contract of purchase, rent, or lease with the User needs to provide the following information:

- the nature and volume of the data likely to be generated by the use of the product or related service;
- whether the data is likely to be generated continuously and in real-time;
- how the user may access those data;
- whether the manufacturer or the service provider intends to use the data itself or allow a third party to use the data and, if so, the purposes for which those data

will be used;
- whether the seller, renter or lessor is the data holder and, if not, the identity of the data holder (trading name and the geographical address);
- the means of communication to contact the data holder quickly and efficiently;
- how the user may request that the data are shared with a third-party;
- the user's right to lodge a complaint with the competent authority.

The right of information is designed in such a way that even companies providing their service for free through a software license are required to comply. Following the solution adopted by GDPR, Article 3 requires to disclose the data transfer to third parties, but also the purposes of the processing and the identity of the Data Holder.
Secondly, the transparency principle is translated in the obligation of the Data Holder to inform the Users on how the data may be accessed, before they enter into a contract (Recitals 20 and 23[63]). The right of access is itself a manifestation of the transparency principle.
In addition, the proposal prescribes transparency in contractual terms between Users and Data Holders with regards on how the latter intend to use the data generated by the use of their products, as explained in Recital 24[64].
Data Holders should also be transparent in explaining the justification of the compensation requested for making data available to third parties and the calculation criteria, in order to make it possible to assess the reasonableness of the request[65].
Public bodies are prescribed to be transparent as well when requesting data in cases of exceptional need, clearly stating the purpose of the request, the intended use of the data and the duration of that use[66]. They must notify the Data Holder when they

[63] Recital 23 explains the provisions regarding data access: «Before concluding a contract for the purchase, rent, or lease of a product or the provision of a related service, clear and sufficient information should be provided to the user on how the data generated may be accessed. This obligation provides transparency over the data generated and enhances the easy access for the user».

[64] «This Regulation [...] should not be understood as conferring any new right on the data holder to use data generated by the use of a product or related service. This applies in particular where the manufacturer is the data holder. In that case, the basis for the manufacturer to use non-personal data should be a contractual agreement between the manufacturer and the user. This agreement may be part of the sale, rent or lease agreement relating to the product. Any contractual term in the agreement stipulating that the data holder may use the data generated by the user of a product or related service should be transparent to the user, including as regards the purpose for which the data holder intends to use the data».

[65] As pointed out in Recital 47: «Transparency is an important principle to ensure that the compensation requested by the data holder is reasonable, or, in case the data recipient is a micro, small or medium-sized enterprise, that the compensation does not exceed the costs directly related to making the data available to the data recipient and is attributable to the individual request. In order to put the data recipient in the position to assess and verify that the compensation complies with the requirements under this Regulation, the data holder should provide to the data recipient the information for the calculation of the compensation with a sufficient degree of detail».

[66] Recital 61 explains that «[...] data requests by public sector bodies and by Union institution, agencies and bodies to data holders should be transparent and proportionate in terms of their scope of content and their granularity. The purpose of the request and the intended use of the data requested should be specific and clearly explained, while allowing appropriate flexibility for the requesting entity to perform its tasks in the public interest. The request should also respect the legitimate interests of the businesses to whom the request is made. [...] To ensure transparency, data requests made by public sector bodies and by Union institutions, agencies or bodies should be made public without undue delay by the entity

transmit or otherwise make data available to another public entity pursuant to Articles 17 and 21. They also need to inform the Data Holder about the penalties prescribed according to Article 33 for the infringement of the Data Act, as required by Article 17. However, in such cases no obligation of informing the Users is laid down by the current version of the proposal, unless the requested data set contains personal data, and this circumstance seems at odds with the general transparency obligation imposed in the rest of the act.

Lastly, DPSs are requested to enact the transparency principle when receiving a request to access the data from a foreign authority[67]. This provision ensures that Users in EU have the possibility to promptly prepare to defend their rights and seek legal assistance, since the foreign country requesting the data may have a very different legal system, with different limitation of action time frames that require an immediate reaction.

8. Regulating Smart Contracts

The proposal regulates also the use of Smart Contracts (SCs) for data sharing (Article 30). SCs «are pieces of code that enable users to write their own arbitrary rules for ownership, transaction formats and state transition functions. This means, two parties can digitally interact following a set of customized rules (defined by one of the parties) without the need of a third trusted party to secure the transaction. The deployment and/or interaction with smart contracts are immutable, permanent and irreversible. The process of deploying or interacting with an already deployed smart contract over the blockchain requires the users to connect to the peer-to-peer network through a client. Nodes in the network execute the smart contracts in return for a reward that keeps them incentivized. Rewards are referred to as gas, an execution fee willingly paid by nodes deploying or triggering the smart contracts»[68].

SCs are based on blockchain technology, which is «a distributed, decentralized, and tamper-proof shared ledger technology that allows peer-to-peer transmission»[69]. This technology has gained popularity in recent years as a method to mitigate privacy, security, and efficiency issues of centralized platforms[70], as in these systems a public

requesting the data and online public availability of all requests justified by a public emergency should be ensured».

[67] Recital 77 states in this regard that «Wherever possible under the terms of the data access request of the third country's authority, the provider of data processing services should be able to inform the customer whose data are being requested in order to verify the presence of a potential conflict of such access with Union or national rules, such as those on the protection of commercially sensitive data, including the protection of trade secrets and intellectual property rights and the contractual undertakings regarding confidentiality».

[68] E. Zaghloul – T. Li – J. Ren, *Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts*, in *2019 International Conference on Computing, Networking and Communications (ICNC)*, IEEE, 2019, 375 ss.

[69] S. Xuan et al., *An incentive mechanism for data sharing based on blockchain with smart contracts*, in *Computers & Electrical Engineering*, 83, 2020, 106587.

[70] E. Zaghloul – T. Li – J. Ren, *Security and privacy of electronic health records*, cit.

ledger of records and transactions ownership is maintained by the network in real-time, secured by cryptography[71]. A key difference between centralized systems and blockchain-based systems is that the latter «do not suffer from a single point of failure and do not require a third trusted party to maintain the integrity of data ownership and flow»[72].

Because of the fact that once in the blockchain it is not possible to erase the data, which will be stored in a decentralized network, it must be ensured that no personal data is stored in the blockchain, in accordance with GDPR. This is one of the reasons that justify the need for regulating SCs.

The proposal requires whoever deploys SCs in the context of an agreement to make data available to comply with the following rules, being responsible for the compliance:

- robustness by design: ensure that the SC offers a very high degree of robustness by design, to avoid functional errors and to withstand manipulation by third parties;
- safe termination and interruption: ensure that it is possible to terminate the continued execution of transactions; the SC must be equipped with internal functions to stop or interrupt the operation to avoid future (accidental) executions;
- data archiving and continuity: foresee the possibility to archive transactional data, the SC logic and code, to keep the record of the operations performed on the data in the past (auditability), when a SC must be terminated or deactivated;
- access control: a SC must be protected through rigorous access control mechanisms and smart contract layers;
- conformity assessment: assess the compliance with the requirements and issue an EU declaration of conformity.

The provision also provides that a SC that meets the harmonised standards published in the Official Journal of the European Union is presumed to be in conformity with the above-mentioned requirements to the extent those standards cover them.

9. Provision regarding Data Processing Services

The Regulation introduces the concept of Data Processing Service, defined as «a digital service other than an online content service as defined in Article 2(5) of Regulation (EU) 2017/1128, provided to a customer, which enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature». The reference is obviously to cloud services providers, such as Microsoft, Amazon, Google. The proposal anticipates the expansion in the market related to DPSs, which will be likely prompted by the enacting of the Data Act itself, since, by limiting the power of large foreign companies, it will enhance the competition for European actors.

A cloud computing service is a common IT solution that allows Users to store and

[71] *Ibid.*

[72] *Ibid.*

process their data on third-party IT facilities, such as servers, computing power, and software, accessible on demand through Internet technologies[73].[74]There are many different types of cloud services and the simplest is the mere storage solution (such as Dropbox), which allows Users to just upload and store their data online. Because Users are physically giving a copy of their data (uploading it online) to a third party, it basically can be thought of as an agreement of mixed nature, composed of a custodial contract and a service contract, in which one party (the DPS provider) commits to keep and guard the other party's data, making them available at request, and sometimes also to provide other services (such as software applications that provide analysis tools) through their own means and facilities, and the depositor commits to pay a fee for the whole service. Part of legal scholars consider it as a mixed contract composed of a lease agreement and a service agreement,[75] others as a mere service contract, and others as a custodial contract[76] when no other service but the storage space is provided. The ownership of the data remains of the depositor, while the cloud service provider is a mere possessor and custodian, and generally has no intention of exercising property rights on the data (*animus detinendi*), unless otherwise agreed.
The qualification of the contract is very important to understand duties and rights of the parties. For example, in the custodial contract, the custodian has the duty to i) make the objects available to the depositor at request, in the same state they were handed; ii) keep the objects safe in their facilities and prevent them from being stolen or accessed, or used by third parties, with the same *diligentiam quam in rebus suis adhibere solet*;[77] iii) not making use of the objects for their own purposes (*Depositum consistit ex custodia non ex usu*) iv) return the objects and their unearned income to the depositor at the end of the contract, in the same state they were handed. In the lease contract, at the contrary, the lessor has the duty to i) make their facilities available to the lessee in a good state ii) keep the facilities available and accessible during the whole duration of the contract so that the lessee can use it as agreed iii) repair and perform the maintenance of the facilities iii) prevent other parties from interrupting of disturbing the use of the facilities. On the other hand, in the service contract, the contractor has the duty of i) render the agreed services through their own means and facilities and at their own risk ii) keep the objects safe and prevent them from being stolen, accessed or used by third parties, with the same *diligentiam quam in rebus suis adhibere solet* iii) let the commissioner check the status and performance of the services iv) guarantee that the services are executed as agreed and without flaws v i) make the objects available to the commissioner at request.

[73] The National Institute of Standards and Technology (NIST) defines it as «a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction».

[74] M. Hogan et al., *Nist cloud computing standards roadmap*, in *NIST Special Publication*, 35, 2011, 6 ss.

[75] A. Mantelero, *Il contratto per l'erogazione alle imprese di servizi di cloud computing (Cloud Computing Contracts: B2B)*, in *Contratto e impresa*, 4-5, 2012, 1216 ss.

[76] G. Sicchiero, *Il contratto di deposito di beni immateriali: i-cloud e files upload*, in *Contratto e Impresa*, 2, 2018, 681 ss.

[77] *Ibid.*

Cloud computing contracts are usually composed of three distinguished documents, one containing the general conditions of the service, one inherent the polices regarding the behaviour of the parties, and one prescribing the modalities of the data processing.[78] However, because of the unbalance of powers between the cloud providers and their clients, these terms are often unilaterally drafted and imposed, and no negotiation of the clauses is possible. To tackle this issue, the proposal provided some mandatory terms, to be included in all contracts, protecting Users from vexatious contractual clauses. At Articles 23, 24, 25, and 26, some guidelines are drawn to eliminate obstacles to the switching between providers of DPS, in order to ensure interoperability, both from a technical and business perspective. This is motivated by the necessity of preventing "lock-in" practices, which are very common in cloud computing contracts.

In particular, the provisions are aimed at removing commercial, technical, contractual and organisational obstacles to let Users switch between different DPSs. Such obstacles are first identified in contractual practices preventing Users from:

- cancelling the contract with more than 30 days of notice;
- entering into a contract with a different DPSs which provide the same service type;
- transferring their data, applications and other digital assets to other DPSs;
- maintaining functional equivalence of the service in the IT-environment of the DPSs to which they are switching.

To protect the User from the most common unfair contractual terms, Article 24 forces DPSs to clearly set in a contract their obligations and the rights of the customer related to the switching between providers[79]. It prescribes that at least the following elements must be included in the contract:

- the possibility for customers to switch to a DPS offered by a different company, or to port all data, applications and digital assets generated by them to an on-premise system. The request must be fulfilled within 30 calendar days, during which the DPS must assist and, if technically feasible, complete the switching process, and ensure full continuity in the functions or services;
- an exhaustive specification of all data and application categories exportable during the switching process, including, at minimum, all data imported by the customer at the inception of the service agreement and all data and metadata created by the customer and by the use of the service during the period the service was provided, including configuration parameters, security settings, access rights and access logs to the service;
- a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transition period that was agreed between the customer and the service provider.

[78] A. Mantelero, *Il contratto per l'erogazione alle imprese di servizi di cloud computing,* cit.; S. Bradshaw – C. Millard – I. Walden, *Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services*, in *International Journal of Law and Information Technology*, 19(3), 2011, 187 ss.

[79] The provision stresses the fact that it is without prejudice to Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

It is also provided that, if the mandatory transition period of 30 days is technically unfeasible, the DPS must notify the customer within 7 days, duly motivating the technical unfeasibility with a detailed report and indicating an alternative transition period of maximum 6 months, during which full service continuity must be ensured.

9.1 Interoperability

The proposal also establishes a right to data interoperability for the User, in order to remove technical obstacles for the switching. Interoperability means that different cloud solutions are able to communicate and exchange data between each other's. In concrete terms, it allows users to transfer their data from one provider to another across heterogeneous hardware and software resources, without losing any data, in terms of functionality or accessibility.

In fact, in order to be able to switch from one DPS provider to another, Users need to be able to i) access their data before their contract is ending, or soon after (accessibility); ii) transfer their data to the other provider, e.g., by downloading it and then uploading to the new servers, or by directly transferring it (portability); iii) have their data in a format that is compatible with the new provider's systems (interoperability). In commercial practice, it often happens that vendors adopt proprietary format that prevents Users to efficiently port their data in different environments (the so-called lock-in practice). If the format is not compatible with the new provider's system, and it is not possible to convert it to a compatible format, then the User loses its data. This often happens for applications specifically built for a certain environment (e.g., Microsoft Azure).

Although many studies highlight the fact that lock-in practices constitute a major barrier to cloud computing adoption,[80] the research on cloud interoperability issues is limited.[81] Some industry bodies have tried to develop standards, but the issues has not been solved so far. The Data Act aims at tackling the issue at least with regards to portability of Users' data.

Firstly, in case the cloud services «concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure», but «do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements», that is the most basic DPS service, the DPS must ensure that the customer, after switching to a different provider offering the same kind of services, is able to enjoy «functional equivalence in the use of the new service». The reference is probably to cloud computing providing storage services, however the wording is not very clear and may lead to uncertainty regarding the

[80] D. Petcu – A. V. Vasilakos, *Portability in clouds: approaches and research opportunities*, in *Scalable Computing: Practice and Experience*, 15(3), 2014, 251 ss.; J. Opara-Martins – R. Sahandi – F. Tian, *Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective*, in *Journal of Cloud Computing*, 5(1), 2016, 1 ss.

[81] X. V. Wang – L. Wang – R. Gördes. *Interoperability in cloud manufacturing: a case study on private cloud structure for SMEs*, in *International Journal of Computer Integrated Manufacturing*, 31(7), 2018, 653 ss.

subjects of this provision.
Secondly, for all other services, which means those providing access to «the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements», the proposal prescribes that DPSs must «make open interfaces publicly available and free of charge and ensure compatibility with open interoperability specifications or European standards for interoperability», where existing. If the standards do not exist, the DPS must, at the request of the customer, export all generated or co-generated data «in a structured, commonly used and machine-readable format». The wording is again unclear and the impact of this provision is still uncertain. Is the legislator expecting Amazon to create an «open interfaces publicly available and free of charge» for their services, or just for the switching of data to a different service, in order to provide functional equivalence?
The Recitals stress the necessity of an intervention at EU level, however it is unclear how DPSs will need to comply to the Data Act in the meantime that those standards are developed and tested. It is hoped that these provisions will be modified by the EU bodies before the regulation is enacted.

9.2 International transfer of data

Similarly to GDPR, the legislator provided for some limit to the transfer of data outside the EU, requiring DPSs to «take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State». Even if it is only related to nonpersonal data, the provision was clearly inspired by the Schrems II judgments of the Court of Justice of the European Union (CJEU) in 2020, which invalidated the Privacy Shield between the US and the EU. In fact, the judgment highlighted that the US law is very invasive of privacy even when data are not located in the US, because companies are forced to transfer the data in their possession to the US authorities.
The European Data Protection Board noted that «the US CLOUD Act also extends the possibility to request data wherever they are stored or located to the whole of Chapter 121 of USC Title 18 on 'Stored wired and electronic communications and transactional records access'. To our understanding, this means that this applies to many other data collection avenues, in particular to requests to access content data through a court order or a subpoena (either administrative, grand jury or trial subpoena). It also applies to requests for non-content data (so-called 'metadata') under §2703 of Chapter 121 USC Title 1811, which covers (subsection (c)) a whole range of avenues, including warrants and court orders, but also avenues that do not necessarily require judge intervention or a probable cause test, such as formal written requests or subpoenas. Furthermore, the US CLOUD Act opens the possibility for service providers to 'intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government' (this covers real-time interception)

under the condition that this foreign government has entered into an executive agreement with the US». This circumstance poses a risk not only for personal data, but also for trade secrets, government classified documents, and other data that may be relevant for the protection of EU interests.

The Data Act aims at making sure that foreign data centers, on which usually cloud providers rely, do not put EU data at risk by communicating relevant information to foreign governments, not only in the US, but also in other countries where the relationships are tenser. Therefore, it is provided that even when a judicial or administrative decision requiring the transfer of data is present, it «may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or any such agreement between the requesting third country and a Member State».

In the absence of such an international agreement, the transfer to or access to the data by third-country authorities can take place only in three cases, notably when the rule of law is respected:

- where the third-country system requires that the reasons and proportionality of the decision are set out, and it requires such decision to be specific, for instance by establishing a sufficient link to certain suspected persons, or infringements;
- the DPS can file a reasoned objection, which is subject to a review by a competent court in the third-country;
- the competent court or authority is empowered, under the law of that country, to take duly into account the relevant legal interests of the provider of the data protected by Union law or national law of the relevant Member
- State.

The DPS which receives the request according to a judicial or administrative decision has the possibility to ask the opinion of the relevant competent authorities of the EU to be sure that the required conditions are met, especially if commercially sensitive data, or national security or defense interests of the Union or its Member States are at stake.

While it may be easy to make sure that European DPSs respect this provision, it might be questionable to assume that foreign companies would refuse to comply with a decision of their own country, therefore the impact of this provision might be limited. It would be wise for the legislator to provide a different compliance mechanism other than just providing a body that will give an advice on the transfer. For example, a provision may be inserted to give companies a stronger leverage to oppose their government, such as a judicial decision from a European Court. In the case of GDPR, the enforcement mechanism is just limited to the stopping of all transfer to third countries. It is unknown, however, if this solution will be adopted in the case of the Data Act, and how it will be enforced in practice.

10. Provisions regarding unilaterally imposed unfair clauses

The new legal framework tackles the issue of unfair contractual terms unilaterally imposed on a micro enterprises and SMEs by providing, in Chapter IV of the proposal, some mandatory terms, non-derogable in any way by the parties. The discipline is borrowed by consumer protection law, and in particular Directive 93/13/EEC.
The introduction of this discipline for the protection of non-consumers builds upon a long tradition both at EU level and at national level; the theme of unfair commercial practices in B2B contracts has seen multiple failed attempt of regulation within the EU[82], while it has successfully been implemented in some Member States[83]. Recently, a further step towards the harmonization of the discipline has been made by the Regulation on promoting fairness and transparency for business users of online intermediation services, which provides some rules to prevent unfair contractual practices.
The scope of application of the Chapter is not restricted to specific cases, but it applies to all contracts regardless of their nature, field, or duration, provided that they pertain to the access to and use of data, liability, remedies for the breach, or termination of data related obligations. In fact, it provides that, when it comes to those specific subject, unilaterally imposed terms are not binding on micro enterprises and SMEs if they are unfair. The concept of unfairness was introduced by Directive 93/13/EEC, which provides that contractual terms which have not been individually negotiated must be considered unfair whenever they cause an imbalance of rights and obligations against the weaker party[84].
"Unilaterally imposed" means that «it has been supplied by one contracting party and the other contracting party has not been able to influence its content despite an attempt to negotiate it». The concept is slightly different from that of consumer protection enshrined in Directive 93/13/EEC[85], as it does not refer only to pre-formulated standard contracts, but, being in the context of B2B relationships, it expands its scope to clauses that have been individually negotiated outside the context of a pre-formulated standard contract, albeit without success. Companies have more contracting power than consumer, therefore they might be able to negotiate many clauses in a contract; however, larger enterprises are still able to impose most of their own terms to the detriment of their counterpart.

[82] Such as the proposal for a Common European Sales Law in 2011, which can now be considered shipwrecked.

[83] See, for example, in Belgium, the Law of 4 April 2019, and, in Italy, Articles 1341 and 1342 of the Civil Code.

[84] As drawn up by Article 3: «A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer».

[85] Article 3: «A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract. The fact that certain aspects of a term or one specific term have been individually negotiated shall not exclude the application of this Article to the rest of a contract if an overall assessment of the contract indicates that it is nevertheless a pre-formulated standard contract».

Like in the above-mentioned Directive[86], the burden of proof is reversed on the contracting party that supplied a contractual term, that is, the other party can claim that the term was unilaterally imposed without having to prove the claim. This provision is intended to protect the weaker part from the most common unfair practices of larger companies, which usually have the bargaining power to decide the most favourable terms for themselves.

The Directive makes reference to the criterion of objective good faith, which is transposed in the text of the novel legislation. The second paragraph of Article 13, in fact, defines unfairness as the grossly deviation from good commercial practice in data access and use, contrary to good faith and fair dealing. Good faith and fair dealing are then the measure that makes it possible to distinguish between lawful practices and illicit ones. The third paragraph draws a list of clauses that are considered unfair by law:

excluding or limiting the liability of the party that unilaterally imposed the term for intentional acts or gross negligence;

excluding the remedies available to the party upon whom the term has been unilaterally imposed in case of non-performance of contractual obligations, or the liability of the party that unilaterally imposed the term, in case of breach of those obligations;

giving the party that unilaterally imposed the term the exclusive right to determine whether the data supplied are in conformity with the contract or to interpret any term of the contract.

Other terms are presumed unfair if their object or effect is to:

- «inappropriately limit the remedies in case of non-performance of contractual obligations or the liability in case of breach of those obligations;
- allow the party that unilaterally imposed the term to access and use data of the other contracting party in a manner that is significantly detrimental to the legitimate interests of the other contracting party;
- prevent the party upon whom the term has been unilaterally imposed from using the data contributed or generated by that party during the period of the contract, or to limit the use of such data to the extent that that party is not entitled to use, capture, access or control such data or exploit the value of such data in a proportionate manner;
- prevent the party upon whom the term has been unilaterally imposed from obtaining a copy of the data contributed or generated by that party during the period of the contract or within a reasonable period after the termination thereof;
- enable the party that unilaterally imposed the term to terminate the contract with an unreasonably short notice, taking into consideration the reasonable possibilities of the other contracting party to switch to an alternative and comparable service and the financial detriment caused by such termination, except where there are serious grounds for doing so».

The proposal follows the principle *utile per inutile non vitiatur*, therefore providing that if a clause is non-binding, it doesn't invalidate the whole contract.

As it is easy to note, the list is significantly shorter than the one provided by the An-

[86] Article 3: «Where any seller or supplier claims that a standard term has been individually negotiated, the burden of proof in this respect shall be incumbent on him».

nex to Directive 93/13/EEC, although it can be argued that the regulation does not intend to establish a *numerus clausus* of terms, but different cases are left open by the general provision contained in the second paragraph of Article 13.
The list does not mention the most common clauses that are present in IoT and cloud computing contracts, such as the ones granting to the Data Holder the indiscriminate right to make use of the data as they wish (e.g., to improve their services, to sell the data to third parties, to profile users for advertisement purposes), as they fall out of scope of the proposal. However, in a study conducted by EY in 2018 about unfair cloud computing contracts, most SMEs reported a number of problems, such as unilateral changes of the contract, that lead to significant economic detriment, which have not yet been addressed by the legislator.[87]
This circumstance limits the significance of the regulation and it is a missed chance to complement the provisions of GDPR. Gaining access to the data is a good starting point for Users, but it does not significantly affect the EU market. Larger companies do not have an advantage only because of the mere fact that they are the only ones being able to access Users' data, but mostly because they have larger and better means to exploit that data without any control, including selling it to advertisers. While GDPR was able to limit these practices, even if not significantly, the Data Act fails to have the same impact.

11. Conclusion

The new proposal complements the legislative framework of the European Digital Strategy and confers to Users new rights, complementing those envisaged by GDPR. It is, in fact, shaped with a view of GDPR, of which it mimics the rights of access, right to portability, and the principles of transparency, purpose limitation, storage limitation, the limitations to international transfers, and the enforcement model. It also takes into account the principles of fairness, reasonableness and non-discrimination, extending them to the whole data sharing legal framework. Users are now empowered to obtain, port, and use the data they generate through IoT devices.
It is aimed at balancing the market and protecting consumers and smaller enterprises against the power of larger companies dominating the IoT field. To avoid claims of copyright infringement related to the IoT data, which could hinder the right of access, it modifies the Database Directive, excluding the application of the *sui generis* right. It also provides for a novel discipline of unfair clauses, previously limited to business-to-consumer relationships.
In addition, the right of access is extended to public sector bodies, as they are now able to directly request IoT data in case of exceptional need, and Data Holders have only limited grounds for refusing to disclose those data.
The proposal regulates cloud computing and smart contracts as well, providing for the first time some interoperability requirements.

[87] European Commission, *Study on the Economic Detriment to Small and Medium-Sized Enterprises Arising from Unfair and Unbalanced Cloud Computing Contracts*, 2018.

However, some issues still remain open, such as the fact that European standards for interoperability are still needed in order to obtain an effective enacting of the new provisions on cloud computing; the fact that there seems to be an imbalance between the provisions regarding Data Holders' trade secrets protection and those regarding Third Parties; the limited number of clauses deemed as unfair.
Lastly, the proposal does not go as far as fully regulating the way in which Data Holder can use Users' data, therefore failing to limit the true power of larger enterprises.
It is hoped that the upcoming revisions of the proposal will take all of these aspects into consideration.

Note a sentenza

Negazionismo: la Cassazione precisa i contorni dell'aggravante in linea con la giurisprudenza di Strasburgo

Marina Castellaneta

Corte di Cassazione, sez. I penale, 3 febbraio 2022, n. 3808

Il negazionismo è una forma di *hate speech* e se riguarda l'Olocausto non va considerata come libera manifestazione del pensiero ma come forma di discriminazione. La circostanza che atti di negazionismo siano perpetrati nella Giornata della Memoria indica l'esistenza dell'elemento psicologico e del dolo. È, quindi, applicabile l'aggravante del negazionismo in una situazione che corrisponde totalmente alla giurisprudenza della Corte europea dei diritti dell'uomo che, in più occasioni, ha chiarito che il negazionismo dell'Olocausto non rientra nella protezione accordata dalla Convenzione alla libertà di espressione.

Sommario

1. Premessa. - 2. La ricostruzione della vicenda. - 3. Il quadro normativo italiano in materia di negazionismo dell'Olocausto e la situazione in altri Stati. - 4. La continuità tra la conclusione della Cassazione e la giurisprudenza della Corte europea. - 5. Osservazioni conclusive.

Keywords

negazionismo – Convenzione ONU sull'eliminazione di ogni forma di discriminazione razziale - Giornata della Memoria – libertà di espressione – Corte europea dei diritti dell'uomo

1. Premessa

La diffusione dell'antisemitismo in tutta Europa, accompagnata dalla frequente impunità di coloro che compiono gesti di discriminazione e di odio nei confronti degli ebrei, come attestato nel rapporto sugli episodi di antisemitismo registrati nell'Unione europea tra il 2011-2021 diffuso il 3 novembre 2022 dall'Agenzia dell'Unione europea

per i diritti fondamentali[1], è stata connotata, negli ultimi anni, dal negazionismo della Shoah e finanche dell'esistenza delle camere a gas nei campi di concentramento[2]. Questo fenomeno, indice, come vedremo, di odio razziale, che mira a negare l'identità di singoli individui e di un gruppo, ha spinto l'Assemblea generale delle Nazioni Unite, con la risoluzione 76/250 sul negazionismo dell'Olocausto, adottata il 25 gennaio 2022, a intervenire per condannare il negazionismo e per chiedere agli Stati di reprimere questa pratica che va considerata illecita, assicurando la punizione dei colpevoli[3] e garantendo la preservazione dei luoghi della memoria, nonché educando le generazioni future sui fatti storici che hanno portato allo sterminio degli ebrei, anche al fine di impedire nuovi genocidi. La risoluzione, che evidenzia la necessità di non consentire che il negazionismo dell'Olocausto sia impunito, fornisce anche una nozione di negazionismo[4], inteso come ogni tentativo volto a negare una realtà storica e l'ampiezza dello sterminio degli ebrei, compresa la minimizzazione dei crimini nei confronti degli ebrei e affermazioni che addirittura indicano gli stessi ebrei come responsabili dell'Olocausto[5]. Nella risoluzione, preso atto della pericolosità per l'intera collettività dell'impunità diffusa anche a causa dell'utilizzo della tecnologia che permette maggiori possibilità di occultamento agli autori delle dichiarazioni negazioniste, si evidenzia il ruolo centrale degli organi giurisdizionali nazionali e l'urgenza di interventi in ragione della circostanza che questa forma di *hate speech* trova oggi diffusione ancora maggiore a causa dei *social media* che agevolano lo spargimento dei semi di violenza e di odio. Questo comporta, a nostro avviso, una pericolosità crescente anche in ragione della progressiva scomparsa dei sopravvissuti ai campi di sterminio che può portare a un affievolimento della memoria, indispensabile per impedire il ripetersi di questi crimini.

---

[1] Si tratta del rapporto *Overview of Antisemitic incidents recorded in the European Union – 2011-2021*, reperibile nel sito *fra.europa.eu*. Nel documento sono riportati i dati relativi agli episodi di antisemitismo nei Paesi membri. Per quanto riguarda l'Italia, si evidenzia che nel 2011 i casi registrati sono stati 23, saliti a 101 nel 2021. Dalla tabella n. 30 risulta che nel 2021 ci sono stati due arresti (nessuno nel 2020) e che le persone denunciate sono state 40 (erano 11 nel 2020 e 1 nel 2011).

[2] Cfr., tra gli altri, A. Pietrobon, *State Negationism and the Rule of Law*, in A. Gattini - R. Garciandia - P. Webb - E. Fronza (a cura di), *Human Dignity and International Law,* Leiden - Boston, 2021, 164 ss.; G. Sacerdoti, *Criminalizing Holocaust Denial: From International Standards to Domestic Implementation. The Case of Italy,* ivi, 154 ss.; E. Fronza, *Il negazionismo come reato,* Milano, 2012; M. Manetti, *Libertà di pensiero e negazionismo,* in M. Ainis (a cura di), *Informazione, potere, libertà,* Torino, 2008, 41 ss.; M. Castellaneta, *L'hate speech: da limite alla libertà di espressione a crimine contro l'umanità*, in G. Venturini - S. Bariatti (a cura di), *Diritti individuali e giustizia internazionale, Liber Fausto Pocar,* Milano, 2009, 157 ss.

[3] Il documento è reperibile nel sito *un.org*. In precedenza, era stata adottata la risoluzione 61/255 del 26 gennaio 2007. Su altri interventi sul piano internazionale si veda R. Sabel, *Anti-Semitism,* in *Max Planck Encyclopedias of International Law,* nel sito *opil.ouplaw.com.*

[4] Nel documento non vincolante dell'*International Holocaust Remembrance Alliance* (IHRA) si dichiara che il negazionismo è «l'affermazione propagandistica che nega la realtà storica e la portata dello sterminio degli ebrei» e che esso si riferisce «specificamente a qualunque tentativo teso a sostenere che l'Olocausto/Shoah non abbia avuto luogo», con l'obiettivo di «colpevolizzare gli ebrei e rendere di nuovo legittimo l'antisemitismo». Il documento è reperibile nel sito *holocaustremembrance.com.*

[5] Nel Preambolo si chiarisce che rientrano nel negazionismo dell'Olocausto, *«(a) Intentional efforts to excuse or minimize the impact of the Holocaust or its principal elements, including collaborators and allies of Nazi Germany, (b) Gross minimization of the number of the victims of the Holocaust in contradiction to reliable sources, (c) Attempts to blame the Jews for causing their own genocide, (d) Statements that cast the Holocaust as a positive historical event, (e) Attempts to blur the responsibility for the establishment of concentration and death camps devised and operated by Nazi Germany by putting blame on other nations or ethnic groups*».

In ragione della pericolosità di questo reato, l'Unione europea, che è stata scenario dell'Olocausto e del genocidio di Srebrenica[6], ha agito tempestivamente, optando per un intervento nel campo penale, considerato più efficace a combattere la diffusione di messaggi discriminatori, lesivi della dignità di ogni essere umano, in particolare con la decisione quadro 2008/913/GAI del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale[7]. Tuttavia, malgrado tale atto, nel rapporto annuale dell'Agenzia UE per i diritti fondamentali presentato l'8 giugno 2022[8] è stato sottolineato che in alcuni Stati l'indicata decisione quadro non ha portato alla criminalizzazione del diniego o della minimizzazione grossolana di crimini internazionali e dello stesso Olocausto. Anche il Parlamento europeo è intervenuto: con la risoluzione del 25 ottobre 2018 sull'aumento della violenza neofascista in Europa ha invitato gli Stati a condannare e a contrastare ogni forma di negazione dell'Olocausto «tra cui la banalizzazione e la minimizzazione dei crimini dei nazisti e dei loro collaboratori», evidenziando che «la verità sull'Olocausto non deve essere banalizzata dalla narrazione politica e mediatica»[9]. E, in questa direzione, il 5 ottobre 2021, per la prima volta, l'Unione europea ha adottato la "Strategia dell'UE sulla lotta contro l'antisemitismo e il sostegno alla vita ebraica (2021-2030)"[10], nella quale è stato sottolineato che anche i sistemi di intelligenza artificiale possono essere utilizzati per fronteggiare l'antisemitismo e la distorsione online dell'Olocausto. Nello stesso documento si evidenzia altresì che gli episodi di negazione, distorsione e di minimizzazione dell'Olocausto sono in aumento in tutta Europa e che questi atti sono utilizzati «per alimentare l'odio contro il popolo ebraico»[11]. La Commissione europea, inoltre, nella Comunicazione "Un'Europa più inclusiva e protettiva: estendere l'elenco

[6] Si veda S. Šarić, *The Denial of Genocide in Srebrenica in the Context of Strengthening Neo-fascism and Relativization of the Holocaust in Europe*, in *Bosnian Studies: Journal for research of Bosnian thought and culture,* 5, 2021, 66 ss.

[7] In *GUUE* L 328, 6 dicembre 2008, 55 ss. Nella direttiva 2012/29/UE del 25 ottobre 2012, che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI (in *GUUE* L 315, 14 novembre 2012, 57 ss., recepita in Italia con d.lgs. n. 212 del 15 dicembre 2015) le vittime di messaggi di incitamento all'odio sono incluse tra quelle particolarmente vulnerabili. La direttiva 2000/43/CE del 29 giugno 2000 che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica, invece, non si occupa del negazionismo: in *GUCE* L 180, 18 luglio 2000, 22 ss.

[8] Si veda anche la Comunicazione della Commissione del 18 settembre 2020 (COM (2020)565) intitolata *A Union of equality: EU anti-racism action plan 2020-2025*.

[9] P8_TA-Prov(2018)0428, nel sito *europarl.europa.eu*.

[10] COM(2021)615. In Italia, nel 2021 è stata elaborata la Strategia Nazionale per la lotta contro l'antisemitismo, in attuazione di quanto richiesto dal Consiglio dell'Unione europea nella Dichiarazione n. 13637/20 del 2 dicembre 2020. Nella Strategia si sottolinea che l'antisemitismo si può manifestare anche con il negazionismo, il revisionismo, il riduzionismo e la distorsione dell'Olocausto.

[11] Anche in Italia, per rafforzare la lotta all'antisemitismo, sono state adottate talune misure come l'istituzione del Coordinatore nazionale per la lotta contro l'antisemitismo presso la Presidenza del Consiglio dei Ministri, in conseguenza della risoluzione del Parlamento europeo del 1° giugno 2017 sulla lotta contro l'antisemitismo con la quale i deputati avevano chiesto agli Stati membri di nominare un Coordinatore nazionale (il 1° gennaio 2020 è stata nominata in Italia la professoressa Milena Santerini). È stata altresì istituita la Commissione straordinaria per il contrasto dei fenomeni di intolleranza, razzismo, antisemitismo, istigazione all'odio e alla violenza, presieduta dalla senatrice Liliana Segre, che ha pubblicato una relazione il 20 giugno 2022.

dei reati riconosciuti dall'UE all'incitamento all'odio e ai reati generati dall'odio"[12], ha rilevato, tra i problemi principali dell'*hate speech,* la rapida condivisione digitale e ha sottolineato la necessità di un ulteriore sviluppo rispetto alla decisione quadro 2008/913. In ragione dell'evoluzione dei fenomeni criminali, l'art. 83, par. 1, TFUE, dovrebbe portare a individuare ulteriori sfere di criminalità proprio con riguardo all'incitamento all'odio per assicurare protezione alle vittime e la punizione dei responsabili.

Un elemento che mostra la consapevolezza sul piano internazionale ed europeo della pericolosità ad ampio raggio delle dichiarazioni negazioniste o distorte dell'Olocausto si può rintracciare anche dall'intervento delle istituzioni internazionali sulle società private che gestiscono piattaforme sul web, in particolare attraverso iniziative come quelle dell'Unione europea che ha adottato, nel 2018, il codice di condotta sulla disinformazione con il quale gli operatori del settore hanno concordato su standard di autoregolamentazione e, il 16 giugno 2022, il codice di condotta rafforzato sulla disinformazione. Sono altresì rilevanti le iniziative individuali delle società private che operano attraverso i *social media*[13]. Ad esempio, Facebook nella revisione della propria politica per la lotta all'incitamento all'odio ha inserito, nel documento del 24 settembre 2020, tra i contenuti da non pubblicare inclusi nel "Livello 1" proprio le informazioni negazioniste o distorte sull'Olocausto, elemento che non era presente in precedenza[14].

In questo contesto, che mostra il ruolo di primo piano esercitato dall'azione penale si inserisce la sentenza n. 3808 della Corte di cassazione, resa dalla prima sezione penale il 3 febbraio 2022, con la quale, per la prima volta, a fronte della diffusione di idee fondate sulla superiorità e sull'odio razziale o etnico e della negazione della Shoah, diffusione avvenuta proprio il 27 gennaio 2017, Giorno della Memoria, è stata applicata ai responsabili l'aggravante speciale del negazionismo. La Suprema Corte, infatti, richiamando in più punti il diritto internazionale e la giurisprudenza della Corte europea dei diritti dell'uomo, ha confermato la pronuncia del Tribunale di Milano e poi della Corte di appello che avevano accertato la colpevolezza di un uomo, in concorso con ignoti, per violazione dell'art. 110 c.p.[15], nonché dell'art. 3-*bis* della legge n. 654 del 1975 (ora art. 604-*bis* c.p.)[16]. La Cassazione, come vedremo, ha respinto ogni giustificazione dell'imputato ammantata da una sorta di revisionismo scientifico della storia, precisando che la Shoah è stata provata in modo «definitivo e perciò incontrovertibile» con la liberazione da parte dell'Armata Rossa, il 27 gennaio 1945, del campo

[12] COM(2021)777.

[13] Si veda anche il codice di condotta per contrastare l'incitamento all'odio online voluto dalla Commissione europea, adottato nel 2016 e modificato a giugno 2022, reperibile nel sito nel sito *europa.eu*.

[14] Si veda il sito *transparency.fb.com*. Il negazionismo dell'Olocausto non era presente nelle versioni antecedenti come, ad esempio, nelle regole di agosto 2020.

[15] La norma si occupa del concorso di persone in un reato stabilendo che «Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita, salve le disposizioni degli articoli seguenti». Sulla sentenza si veda S. Gimigliano - A. Magrassi, È *negazionismo, non revisionismo: verità della memoria e memoria della verità,* in *dirittifondamentali.it,* 2, 2022, 104 ss.

[16] Cfr. E. Fronza, *L'introduzione dell'aggravante del negazionismo,* in *Diritto penale e processo*, 2017, 155 ss.; P. Caroli, *Aggravante di negazionismo e nuove condotte tipiche, ivi,* 2018, 605 ss.; M. Donini, *Negazionismo e protezione della memoria*, in *Sistema penale,* 2021, reperibile nel sito *sistemapenale.it*.; D. Pulitanò, *Di fronte al negazionismo e al discorso d'odio,* in *Diritto penale contemporaneo,* 4, 2015, 325 ss.

di concentramento di Auschwitz. Così la Cassazione, in relazione a fatti storicamente accertati, ha chiarito che «l'orrore e la follia omicida che erano stati scientificamente e metodicamente attuati in quegli anni per sterminare un popolo e gli oppositori del regime nazista» non possono in alcun modo essere negati, con la conseguenza che colui che lo fa agisce con un evidente dolo nel compimento di un atto discriminatorio.

2. La ricostruzione della vicenda

Prima di esaminare gli aspetti legati all'incidenza del diritto internazionale sulla decisione della Corte di Cassazione, è necessario ricostruire, seppure brevemente, la vicenda al centro della pronuncia della Suprema Corte.
Il ricorrente, aderente al movimento N.S.A.B. – M.L.N.S. (Movimento Nazional Socialista dei Lavoratori), il 27 gennaio 2017, Giorno della Memoria, istituito dalle Nazioni Unite con risoluzione 60/7 del 1° novembre 2005 e considerato uno strumento importante per la prevenzione del genocidio in forza del ricordo del più grave crimine commesso nella storia dell'umanità, aveva compiuto una serie di atti, come la distribuzione di volantini nelle vie del centro di Milano con scritte «che s'ispiravano al Nazional Socialismo, inneggiando alla superiorità della razza bianca contro ogni presenza di giudaismo in Europa, negando l'Olocausto ebraico»[17]. Le manifestazioni erano state particolarmente offensive e volte a negare l'Olocausto definendo come bugiarde le vittime con frasi oltraggiose come «Credi ancora a quel che insinua Pinocchio», volte a offendere le stesse vittime dell'Olocausto e i loro discendenti. Nell'abitazione dell'imputato erano stati trovati altri volantini inneggianti alla superiorità della razza bianca, ma questo fatto non era stato considerato penalmente rilevante perché il materiale non era stato diffuso. L'uomo era stato condannato a sei mesi di reclusione con il beneficio della sospensione condizionale della pena per il reato di concorso con ignoti nella diffusione di idee fondate sulla superiorità o sull'odio razziale o etnico e di negazione della Shoah.
Tra i motivi di ricorso in Cassazione, è stata sollevata dal ricorrente la questione relativa alla violazione dell'art. 10 della Convenzione europea dei diritti dell'uomo (in prosieguo anche CEDU) che assicura il diritto alla libertà di espressione[18]. In pratica, secondo l'imputato, la sua "opinione" era da tutelare anche perché l'esistenza della Shoah sarebbe stata contestata da numerosi studiosi e la sua negazione sarebbe supportata da studi di storici. L'uomo, inoltre, respingeva la necessità di fornire una particolare protezione alla Shoah che, a suo avviso, non sarebbe l'unico genocidio, tesi particolarmente priva di pregio visto che l'esistenza di altri genocidi non esclude che, proprio per le particolarità dell'Olocausto, la comunità internazionale intenda garantire una particolare protezione al ricordo di quel genocidio e che lo stesso legislatore

[17] Così la ricostruzione della Corte di Cassazione.

[18] Tra la sterminata bibliografia, si veda, per tutti, T. McGonagle, *Freedom of Expression and Defamation,* Strasbourg, 2016; M. Oetheimer - A. Cardone, *Art. 10*, in S. Bartole - P. De Sena - V. Zagrebelsky (a cura di), *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2012, 397 ss.

italiano avverta quest'esigenza proprio tenendo conto dell'alto numero di vittime italiane e dell'adozione, durante il periodo fascista, delle leggi razziali.
Nell'atto di ricorso, inoltre, è stato sostenuto che non è stato provato che l'imputato «abbia voluto diffondere un'idea che negasse l'Olocausto e non quella di criticare la ricostruzione storica ufficiale», con ciò evidentemente confermando che, nella visione dell'imputato, una realtà storica accertata possa essere rimessa in discussione senza alcun elemento di fatto.
Il ricorrente aveva così cercato di ammantare con una sorta di base storica la propria dichiarazione negazionista, non tenendo conto del fatto che non solo la Shoah è stata ampiamente dimostrata da storici, ma anche da tribunali internazionali come quello di Norimberga e da tribunali nazionali che hanno condannato gli autori dei crimini contro gli ebrei deportati nei campi di concentramento[19].

3. Il quadro normativo italiano in materia di negazionismo dell'Olocausto e la situazione in altri Stati

Come detto in premessa, la Corte di Cassazione ha applicato per la prima volta l'aggravante del negazionismo che s'inserisce in un quadro normativo interno costituito da un insieme di norme volte a punire l'*hate speech* e la discriminazione, in molte occasioni grazie all'attuazione di obblighi internazionali. È il caso, infatti, della Convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale adottata a New York il 7 marzo 1965, alla quale l'Italia ha dato esecuzione con la legge 13 ottobre 1975 n. 654 (nota come legge Mancino), con la quale è stata introdotta la fattispecie penale dell'incitamento all'odio e il reato di propaganda, istigazione e incitamento nei confronti di persone in quanto appartenenti a un determinato gruppo nazionale, etnico o razziale. In particolare, l'art. 3, nella sua versione originale, prevedeva la punizione di coloro che diffondono «in qualsiasi modo, idee fondate sulla superiorità o sull'odio razziale», nonché di coloro che «incitano alla discriminazione o a commettere atti di violenza o di provocazione alla violenza», con riguardo a persone appartenenti a un determinato gruppo nazionale, etnico o razziale. È stata altresì vietata ogni organizzazione o associazione avente tra i suoi scopi l'incitamento all'odio o alla discriminazione razziale ed è stata prevista la punizione per la partecipazione a tali organizzazioni, nonché per l'assistenza a queste attività[20]. Il quadro normativo è mutato a seguito dell'adozione della legge n. 205 del 1993 di conversione, con modificazioni, del d.l. n. 122/1993 "recante misure urgenti in materia di discriminazione razziale, etnica e religiosa"[21]. Un ulteriore passo è stato compiuto con la legge n. 115 del

[19] Si veda V.N. Dadrian, *The Historical and Legal Interconnections Between the Armenian Genocide and the Jewish Holocaust: From Impunity to Retributive Justice*, in *Yale Journal of International Law,* 1998, 504 ss.; D. Bloxham, *Genocide on Trial: The War Crimes Trials and the Formation of Holocaust History and Memory*, Oxford, 2001; M. Bazyler, *Holocaust, Genocide, and the Law: A Quest for Justice in a Post-Holocaust World*, Oxford, 2016.

[20] La pena prevista va da uno a cinque anni, con un aumento di pena «per i capi e i promotori di tali organizzazioni o associazioni».

[21] Tra le novità introdotte da tale modifica vi è la possibilità per le autorità giudiziarie di prevedere

2016 di modifica dell'art. 3 della legge n. 654/75, che ha portato all'aggiunta dell'art. 3-*bis* con il quale è disposta la «pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale, ratificato ai sensi della legge 12 luglio 1999, n. 232».

Per completezza, va altresì ricordato che, in epoca successiva ai fatti al centro della pronuncia della Corte di Cassazione, è stato adottato il d.lgs. n. 21 del 1° marzo 2018[22], con il quale, grazie all'art. 604-*bis* c.p. (Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa), è stato previsto, salvo i casi in cui il fatto costituisca un reato più grave, che sia punito: «a) con la reclusione fino ad un anno e sei mesi o con la multa fino a 6.000 euro chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi; b) con la reclusione da sei mesi a quattro anni chi, in qualsiasi modo, istiga a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi»[23]. Nell'art. 604-*ter* è stata inserita una circostanza aggravante per i reati punibili con pena diversa da quella dell'ergastolo commessi per finalità di discriminazione o di odio etnico, nazionale, razziale o religioso, ovvero al fine di agevolare l'attività di organizzazioni, associazioni, movimenti o gruppi che hanno tra i loro scopi le medesime finalità, con un aumento di pena fino alla metà[24]. A rafforzare la portata punitiva è intervenuta la legge 25 ottobre 2017 n. 163 "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017", con la quale, per assicurare la completa attuazione della decisione quadro 2008/913/GAI, tenendo conto che la stessa Commissione europea aveva evidenziato la lacune nell'ordinamento italiano[25], è stata modificata l'aggravante

sanzioni accessorie per uno dei reati previsti dall'art. 3 della legge 13 ottobre 1975, n. 654, o per uno dei reati previsti dalla legge 9 ottobre 1967, n. 962. Cfr., tra gli altri, M. Manetti, *Libertà di pensiero e negazionismo,* cit.; E. Fronza, *Il negazionismo come reato,* cit.

[22] Il testo è intitolato "Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'art. 1, comma 85, lettera q), della legge 23 giugno 2017, n. 103".

[23] È altresì «vietata ogni organizzazione, associazione, movimento o gruppo avente tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali o religiosi. Chi partecipa a tali organizzazioni, associazioni, movimenti o gruppi, o presta assistenza alla loro attività, è punito, per il solo fatto della partecipazione o dell'assistenza, con la reclusione da sei mesi a quattro anni. Coloro che promuovono o dirigono tali organizzazioni, associazioni, movimenti o gruppi sono puniti, per ciò solo, con la reclusione da uno a sei anni». Si applica la pena della reclusione da due a sei anni se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, come definiti dagli artt. 6, 7 e 8 dello statuto della Corte penale internazionale.

[24] Per quanto riguarda le circostanze attenuanti, diverse da quella prevista dall'art. 98, è stato stabilito che quelle «concorrenti con l'aggravante di cui al primo comma, non possono essere ritenute equivalenti o prevalenti rispetto a questa e le diminuzioni di pena si operano sulla quantità di pena risultante dall'aumento conseguente alla predetta aggravante».

[25] Si veda il rapporto della Commissione sull'attuazione della direttiva 2008/913, presentato il 27 gennaio 2014, COM(2014) 27, reperibile nel sito *europa.eu*.

del negazionismo aggiungendo i casi di minimizzazione grave o l'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità, dei crimini di guerra come stabiliti nello Statuto della Corte penale internazionale[26]. Inoltre, con tale legge è stato modificato il d.lgs. 8 giugno 2001, n. 231 con l'inserimento dell'art. 25-*terdecies* (Razzismo e xenofobia) in base al quale, nel caso di reati cui all'art. 3, c. 3-*bis* della legge n. 654/1975, è prevista una sanzione pecuniaria da duecento a ottocento quote per l'ente e, nei casi di condanna per i delitti di cui al c. 1, l'applicazione delle sanzioni interdittive previste dall'art. 9, c. 2, per una durata non inferiore a un anno. In aggiunta, se l'ente o una sua unità organizzativa sono stabilmente utilizzati allo scopo unico o prevalente «di consentire o agevolare la commissione dei delitti indicati nel comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16, comma 3»[27].

L'Italia, quindi, con l'introduzione dell'aggravante del negazionismo ha applicato in modo più corretto la decisione quadro 2008/913, prevedendo, tuttavia, che non sia sufficiente la sola negazione della Shoah, ma debba sussistere un pericolo concreto della diffusione di idee razziste, con un accertamento effettuato dal giudice. Il quadro normativo italiano, così, ha oggi colmato la lacuna rilevata da diversi anni, a partire dal caso del professore Moffa, che, nel corso di una lezione tenuta in un master dell'Università di Teramo il 25 settembre 2010, aveva negato l'esistenza dell'Olocausto[28]. A seguito di quella vicenda era stata invocata l'introduzione del reato di negazionismo[29]. Il percorso è stato lungo e, per arrivare a una conclusione positiva, è stata centrale l'adozione della decisione quadro 2008/913, che ha permesso un ravvicinamento tra le legislazioni degli Stati membri con la punizione del negazionismo anche in altri ordinamenti[30]. È opportuno ricordare, però, che rispetto all'atto Ue alcuni Paesi già in precedenza avevano adottato norme penali per reprimere il negazionismo. Si possono ricordare l'Austria[31], la Germania[32], la quale con una sentenza della Corte costituzio-

[26] In senso critico rispetto all'ampliamento degli «spazi di rilevanza penale del negazionismo nell'ordinamento interno», si veda C.D. Leotta, *Negazionismo, Dig. Disc. Pen., Aggiornamento,* X, 2018, 476 ss.

[27] Per alcune osservazioni critiche sull'introduzione del negazionismo tra i reati presupposto della responsabilità della persona giuridica si veda A. Galluccio, *Modificata l'aggravante di negazionismo e inserito l'art. 3 C.3-bis L. 654/1975 nel novero dei reati presupposto ex D.lgs. 231/2001,* in *Dir. pen. contemporaneo,* 2017, nel sito *archiviodpc.dirittopenaleuomo.org.*

[28] Si rinvia a M. Castellaneta, *La repressione del negazionismo e la giurisprudenza della Corte europea dei diritti dell'uomo*, in *Diritti umani e diritto internazionale,* 2011, 65 ss.

[29] La richiesta era stata presentata dal Presidente della Comunità ebraica di Roma, Riccardo Pacifici. In senso contrario si era espresso S. Luzzatto, *Shoah vera o falsa? Non si decide per legge,* in *Il Sole 24 Ore,* 17 ottobre 2010, 11, che invocava interventi sul piano culturale e sociale e non attraverso la via giudiziaria.

[30] Per un quadro delle legislazioni di alcuni Stati membri Ue, cfr. il documento del Parlamento europeo *Holocaust denial in criminal law*, a cura di P. Bakowski, PE 698.043, gennaio 2022. Si veda anche A. Gliszczyńska-Grabias, *Penalizing Holocaust Denial: A View from Europe*, in *Global Antisemitism: A Crisis of Modernity*, Leiden, 2013, 237 ss., nonché M.J. Bazyler, *Holocaust Denial Laws and Other Legislation Criminalizing Promotion of Nazism*, reperibile nel sito *yadvashem.org.*

[31] In Austria era stato adottato il *National Socialism Prohibition Act* dell'8 maggio 1945, modificato dalla legge 26 febbraio 1992. Sulla legislazione austriaca si veda F. Müller, *The Nazi Prohibition Act in Relation to Freedom of Speech,* reperibile nel sito internet *etudes-europeennes.fr*, 12(1).

[32] Si veda la legge 23 ottobre 1994 reperibile nel sito *bgbl.de.* Già, in precedenza, in via interpretativa,

nale del 1994 relativa al caso dello storico David Irving ha chiarito che il diniego dell'esistenza dell'Olocausto non gode della protezione accordata nell'ambito dell'esercizio del diritto alla libertà di espressione e costituisce un reato[33]; la Francia, con la legge Gayssott n. 90-615 del 13 luglio 1990[34]; la Repubblica ceca che con le modifiche al codice penale in vigore dal 1° gennaio 2010 ha inserito il reato di negazionismo dell'Olocausto e poi ha ampliato questa fattispecie anche ai casi di altri crimini commessi durante il periodo nazista e comunista; la Polonia, con l'art. 55 ha introdotto il reato attraverso la legge che istituisce l'Istituto della memoria nazionale del 18 dicembre 1998[35]; l'Ungheria il 24 luglio 2010 ha disposto un emendamento al codice penale che punisce il negazionismo con riferimento al genocidio, a crimini contro l'umanità, anche quando commessi durante il regime comunista; la Lituania, con modifiche all'art. 170 c.p. introdotte nel 2009; il Lussemburgo con l'art. 457-3 c.p. che è stato modificato nel 2011 con la legge di attuazione della direttiva 2008/913; il Liechtenstein con l'art. 283; il Belgio secondo la legge 23 marzo 1995 ("*Belgian Holocaust denial law*") che ha innovato l'art. 444 c.p.[36]. Modifiche in questa direzione sono state introdotte anche in Danimarca, grazie alla ratifica del Protocollo alla Convenzione sul cybercrime del 21 novembre 2001, in vigore dal 1° luglio 2004. Il Protocollo del 28 gennaio 2003, entrato in vigore il 1° marzo 2006, riguardante la criminalizzazione di atti dal contenuto razzista o xenofobo attraverso i sistemi informatici richiede che gli Stati puniscano in sede penale gli autori in relazione a casi «*which denies, grossly minimises, approves or justifies act constituting genocide or crimes against humanity*» come definiti dal diritto internazionale, dal Tribunale di Norimberga o da altri tribunali internazionali. Questo ha condotto a cambiamenti del codice penale anche in Lettonia, proprio a seguito della ratifica del suddetto Protocollo, così come a Cipro. Altre modifiche sono intervenute in Portogallo (art. 240 c.p.); in Romania (legge n. 31 del 13 marzo 2002); in Slovacchia secondo la legge 300/2005, che ha modificato l'art. 422 c.p.; in Slovenia con novità introdotte nel 2008 all'art. 297 c.p.; in Grecia il negazionismo che riguarda l'Olocausto è punito con la legge n.

era possibile utilizzare altre norme volte a tutelare la dignità che permettevano una punizione del negazionismo. Cfr. E. Stein, *History against free speech: the new German law against the "Auschwitz" – and other – "lies"*, in *Michigan Law Review* 1986, 277 ss.; D. Grimm, *The Holocaust Denial Decision of the Federal Constitutional Court of Germany,* in I. Hare - J. Weinstein (a cura di), *Extreme Speech and Democracy*, Oxford, 2009, 557 ss.

[33] Cfr. R. Kahn, *Cross-Burning, Holocaust Denial, and the Development of Hate Speech Law in the United States and Germany*, in *University of Detroit Mercy Law Review,* 2006, 163 ss.; C. Haupt, *Regulating Hate Speech-Damned if you do and Damned if you don't: Lessons Learned from Comparing the German and U.S. Approaches*, in *Boston University International Law Journal,* 2005, 299 ss.

[34] Con l'indicata legge sono state introdotte modifiche alla normativa sulla libertà di stampa del 29 luglio 1881, che classifica come reato la contestazione dell'esistenza dei crimini contro l'umanità durante il nazismo. In base a tale legge, i tribunali francesi hanno condannato, l'8 febbraio 2008, Jean-Marie Le Pen, il quale sosteneva che l'occupazione dei nazisti in Francia non era stata particolarmente disumana, negando le persecuzioni subite dagli ebrei. Si veda quanto riportato nel sito *jurist.law.pitt.edu*. Il Presidente del Fronte nazionale, in precedenza, era stato condannato, il 2 aprile 2004, dal tribunale penale di Parigi, per incitamento all'odio razziale nei confronti dei musulmani.

[35] La Polonia, tuttavia, limita il reato di negazionismo solo ai casi in cui tale reato sia commesso a danno di cittadini polacchi (si veda il rapporto annuale dell'Agenzia europea dei diritti fondamentali del 2022).

[36] La legge è stata modificata nel 1999. Cfr. M. Whine, *Expanding Holocaust Denial and Legislation Against It*, in in I. Hare - J. Weinstein (a cura di), *Extreme Speech and Democracy*, cit., 538 ss.

927/1999, modificata, per quanto riguarda l'entità delle sanzioni, in diverse occasioni. Accanto, però, agli interventi legislativi volti a punire il negazionismo dell'Olocausto e di altri crimini contro l'umanità accertati dalla storia, va evidenziata la tensione tra tale divieto e il diritto alla libertà di espressione, aspetto che è venuto in rilievo anche nella sentenza della Corte di Cassazione che qui si commenta. Basti pensare, in questa direzione, alla situazione in Spagna: nel Paese il negazionismo era punito e vietato dall'art. 607 c.p., ma a seguito della sentenza della Corte costituzionale n. 235 del 7 novembre 2007, che ha ritenuto la norma in contrasto con la libertà di espressione, è stata introdotta una modifica con la legge n. 1/2015 prevedendo che il diniego del genocidio deve essere affiancato dall'incitamento diretto all'odio. In direzione analoga, in Francia, il disegno di legge n. 3957, di modifica della legge 2001-70 del 29 gennaio 2001 sul riconoscimento del genocidio degli armeni che conteneva l'inserimento di una norma in base alla quale «*La négation ou contestation du génocide arménien de 1915, dans des conditions fixées par décret pris en Conseil d'État, est passible d'une peine d'un an d'emprisonnement et de 45 000 € d'amende*»[37], non è stato approvato perché la Corte costituzionale, con sentenza del 28 febbraio 2012, n. 2012-647, ha considerato la norma contraria al diritto alla libertà di espressione[38].

Nonostante questi rallentamenti nell'affermazione su ampia scala del reato del negazionismo, sono pochi gli Stati nei quali non vi è una specifica previsione del reato del negazionismo o di un'aggravante[39] e, quindi, dal quadro delineato risulta che ormai esiste un consenso degli Stati circa la classificazione del negazionismo come forma di incitamento all'odio e alla discriminazione, con la conseguenza che in quanto atto di *hate speech* non può godere della protezione offerta dal diritto alla libertà di espressione proprio perché – come osservato anche dalla Corte di Cassazione con la sentenza n. 3808 che, come vedremo, aderisce alle conclusioni della Corte europea – «è indubitabile che esiste un legame di continuità tra la politica nazista di occultamento delle prove del genocidio, come accertata dalle truppe alleate alla fine della Seconda guerra mondiale, e le attività di alcuni autori (che si definiscono storici) che tentano di convincere il mondo che la Shoah sia la grande impostura del ventesimo secolo».

4. I chiarimenti della Cassazione sull'applicazione dell'aggravante del negazionismo e il filo diretto con la Corte europea dei diritti dell'uomo

La sentenza della Corte di Cassazione, oltre a chiarire il percorso seguito dalla Corte europea dei diritti dell'uomo in materia di negazionismo e a stabilire la corretta applicazione sul piano interno, che era contestata dal ricorrente, fornisce chiarimenti sui parametri necessari per applicare l'aggravante del negazionismo. A tale riguardo,

[37] In *assemblee-nationale.fr*.

[38] La pronuncia è reperibile nel sito *conseil-constitutionnel.fr*.

[39] Bulgaria, Estonia, Finlandia, Irlanda, Malta, Paesi Bassi, Svezia e Regno Unito hanno, infatti, nel proprio ordinamento, norme volte a punire l'incitamento all'odio o alla discriminazione razziale, ma non disposizioni che considerino reato il negazionismo.

la Cassazione ha respinto la tesi del ricorrente secondo il quale nella sua azione era assente l'elemento di propaganda discriminatoria e di negazione della Shoah. Ed invero, la Corte ha condiviso l'operato dei giudici di merito i quali hanno considerato in modo distinto il rinvenimento di numerosi volantini nell'abitazione del ricorrente che, poiché non diffusi pubblicamente, non potevano rientrare nella fattispecie penale di cui all'art. 604-*bis* (Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa) nella parte in cui esso prevede la reclusione da due a sei anni «se la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concreto pericolo di diffusione, si fondano in tutto o in parte sulla negazione, sulla minimizzazione in modo grave o sull'apologia della Shoah…», rispetto, invece, all'altro atto caratterizzato dall'effettiva diffusione nelle vie di Milano. Effettivamente, nel primo caso, non solo manca l'elemento esteriore della dichiarazione negazionista ma, a nostro avviso, anche il pericolo di diffusione tenendo conto che erano stati ritrovati nell'abitazione e non mentre l'uomo era fuori casa. È stata diversa, correttamente, la conclusione per la condotta legata alla diffusione di alcuni volantini che, nel caso di specie, era stata particolarmente pericolosa proprio perché l'uomo li aveva distribuiti o affissi in città, in luoghi altamente abitati, amplificandone la divulgazione.

Con riguardo al dolo, la Corte di Cassazione ha precisato che l'art. 3, c. 1, lett. *a*) della legge n. 654/1975 configura un reato a dolo generico e che, nel caso in esame, elementi che attestano l'esistenza del dolo sono da rinvenire anche nella scelta dell'imputato di compiere le condotte di cui era accusato nel Giorno della Memoria e, dunque "in pieno e sordo contrasto con una specifica previsione normativa che ha istituito tale momento di ricordo". La previsione normativa che ha disposto la celebrazione di tale giorno «è cristallina nel precetto, maieutica nel metodo e didattica nei mezzi», tanto più che in ragione dell'età dell'imputato era evidente che lo scopo e il senso del Giorno della Memoria gli fossero ben noti[40].

Nel caso in esame, l'uomo aveva inteso amplificare la portata discriminatoria proprio scegliendo il Giorno della Memoria come data per la diffusione, aspetto che mostra la volontà di colpire la dignità di un determinato gruppo e diffondere l'antisemitismo attraverso la distorsione della storia, senza alcun fondamento scientifico e storico, come attestato anche dall'alto numero di Stati che individuano il reato di negazionismo e dalle sentenze della Corte europea dei diritti dell'uomo. In questo senso, la Corte di Cassazione ha respinto i giochi di parole che portano gli autori di queste idee discriminatorie a non qualificarsi come negazionisti – quali in effetti sono – ma come revisionisti. In realtà, la negazione di una verità storica come l'Olocausto non ha alcuna base fattuale e ha un'evidente finalità offensiva e di incitamento all'odio verso un determinato gruppo.

Nel valutare l'elemento del dolo, i giudici di merito, inoltre, hanno tenuto conto del comportamento del ricorrente il quale, come dimostrato nel corso del processo, aderiva ad idee discriminatorie e negazioniste, seppure da lui qualificate nel contesto del revisionismo storico. Ci sembra opportuno sottolineare che, sul punto, l'iter seguito dalla Cassazione è analogo a quello di recente prospettato dalla Corte europea dei dirit-

[40] Per la Suprema Corte, l'uomo «ha preferito rifiutare ostinatamente quanto gli era stato insegnato, deliberatamente disponendosi a negare l'Olocausto ebraico».

ti dell'uomo nella sentenza *Zemmour c. Francia*[41], depositata il 20 dicembre 2022, con la quale la Corte di Strasburgo, precisato che la Convenzione non riconosce alcuna protezione ai discorsi che sostengono o giustificano la violenza, l'odio, la xenofobia o altre forme di intolleranza, tra i quali vi sono le dichiarazioni con finalità discriminatorie, ha valutato, per accertare l'intenzionalità del ricorrente, che l'uomo politico, condannato dai giudici francesi per aver incitato alla discriminazione nei confronti dei musulmani, avesse utilizzato una trasmissione televisiva in prima serata, con un'evidente volontà di divulgare il messaggio su larga scala e verso un vasto pubblico.

Con riguardo alla giurisprudenza della Corte europea relativa alla pronuncia n. 3808, è da rilevare che il ricorrente nel giudizio italiano aveva sostenuto che i giudici di merito avessero violato l'art. 10 della Convenzione non interpretando correttamente la norma. La Cassazione ha respinto questa tesi sostenendo che, in realtà, era il ricorrente ad avere interpretato in modo non corretto la giurisprudenza internazionale. Ed invero, la Corte di Strasburgo ha svolto in passato e continua a svolgere, anche con riguardo all'utilizzo di nuovi mezzi di comunicazione attraverso il web che presentano una pericolosità maggiore nel caso di diffusione di messaggi d'odio, un ruolo centrale nell'individuazione di una linea di demarcazione tra libertà di espressione e posizioni negazioniste, chiarendo i casi in cui dette tesi possono essere classificate come abuso di diritto (art. 17 della Convenzione) o come manifestazioni che non rientrano nel perimetro della libertà di espressione (art. 10), con la conseguenza che è conforme al quadro convenzionale l'adozione, da parte degli Stati, di interventi normativi punitivi[42]. In numerose occasioni, infatti, la Corte ha considerato le "opinioni" negazioniste tra quelle che possono – e finanche devono - giustificare una limitazione al diritto alla libertà di espressione[43], respingendo i ricorsi di coloro che ritenevano di essere stati lesi nel proprio diritto alla libertà di espressione. In taluni casi, la Corte ha precisato che queste manifestazioni d'odio non rientrano neanche nel diritto alla libertà di espressione, configurandosi piuttosto come ipotesi di abuso del diritto. Le dichiarazioni negazioniste di crimini come l'Olocausto e il comportamento di chi le diffonde sono stati collocati, in diverse occasioni, nel perimetro dell'art. 17 il quale stabilisce che nessuna disposizione della Convenzione, inclusa, quindi, la norma che tutela la libertà di espressione (art. 10), può essere interpretata in modo tale da includere il diritto a compiere un'attività o un atto che mira alla distruzione dei diritti e delle libertà convenzionali.

Nella sua giurisprudenza, la Corte ha considerato non solo legittimo ma anche neces-

[41] Ric. 63539/19.

[42] Come sottolineato da P. Lobba, *Holocaust Denial before the European Court of Human Rights: Evolution of an Exceptional Regime,* in *European Journal of International Law*, 2015, 237 ss., la Corte europea ha avuto diverse fasi nel giudicare i casi relativi al diniego dell'Olocausto, ma «*all applications about Holocaust denial have been invariably (and unanimously) dismissed as inadmissible*». In una prima fase, ricorda l'autore, in particolare nel caso *Lowes c. Regno Unito*, ric. 13214/87, decisione del 9 novembre 1988, non fu effettuato un richiamo all'applicazione dell'art. 17 della Convenzione, mentre successivamente la Corte ha iniziato ad applicare l'art. 17 come principio di interpretazione, in particolare dal caso *Kühnen c. Germania*, ric. 12194/86, decisione del 12 maggio 1988. Successivamente, ad avviso dell'autore, nella terza fase, l'art. 17 è stato utilizzato come causa di esclusione dalla protezione dell'art. 10 della Convenzione.

[43] Sull'*hate speech* si v. I. Hare, *Extreme Speech Under International and Regional Human Rights Standards,* in in I. Hare - J. Weinstein (a cura di), *Extreme Speech and Democracy*, cit., 62 ss.; A. Weber, *Manual on hate speech,* Strasbourg, 2009.

sario un intervento degli Stati funzionale a limitare la libertà di espressione nei casi di manifestazione di odio, con la previsione di sanzioni nei confronti di coloro che negano crimini come l'Olocausto e l'inserimento, nel proprio ordinamento, di norme penali *ad hoc*. In un primo tempo, il richiamo all'art. 17 è stato effettuato in rapporto alle dichiarazioni espresse contro gli ebrei. La Francia è stata uno dei primi Paesi a stabilire, con la legge *Gayssot*, norme penali sul negazionismo: la Corte europea, con la decisione *Garaudy c. Francia* del 24 giugno 2003[44] ha respinto il ricorso di uno scrittore francese, il quale sosteneva che il numero delle vittime dell'Olocausto non era stato elevato, mettendo in dubbio anche il piano nazista relativo alla cosiddetta "soluzione finale". La Corte, a fronte delle contestazioni dell'uomo il quale sosteneva che i giudici interni avevano violato l'art. 10 della Convenzione, ha disposto l'applicazione dell'art. 17 della Convenzione in base al quale, come detto, le norme convenzionali non possono essere utilizzate o interpretate per attività o per compiere atti che portano alla «distruzione dei diritti o delle libertà riconosciute nella presente Convenzione», osservando che la negazione di fatti storici chiaramente accertati come l'Olocausto non è in alcun modo espressione di un lavoro di ricerca storica, funzionale a un accertamento della verità, quanto piuttosto un modo per riabilitare il nazionalsocialismo nel periodo della Seconda guerra mondiale e di accusare le stesse vittime di falsificazione della realtà[45]. Proprio la negazione dei crimini contro l'umanità perpetrati durante il nazismo è considerata come una delle forme più gravi di diffamazione nei confronti degli ebrei, in grado di minare la lotta all'antisemitismo e di compromettere l'ordine pubblico, in modo incompatibile con i valori di una democrazia[46]. Con tali affermazioni la Corte esclude ogni possibilità di protezione alle dichiarazioni negazioniste, talvolta ammantate da una sorta di scientificità con un'auto-qualificazione da parte degli autori di queste dichiarazioni come appartenenti al dibattito storico e al revisionismo. Il cammino della Corte europea è proseguito in questa direzione. Poco dopo, con la decisione del 2 settembre 2004 nel caso *W.P. e altri c. Polonia, l*a Corte ha rilevato che i ricorrenti, ai quali era stata negata la costituzione di un'associazione da parte delle autorità polacche, non potessero invocare la Convenzione e, in particolare l'art. 11 che garantisce il diritto di associazione, anche in forza dell'art. 17 in virtù della circostanza che l'associazione da loro fondata e i toni usati «*can be seen as reviving anti-Semitism*», tanto più che il comportamento razzista dei ricorrenti «*also transpire from the anti-Semitic tenor of some of their*

[44] Ric. 65831/01. La Cassazione cita, in realtà, la sentenza *Garaudy c. Francia* del 1998 che, però, non risulta presente.

[45] La Corte ha affermato: «*Il ne fait aucun doute que contester la réalité de faits historiques clairement établis, tels que l'Holocauste, comme le fait le requérant dans son ouvrage, ne relève en aucune manière d'un travail de recherche historique s'apparentant à une quête de la vérité. L'objectif et l'aboutissement d'une telle démarche sont totalement différents, car il s'agit en fait de réhabiliter le régime national-socialiste, et, par voie de conséquence, d'accuser de falsification de l'histoire les victimes elles-mêmes*».

[46] Nella decisione indicata la Corte ha precisato: «*Apparaît comme l'une des formes les plus aiguës de diffamation raciale envers les Juifs et d'incitation à la haine à leur égard. La négation ou la révision de faits historiques de ce type remettent en cause les valeurs qui fondent la lutte contre le racisme et l'antisémitisme et sont de nature à troubler gravement l'ordre public. Portant atteinte aux droits d'autrui, de tels actes sont incompatibles avec la démocratie et les droits de l'homme et leurs auteurs visent incontestablement des objectifs du type de ceux prohibés par l'article 17 de la Convention*». Cfr. M. Levinet, *La fermeté bienvenue de la Cour européenne des droits de l'homme face au négationnisme,* in *Revue trimestrielle des droits de l'homme,* 2004, 653 ss.; S. Giordano, *La repressione legale del negazionismo storico nella giurisprudenza della Corte europea dei diritti dell'uomo,* in *Pace diritti umani*, 2, 2006, 83 ss.

submissions made before the Court»[47]. Quest'orientamento è continuato con la decisione del 20 febbraio 2007 (*Ivanov c. Russia*[48]), con la quale la Corte ha dichiarato irricevibile il ricorso del direttore di un giornale russo (condannato dai giudici interni), che aveva scritto diversi articoli indicando gli ebrei come fonte di pericolo in Russia, negando l'esistenza di ogni diritto alla loro dignità e negando l'esistenza dell'Olocausto, con una giustificazione della politica pro-Nazismo. Per la Corte europea, considerando il chiaro tenore antisemita degli articoli e l'incitamento all'odio nei confronti di un gruppo da essi provocato, il ricorrente, in forza dell'art. 17, non poteva beneficiare della protezione concessa in base all'art. 10 della Convenzione in quanto le sue dichiarazioni erano in contrasto con valori fondamentali come la tolleranza, la pace sociale e la non discriminazione, prescindendo, quindi, da una valutazione del contesto[49].

Anche in diverse sentenze, la Corte ha messo in risalto la particolare gravità del negazionismo dell'Olocausto come forma di discriminazione, di lesione della dignità umana e incitamento indiretto all'odio razziale applicando l'art. 17. Invece, pur con qualche eccezione, nei casi di negazione di altri crimini contro l'umanità, pure accertati dalla storia, la Corte ha fatto leva sui limiti al diritto alla libertà di espressione presenti nell'art. 10. A tal proposito si può ricordare la sentenza *Fatullayev c. Azerbaijan* del 22 aprile 2010[50], nella quale la Corte ha affermato l'inapplicabilità dell'art. 17 perché non si trattava di negazionismo relativo a «*clearly established historical facts such as the Holocaust*»[51], mentre con la decisione del 31 gennaio 2019 nel caso *Williamson c. Germania*[52], la Corte di Strasburgo, con specifico riferimento a una norma tedesca che proibisce con una sanzione penale il negazionismo dell'Olocausto ha ritenuto applicabile l'art. 17[53], senza procedere a una valutazione del contesto – come invece avviene nell'applicazione dei limiti di cui all'art. 10[54] -, con ciò evidenziando la particolare gravità delle tesi negazio-

47 Ric. 42264/08.

48 Ric. 35222/04.

49 La Grande Camera, invece, ha escluso, nel caso *Perinçek c. Svizzera*, ric. 27510/08, del 15 ottobre 2015 che in quel caso trovasse applicazione l'art. 17, che va richiamato in situazioni eccezionali e in ipotesi estreme.

50 Ric. 40984/07.

51 Del pari, nella sentenza *Bingöl c. Turchia*, ric. 36141/04, del 22 giugno 2010, la Corte non ha ritenuto applicabile l'art. 17 – come richiedeva la Turchia – ritenendo, invece, che la condanna per *hate speech* di un uomo politico che aveva criticato il Governo con riferimento alla questione curda, fosse una violazione dell'art. 10.

52 Ric. 64496/17.

53 Il caso riguardava dichiarazioni trasmesse in via principale in un altro Stato (Svezia), pur essendo poi accessibili in Germania con il sistema di *video-on-demand* o su un canale a pagamento.

54 Cfr. M. Castellaneta, *La repressione del negazionismo e la giurisprudenza della Corte europea dei diritti dell'uomo*, cit., nonché la sentenza del 4 dicembre 2003, *Gündüz c. Turchia* (ric. 35071/97), in cui la Corte ha chiarito che le dichiarazioni dal contenuto discriminatorio sono da classificare come incitamento all'odio solo se rese in un contesto nel quale i discorsi di tal genere sono in grado di produrre gli effetti voluti. Del pari, nella decisione sull'irricevibilità del ricorso presentato il 7 maggio 2010 (ric. 18788/09) da Jean-Marie Le Pen contro la Francia, a seguito della condanna subita per decisione dei tribunali nazionali per incitamento all'odio e alla discriminazione, la Corte ha valutato le dichiarazioni del ricorrente ritenendo che esse, in astratto, godevano della protezione di cui all'art. 10, ma che, nel caso di specie, proprio analizzando il contesto, erano in grado di suscitare un forte sentimento di ostilità nei confronti della comunità musulmana.

niste della Shoah. Va anche sottolineato che, di converso, la Corte mostra di rafforzare il diritto alla libertà di espressione di coloro che contestano le opinioni dei negazionisti. Ad esempio, nella sentenza del 1° dicembre 2009, *Karsai c. Ungheria*[55], la Corte ha accolto il ricorso di uno storico che aveva pubblicato un articolo su un settimanale di attualità nel quale aveva criticato la stampa di destra accusata di sostenere l'iniziativa di alcuni politici per la costruzione di una statua per celebrare la figura di Teleki, ex primo ministro ungherese durante la Seconda guerra mondiale, autore di numerose leggi antisemite. La statua, ad avviso dello storico, era un modo per esprimere tesi revisioniste, volte a negare fatti storici commessi durante la Seconda guerra mondiale, con la conseguenza che l'uomo, condannato a causa di un articolo fortemente critico verso il revisionismo del ruolo dell'ex primo ministro ungherese e l'apologia dei suoi atti volti a realizzare «un piano di attacco agli ebrei», usufruiva di una tutela più ampia della libertà di espressione.

Alla luce di questa breve analisi, ci sembra si possa concludere che la Cassazione abbia seguito i criteri individuati dalla Corte europea che, nel complesso, si sostanziano nell'escludere dalla protezione dell'art. 10 le dichiarazioni offensive dell'Olocausto, come avvenuto nella sentenza *Peta Deutschland c. Germania* dell'8 novembre 2012 e nel considerare di maggiore gravità le tesi negazioniste per le quali è applicabile non solo l'art. 10 (con riguardo ai limiti alla libertà di espressione necessari in una società democratica), ma finanche l'art. 17 che, in sostanza, porta a ritenere le tesi negazioniste come lesive dei valori democratici e convenzionali nel suo complesso, in grado di istigare comportamenti discriminatori[56]. Un orientamento che, a nostro avviso, potrebbe portare a ritenere che nei casi di negazionismo sia ormai richiesto un intervento punitivo nell'ambito penale non solo in base alla decisione quadro 2008/913/GAI, ma anche in base alle fonti internazionali inclusa la giurisprudenza della Corte europea dei diritti dell'uomo.

5. Osservazioni conclusive

La pronuncia della Corte di Cassazione, oltre a indicare una piena adesione alla giurisprudenza della Corte europea dei diritti dell'uomo che, da anni, considera il negazionismo in particolare dell'Olocausto come una forma di *hate speech* che ha evidenti finalità discriminatorie, individua l'importanza dei fattori necessari per punire questi reati sul piano interno. In particolare, infatti, la Cassazione ha escluso la rilevanza penale della condotta che consiste nella mera detenzione dei volantini in un'abitazione privata, mentre ha considerato come penalmente rilevante la condotta dell'affissione e la distribuzione di volantini sulle vie pubbliche. Questo ci sembra costituisca un giusto bilanciamento tra limiti alla libertà di espressione e divieto di discriminazione proprio perché è la diffusione dei messaggi discriminatori e di odio a far assumere rilevanza penale a un determinato comportamento. La diffusione del volantino (o il rischio di diffusione che, a nostro avviso, alla luce della sentenza potrebbe configurarsi solo se

[55] Ric. 5380/07.

[56] Si vedano i casi indicati nel par. 4 e, in particolare, la decisione Garaudy (vedi *supra,* nota 44).

un individuo possiede i volantini in luoghi pubblici) o di una dichiarazione negazionista si sostanziano così in atti di propaganda discriminatoria e razzista equiparabili ad atti di *hate speech*. È da segnalare che correttamente la Cassazione non ha ritenuto necessaria, per la configurazione del reato, l'effettiva realizzazione di altri atti materiali nei confronti dei soggetti al centro dei messaggi discriminatori, con ciò sottolineando la gravità in sé della diffusione dei messaggi d'odio. Il negazionismo, quindi, è una forma di *hate speech* da punire in modo analogo alle azioni di incitamento diretto, tendenza che si riscontra anche sul piano internazionale e negli ordinamenti di altri Stati[57]. La scelta di inserire e applicare l'aggravante nel caso di negazionismo e di non prevedere in modo autonomo il fatto di negare in sé, richiedendo invece la diffusione (o il pericolo di diffusione) e la propaganda, ci sembra in linea con l'art. 4 della Convenzione sull'eliminazione di ogni forma di discriminazione razziale, dalla quale ha origine la legge n. 654/1975 in cui è chiesto agli Stati di sradicare ogni forma di incitamento o ogni forma di *disseminazione* di idee basate sulla superiorità razziale. Da un lato, quindi, l'introduzione dell'aggravante corrisponde alla richiesta dell'Assemblea generale delle Nazioni Unite che, nella risoluzione del 7 ottobre 2022 (A/77/512), ha dato seguito alle proposte del Relatore speciale sulle forme contemporanee di razzismo, discriminazione razziale, xenofobia e intolleranza, e ha richiesto agli Stati (e anche alle società che gestiscono i *social media*), proprio per combattere la glorificazione del nazismo, un forte impegno per arginare l'incremento di crimini di odio e di incitamento alla violenza nei confronti di un determinato gruppo; dall'altro lato, richiedendo un'esternazione dei messaggi negazionisti pone un argine a eccessive limitazioni della libertà di espressione. Non si può dire che la previsione della disseminazione intacchi la punizione dei negazionisti dell'Olocausto, perché sul punto basti considerare che nella stessa risoluzione dell'Assemblea generale si pone in primo piano l'aspetto della diffusione (che è anche un elemento della disinformazione) e che, come ricordato dal Relatore speciale, anche in Armenia, Paese molto attento a impedire il negazionismo dei genocidi, nel nuovo codice penale in vigore dal 1° luglio 2022, all'art. 329 si considera come reato l'incitamento alla violenza e alla discriminazione e all'art. 330 si punisce la distribuzione di materiale funzionale a tale scopo[58].

Ci sembra, quindi, che la sentenza della Corte di Cassazione mostri che, nel suo concreto operare, l'aggravante del negazionismo sia in grado di raggiungere il risultato di vietare forme di negazionismo che se all'interno delle mura domestiche non possono produrre effetti di discriminazione e di odio verso determinati gruppi, se realizzate all'esterno sono correttamente punite nei casi in cui si realizzi la diffusione, ad esem-

[57] Il negazionismo si è posto anche con riguardo ad altri genocidi come quello in Ruanda. A tale riguardo, si può ricordare l'arresto di un avvocato statunitense, Peter Erlinder, impegnato in diversi procedimenti dinanzi al Tribunale penale internazionale per i crimini in Ruanda, accusato di aver negato, con alcuni suoi libri, l'esistenza del genocidio nel Paese africano. Arrestato dalle autorità ruandesi, è stato rilasciato il 22 giugno 2010, anche se il procedimento penale era andato avanti. Con decisione del 6 ottobre 2010, la Camera di appello del Tribunale penale internazionale per il Ruanda ha stabilito l'immunità per l'avvocato solo per le dichiarazioni espresse nel corso del procedimento Ntabakuze, del quale il legale era difensore, ma non per quanto scritto e dichiarato nella sua attività privata (ICTR-98-41-A). Cfr. K. Gibson, *The Arrest of ICTR Defense Council Peter Erlinder in Rwanda,* in *Insights*, 14, 26, 2010, nel sito *asil.org*.

[58] Si veda il documento A/77/512.

pio, come nel caso di specie, affiggendo striscioni e distribuendo volantini. La sentenza in esame, inoltre, a nostro avviso smentisce le osservazioni critiche formulate da alcuni studiosi per i quali la norma sul negazionismo avrebbe un valore simbolico e sarebbe priva di effettività[59].

In realtà, sia dal quadro normativo sia dalla sentenza risulta realizzato quanto richiesto dalle organizzazioni internazionali, ossia la punizione in sede penale di coloro che negano crimini accertati dalla storia come l'Olocausto. Da ultimo, ciò è stato richiesto con la risoluzione n. 2447 dell'Assemblea parlamentare del Consiglio d'Europa adottata il 22 giugno 2022 con la quale, accertata la diffusione dell'antisemitismo e della discriminazione razziale che si manifestano anche con il negazionismo di genocidi come l'Olocausto e alla luce del rapporto "*Preventing and combating antisemitism in Europe*"[60], si sottolinea l'importanza di punire in sede penale il diniego dell'Olocausto e di altri crimini di genocidio, anche quando tali crimini sono commessi da pubblici ufficiali. Un'importanza che, a nostro avviso, risiede nel fatto che il negazionismo dell'Olocausto lede la dignità delle vittime, dei sopravvissuti e dell'intera collettività.

[59] Si veda, in questo senso, L. Daniele, *Negazionismo e libertà di espressione. Dalla sentenza Perinçek c. Svizzera alla nuova aggravante prevista nell'ordinamento italiano,* in *Diritto penale contemporaneo*, 10, 2017, 9 ss., in specie 96. Per alcune osservazioni critiche, cfr. M. Donini, *Negazionismo e protezione della memoria,* in *Sistema penale,* 2021, 1 ss. (nel sito *sistemapenale.it*), il quale ritiene che l'aggravante del negazionismo «rischia di imputare addirittura per colpa il discorso negazionista, avendone fatto una circostanza aggravante, che rileva anche se ignorata per colpa ex art. 59, co. 1 c.p., purché il fatto sia commesso in modo che derivi concreto pericolo di diffusione» (13).

[60] Si veda il rapporto n. 15539 del 23 maggio 2022, redatto da Petra Bayr, nel quale si afferma: «*Holocaust denial and distortion aim at negating a part of European history. They can also be used to promote a political agenda. The denial, trivialisation, justification or praise of the Holocaust should be criminalised. History education must include education on the Holocaust and prevent its trivialisation as well as revisionism. Specific educational programmes, as well as awareness-raising campaigns, are instrumental tools to prevent antisemitism. Sufficient funding must be allocated for their creation, if needed, and implementation. New ways of telling the story of the Holocaust, without survivors sharing their story, should be found. The Assembly should also be encouraged to continue its actions on Holocaust remembrance every year*».

The (posthumous) exercise of the right to be forgotten

Federica Casarosa

European Court of Human Rights, *M.L. v. Slovakia*, app. 34159/17, 14 October 2021

Dismissal of action against tabloids, which published unverified tawdry statements on, and pictures of, applicant's son, a priest convicted of sexual offences, years after his death: violation of article 8 ECHR.

Summary

1. Introduction. – 2. Facts. – 3. Judgement. – 4. Comment. – 5. Conclusion

Keywords

Right to be forgotten - freedom of expression - protection of private life - reputation of deceased person

1. Introduction

The right to be forgotten has become a hot topic for the ECtHR, with several decisions delivered on the different applications that this right may have in the offline and online world. Most of the cases delivered in 2021 addressed the interplay between the right to be forgotten and newspapers web archives,[1] whereas only the one analysed here addressed the traditional conflict between freedom of the press and the protection of private life in the offline world. The case M.L. v Slovakia, however, is not without interest as it addresses a specific dimension of the right to be forgotten, namely its exercise when the interested party is deceased.

2. Facts

Ms M.L. was the mother of a Roman Catholic priest. The latter was convicted twice, in 1999 and in 2002, first for sexual abuse against a minor and then for disorderly conduct.[2] The priest died in 2006 after having spent the criminal convictions in com-

[1] See ECtHR, *Hurbain v Belgium*, app. 57292/16, 22 June 2021; *Biancardi v Italy*, app. 77419/16, 25 November 2021.

[2] According to sect. 364 of Slovakian Criminal code, the offence of disorderly conduct was qualified as "Any person who, either verbally or physically, commits gross indecency or disturbs peace in public

pliance with the conditions of the conditional sentence.
In 2008, three Slovakian newspapers published a series of articles on the case involving the priest suggesting not only that his death was the result of suicide but also that it was related to the previous criminal convictions. Moreover, they included a reference to a confession by the priest to a bishop who helped him in the cases by providing a guarantee to the law enforcement authorities to avoid conviction and a detention period. The articles clearly identified the name of the priest, included photos and portrayed the case as an occasion in which the Roman Catholic church was interested in safeguarding the position of a priest in the Church and helping him to be released without conviction or a detention period.
Few months after the publication of the articles, the applicant started proceedings against the three publishers under two grounds: not only post-mortem protection of her son's personal integrity but also her own, contending that the information published in the articles was unfounded and affirming that the articles were a violation of her, and her son's privacy rights. The subsequent steps of the three-tier judicial proceedings resulted in the national courts dismissing the applicant's action, considering that the position of the parish priest was a public figure who should expect to be subject to stricter criticism by the press and public opinion, and deeming that the information in the articles was credible.
After a constitutional complaint before the Slovakian Constitutional Court, on grounds of violation of arts 6 and 8 ECHR, which was deemed inadmissible and ill-founded, the applicant brought the case before the ECtHR, claiming a violation of art. 8 ECHR. The applicant pointed to a misapplication of the relevant criteria established by the ECtHR regarding lawful dissemination of information pertaining to matters of public debate without sufficient attention to the truthfulness of the information published.

3. Judgement

The ECtHR addressed the claim and found it admissible, considering both the violation affecting the applicant and the deceased relative based on its own jurisprudence. Without further analysis the Court acknowledged that art. 8 ECHR also covers cases where an individual deals with the dead out of respect for the feelings of the deceased's relatives.[3]
The Court's assessment then indicated a balancing exercise that should be applied to the conflict between art. 8 and art. 10 ECHR. It referred to the well-known standards that the Court itself had developed in its jurisprudence since 2008 in the Von Hannover v Germany (no. 2) decision.[4] In order to evaluate if the national courts had addressed the conflict between the fundamental rights correctly the ECtHR listed the criteria and analysed each of them in detail.

or in a place accessible to public".

[3] See § 23.

[4] ECtHR, *Von Hannover v Germany* (no. 2), apps. 40660/08 and 60641/08, 7 February 2012.

The first criterion concerned his/her prior conduct. The ECtHR pointed out immediately that the position of the applicant's son and his role in the Church were not so high and important as to consider him a public figure that should tolerate a higher level of interference in his private life. As for prior conduct, the Court distinguished between the application of art. 8 regarding the commission of a criminal offence, the impact of which on one's reputation cannot be complained of, and the exercise of the right to be forgotten after the passing of time.[5] Accordingly, the Court referred to the standard applied in the *M.L. and W.W. v Germany* decision,[6] acknowledging that the conviction and subsequent reintegration of the person into society should allow the individual to request to fade out from the attention of public opinion. The court then affirmed that the national courts had omitted an analysis regarding the amount of time passed since the spent conviction involving the applicant's son.

The second set of criteria analysed were the style and content of the press articles and their impact. The Court focused on the methods used to obtain and disseminate the information. In particular, it made a clear distinction between statements of fact and value judgements, assuming that journalists may provide value judgements although they should be based on reliable sources and they should be diligently researched. A lack of such "reliable and precise" information may violate the ethics of journalism.[7] The ECtHR then evaluated the style used by the journalists in presenting the information, which was not in line with the standard applicable to journalistic activity, that should not exceed the purpose of information in the public interest and be free from insinuations or personal considerations. As the articles were presented in a sensational manner and included information that was not proven or verified by the journalists, the resulting evaluation by the Court was that they constituted a clear violation of responsible journalism. These elements, however, were not duly considered by the national courts, which deemed the journalists' unidentified sources and the unverified evidence they provided during the national proceedings credible. As a result, the Court affirmed that the publications framed in this manner and without reliable sources had an impact on the private life of the applicant, "the reputation of her deceased son being a part and parcel thereof."[8]

Last, the Court addressed the contribution to public debate by the published articles. In this case the Court acknowledged that the attitude of the Roman Catholic Church vis-à-vis sexual abuses by its members is a topic of public interest. However, the Court distinguished between the dissemination of information and opinions on more general issues and the possibility of exploiting the specific case presenting intrusive information on a person's intimate sphere in order to satisfy public curiosity.[9] The fact that the information was presented in a sensational manner and included information that was not relevant to a contribution to a debate of general interest brought the Court to affirm that in this case the principle of freedom of expression should be

[5] See § 38

[6] M.*L. and W.W. v. Germany*, apps. 60798/10 and 65599/10, 28 June 2018.

[7] See § 42.

[8] See § 48.

[9] See § 53.

limited and should give way to the protection of the private life of the individual.
As a conclusion, the Court acknowledged that the domestic courts did not correctly apply the ECHR standards as regards balancing between conflicting rights, resulting in a violation of art. 8 ECHR.

4. Comment

In *M.L. v Slovakia*, the Court addressed a traditional case of conflict between freedom of expression and protection of private life. The publication of articles in the press that may affect the personal sphere and the reputation of an individual has been the subject of several cases discussed by the ECtHR since the Grand Chamber decisions in the *Von Hannover v Germany* (no. 2)[10] and *Axel Springer v Germany*[11] cases. Accordingly, the Court had the opportunity to develop and apply a well-run set of criteria in order to strike the balance between the two conflicting rights. However, these criteria were to be applied to information that pertained to a deceased person and which may affect the private sphere of a relative.
As a matter of fact, in the Court's reasoning it seems to appear that the right to be forgotten may apply to a deceased person, with the possibility of it being exercised also by a relative.[12] This is a critical issue as the Court's decision in this case may also have an impact on the general principle that a personal cause of action dies with the person, as in the case of defamation.
So far, the Court had accepted claims for the violation of privacy protection only when the offence against the reputation of the deceased person had an impact on applicant's private life. The Court mentioned its jurisprudence showing the progressive extension of the scope of art. 8 ECHR also in this issue. In particular, the court pointed to the decisions in *Hadri-Vionnet v Switzerland*[13] and *Putistin v Ukraine*.[14] However, looking at the ECtHR caselaw there is no uniformity in the Court's approach as regards the transferability of the art. 8 right on the death of an individual. While in *Dzhugashvili v Russia* the Court denied the transferability of the right to reputation to relatives,[15] in *Kunitsyna v Russia* it acknowledged that the protection of the reputation of the deceased person can extend to the relatives *only* when the content of publications are able "to make the ordinary reader feel that the statement reflected directly on the individual claimant, or that he was targeted by the criticism."[16] However, in *Genner*

[10] See above at fn 3.

[11] *Axel Springer AG v. Germany* [GC], app. 39954/08, 7 February 2012.

[12] Note that the inclusion of the right to be forgotten within the scope of art. 8 ECHR is well set, with confirmation provided also by the recent decision in *Hurbain v Belgium*, see above fn 1.

[13] ECtHR, *Hadri-Vionnet v. Switzerland*, app. 55525/00, 14 February 2008. In this case, the applicant complained under art. 8 ECHR as she had been unable to attend the funeral of her stillborn child and that her baby's body had been transported in an ordinary delivery van.

[14] ECtHR, *Putistin v Ukraine*, no. 16882/03, 21 November 2013.

[15] ECtHR, *Dzhugashvili v Russia*, app. 41123/10, 9 December 2014, §§ 23-24.

[16] ECtHR, *Kunitsyna v Russia*, § 42.

v Austria[17] the Court moved to a more ambiguous approach, affirming that "to express insult on the day after the death of the insulted person contradicts elementary decency and respect for human beings […] and is an attack on the core of personality rights."[18] In the present case, the Court did not go as far as recognising the protection of the reputation of the deceased person, although it acknowledged that the reputation of the son had to be deemed part and parcel of the applicant's private life. In other words, it is the applicant's own right to reputation or right to be protected against distress or identity injury which fell within the scope of the right to private life.[19] However, it is still to be seen if the Court will proceed in this direction, limiting its interpretation of a deceased's reputation as a legitimate interest that could be taken into account only in a wider analysis of the violation of the right to private life of the relatives.

It must be underlined that the issue of defamation of a deceased person and the connected possibility to exercise the right to be forgotten is approached in different ways by national legal systems. A comparison with the approach adopted in the General Data Protection Regulation (GDPR)[20] and the adaptation of the legal framework in some EU countries is, therefore, useful.

The GDPR does not apply to the personal data of deceased persons as it only applies to an "identified or identifiable natural person," which is a person who is alive. However, the GDPR leaves some leeway to regulate this issue at the national level, as is clarified by recital 27 GDPR. Only a few Member States have introduced regulation on this topic, and in most cases, they rely on the right to self-determination of the data subject before death in order to comply with his will, for instance allowing the data subjects to specify their will as regards the processing of their personal data after their death.[21]

This is clearly the case in France, where pursuant to art. 85 of the *Loi informatique et libertés*,[22] individuals can request that after their death the data controller should follow the indications that they provide regarding the retention, erasure and communication of their personal data. Moreover, they can allocate to a third party the task of verifying if such indications are complied with.

In Spain and Italy, the laws adopted in 2018 to implement the GDPR also include

[17] ECtHR, *Genner v Austria*, app. 55495/08, 12 January 2016.

[18] For an analysis of previous jurisprudence, see G. Malgieri, *R.I.P.: Rest in Privacy or Rest in (Quasi-) Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions*, in R. Leenes - R. van Brackel - S. Gutwirth - P. De Hert (eds.), *Data Protection and Privacy: The Internet of Bodies*, Brussels, 2018, 300 ss.

[19] The protection of relatives' private sphere is not irrelevant as it includes moral protection of grief and memory; commercial protection from elusive forms of sensitive data processing; protection from exploitation of grief through personalised advertisements. See G. Malgieri, *R.I.P.: Rest in Privacy or Rest in (Quasi-)Property? Personal Data Protection of Deceased Data Subjects between Theoretical Scenarios and National Solutions*, cit., 310.

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, 1.

[21] See *GDPR Tracker - Personal data of deceased persons*, in *twobirds.com*.

[22] Loi Informatique et Libertés, 17 June 2019, amending Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*.

specific provisions addressing the rights of deceased persons. In particular, the Spanish Organic Law Act 3/2018 of 5 December on personal data protection and the guarantee of digital rights[23] provides that the relatives, civil partners and heirs of the deceased person are granted a right to exercise the rights to access, rectification and erasure of the personal data of the latter against the controller or the processor unless forbidden by the deceased person or by law.[24] Italian legislative decree 101/2018 provides a more detailed (though ambiguous)[25] set of criteria: the rights of the (deceased) data subject can be exercised by an individual who "has his/her own interest, or acts in order to protect a data subject, in capacity of his/her appointee, or for family reasons worthy of protection."[26] However, this can occur not only when it is not prohibited by law but also in the specific case of information society services when the (deceased) data subject has explicitly prohibited it in a written declaration sent to the data controller.[27]

Although it is apparent that the provisions of the above-mentioned national laws are tailored to the needs emerging from the management of social media accounts that may remain available online long after the death of the data subject,[28] the same principles may also apply to traditional media. Whenever the publication of information that refers to a deceased person may affect his/her identity, it is possible for a relative to act in order to protect the deceased data subject. However, where the publication can contribute to public debate without only appealing to public curiosity and it is done in a style and manner that comply with journalistic standards, then the freedom of expression may be safeguarded against interference in the private life of the deceased data subject.[29]

---

[23] Ley Orgánica 3/2018, "BOE" núm. 294, 6 December 2018, p. 119788, available at *boe.es*.

[24] See art. 3 of Constitutional Law 3/2008 regulating the data of deceased persons.

[25] T. Fia, *Death is real. How rights of deceased persons are treated under data protection laws*, in *gamingtechlaw.com,* 7 September 2018.

[26] See art. 2-*terdecies* of Legislative Decree 101/2018 regulating the data of deceased persons.

[27] This provision was applied by the Italian DPA in a recent decision, affirming that if the data subject had never requested the removal of a publication (still available online after his death), or has otherwise expressed the will to disavow the content, existence of an interest of the deceased data subject through his heir in the deletion of the publication cannot therefore be considered demonstrated. The publication instead retains its historical value as a testimony of the life of a deceased person and free expression of the latter's thought pursuant to art. 17 (3) (d) GDPR. See decision Italian DPA, no. 207, 29 October 2020, doc. web no. 9509538.

[28] Note that many social media have already started to provide dedicated functions and processes to deal with a person's information after they have died. For instance, Facebook turns its deceased users' accounts into online memorials allowing the content previously shared to remain visible. The person is also able to identify a "legacy person" who can manage the memorialised account. See the guidelines of Facebook on this issue at "What Happens When a Deceased Person's Account Is Memorialised?", available at *facebook.com*.

[29] See also the Decision of the Italian Court of Cassation, 27 March 2020, no. 7559, where the Italian Court affirmed that the right to be forgotten as regards criminal proceedings involving a deceased person cannot be claimed by the heir in his own right but only in the capacity of heir. The Court affirmed that the right to be forgotten cannot be exercised by the heir when the publisher has: a) excluded accessibility to the article in an online archive containing the data in question by means of general search engines; b) inserted in the article an update on further developments in the judicial proceedings.

5. Conclusion

The decision of the Strasbourg Court in *M.L.* touches upon a critical issue that is still unevenly addressed in the previous jurisprudence of the Court. In this case, the Court accepted that a deceased's reputation is a legitimate interest that could be considered only in a wider analysis of the violation of the right to private life of the relatives. However, it is not possible to rule out that, in the future, the Court will allow a claim for a violation to the right to private life also for a deceased person.
Given that individual's life is increasingly carried on digital platforms, whose existence outlast the life of its users, it is possible that cases addressing the possibility for heirs and relatives to exercise the right to be forgotten of deceased users will emerge soon.

Il concetto di algoritmo in una recente sentenza del Consiglio di Stato*

Silvia Cereda

Consiglio di Stato, sez. III, 25 novembre 2021, n. 7891

Al fine di ottenere la fornitura di un pacemaker di alta fascia con elevato grado di automazione non occorre che l'amministrazione faccia espresso riferimento a elementi di intelligenza artificiale, essendo del tutto sufficiente, anche in considerazione della peculiarità del prodotto, il riferimento allo specifico concetto di algoritmo, ossia di istruzioni capaci di fornire un efficiente grado di automazione, ulteriore rispetto a quello base, sia nell'area della prevenzione che del trattamento delle tachiaritmie atriali.

Sommario

1. L'analisi del fatto. — 2. L'algoritmo «di prevenzione + algoritmo di trattamento». — 3. Il concetto di automazione può rientrare nella definizione di algoritmo?. — 4. Esiste una relazione tra il concetto di azione autonoma e di algoritmo?

Keywords

algoritmo - bando di gara - azione autonoma - human in the loop – nozione di algoritmo

1. L'analisi del fatto

La vicenda vede coinvolte due società, X s.r.l. e Y s.r.l., in una gara d'appalto che ha per oggetto la fornitura di pacemaker e defibrillatori per gli enti sanitari lombardi. Tra i parametri di valutazione dell'offerta viene evidenziato «il parametro tabellare "algoritmo di prevenzione + trattamento delle tachiaritmie atriali"»[1] che prevede l'assegnazione di 15 punti qualora entrambi gli algoritmi siano presenti e di 7 punti se solo uno dei due algoritmi è presente. La gara viene vinta da X s.r.l.

La società Y s.r.l. impugna il provvedimento di aggiudicazione dinanzi al Tar Lombardia, lamentando «l'insufficienza del punteggio ottenuto in merito al criterio di valutazione "algoritmo di prevenzione + trattamento delle tachiaritmie atriali"»[2]. Infatti, la

*Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

[1] Cons. Stato, sez. III, 25 novembre 2021, n. 7891.

[2] Ivi, 3.

società aveva ottenuto solo 7 punti poiché, secondo la Commissione di gara, il prodotto offerto presentava solo l'algoritmo di prevenzione ma non quello di trattamento. Il Tar Lombardia accoglie la doglianza di Y s.r.l.

X s.r.l. ricorre, a sua volta, in Appello e contestualmente richiede una misura cautelare. Il Consiglio di stato accoglie la richiesta cautelare di sospensione della sentenza di primo grado, ritenendo di dover approfondire la questione della «perimetrazione tecnica della nozione di "algoritmo di trattamento" nell'ambito e nel contesto di una procedura di gara per la fornitura di pacemaker di alta fascia».

La Commissione di gara ha attribuito il punteggio massimo, ossia 15 punti, alla società X s.r.l. poiché essa ha sviluppato un algoritmo di trattamento che «in maniera autonoma è in grado di contrastare il ritmo prefibrillatorio mediante il riconoscimento di ectopie atriale e trattamento mediante riduzione/omogeneizzazione dei periodi refrattari atriali»[3]. Il dispositivo della società X s.r.l. non solo rileva l'anomalia cardiaca ma, una volta individuata, è in grado di intervenire autonomamente, senza l'intervento umano. L'algoritmo di trattamento della società Y s.r.l., invece, costituisce «uno studio elettrofisiologico eseguito in office da un operatore specialistico»[4] ossia, una volta ricevuta la segnalazione l'operatore decide come intervenire.

Il giudice del primo grado, interpellato da Y s.r.l., sostiene che la Commissione di gara aveva «confuso» la nozione di algoritmo con quella di Intelligenza Artificiale, la quale prevede nel suo funzionamento dei meccanismi di machine learning. Di conseguenza, il criterio per cui l'algoritmo era in grado di riconoscere la problematica cardiaca ed intervenire in modo automatico era un elemento ulteriore, che non era indicato nel bando di gara[5]. Dunque, è tramite questa motivazione che il Tar accoglie il ricorso di Y s.r.l. Infatti il giudice di prime cure sottolinea come «l'algoritmo di trattamento dell'aritmia non è altro che l'insieme di passaggi necessari al trattamento del singolo tipo di aritmia. Questo concetto non include necessariamente, invece come erroneamente ritenuto dalla stazione appaltante, che il dispositivo debba essere in grado di riconoscere in automatico l'esigenza»[6].

Al contrario, il Consiglio di stato accoglie l'appello della società X s.r.l. riformando la sentenza del Tar Lombardia. Il giudice del secondo grado si concentra sull'importanza del bando di gara. Il Consiglio di stato rileva che «la nozione di algoritmo che è applicata a sistemi tecnologici è ineludibilmente collegata al concetto di automazione ossia a sistemi di azione e controllo idonei a ridurre l'intervento umano»[7]. Infatti il giudice di secondo grado sostiene che non era necessario il riferimento all'Intelligenza Artificiale poiché il concetto di automazione, legato a sua volta al concetto di algoritmo, è insito nelle particolari caratteristiche del prodotto richiesto dalla PA. L'Amministrazione, infatti, è «orientata su un apparecchio tecnologicamente avanzato»[8] che sia in grado di coprire, senza un intervento umano, sia la prevenzione sia il trattamento.

[3] *Ibid.*

[4] Ivi, *4*.

[5] *Ibid.*

[6] *Ibid.*

[7] Ivi, 6.

[8] *Ibid.*

2. L'algoritmo «di prevenzione + algoritmo di trattamento»

Il primo dei due algoritmi, quello di prevenzione, ha la funzione di andare a rilevare l'anomalia cardiaca e di effettuare una segnalazione. Esso si basa su sistemi di machine learning. L'algoritmo di prevenzione non è una novità. Un meccanismo simile è presente nel famoso Apple Watch prodotto dalla Società Apple. Infatti l'Apple Watch prevede, tra le sue funzioni, la possibilità di controllare «periodicamente il ritmo cardiaco per verificare un'eventuale irregolarità che potrebbe indicare la presenza di fibrillazione atriale»[9]. Se l'algoritmo rileva una irregolarità viene inviata una notifica al paziente con la data, l'ora e la frequenza cardiaca anomala[10]. Inoltre le frequenze anomale vengono registrate sulla App Salute[11], presente sullo smartphone del paziente.
L'algoritmo di prevenzione, però, non risulta essere l'oggetto del contendere. Infatti, entrambe le società sono state in grado di sviluppare tale algoritmo.
Discorso diverso per quanto riguarda l'algoritmo di trattamento, ago della bilancia nella vincita del bando di gara, che, invece, rappresenta l'oggetto del contendere. L'algoritmo di trattamento permette di agire senza l'intervento umano. Solo la società X s.r.l. ha sviluppato l'algoritmo di trattamento. Infatti, l'algoritmo progettato dalla società X s.r.l., una volta individuata l'anomalia, agisce autonomamente, senza l'intervento umano, sul funzionamento del pacemaker. Diversamente, l'algoritmo della società Y s.r.l. è solo in grado di rilevare l'anomalia senza l'intervento umano, mentre per l'intervento si affida alla decisione di un operatore sanitario. Nella pratica l'algoritmo della società Y s.r.l. effettua una semplice segnalazione, in seguito l'operatore sanitario assume «temporaneamente il controllo a distanza del pacemaker del paziente»[12].
Dunque, l'algoritmo della società Y s.r.l. non riduce l'intervento umano come richiesto dalla PA e perciò non è stato considerato ai fini del punteggio.

3. Il concetto di automazione può rientrare nella definizione di algoritmo?

Una volta effettuata l'analisi del fatto, è giunto il momento di astrarre il concetto di algoritmo dalla sentenza del Consiglio di stato. I tre diversi attori che si sono interfacciati in questa vicenda sono: la Commissione di gara, il Tar Lombardia e il Consiglio di stato. La Commissione e il Consiglio di stato ritengono che il concetto di algoritmo ricomprenda al suo interno anche il concetto di automazione, intesa come azione autonoma. In generale, il concetto di automazione, così come viene inteso dalla Commissione e dal Consiglio di stato, indicherebbe che l'algoritmo è in grado di agire senza l'intervento umano. Di opinione contraria, invece, è il Tar Lombardia, il quale sostiene che non vi sia alcun collegamento tra il concetto di algoritmo e quello di automazione.

[9] Cfr. Salute-Apple Watch, *Apple Watch. Aiuta le persone che hai in cura a vivere in maniera più sana*, 2022.

[10] *Ibid.*

[11] *Ibid.*

[12] Cons. Stato, sez. III, 25 novembre 2021, n. 7891.

Per comprendere meglio il concetto di algoritmo, e, a sua volta, il legame con il concetto di azione autonoma, è necessario discostarsi dalla pronuncia del Consiglio di stato. Di seguito verranno proposte delle due definizioni di algoritmo: la prima di carattere intuitivo, probabilmente la più nota[13], e la seconda elaborata dal governo inglese[14].

La definizione intuitiva, classica di algoritmo è la seguente: «sequenza di istruzioni che specifica una combinazione di azioni da compiere per risolvere un problema». In altre parole, l'algoritmo non è altro che una sequenza di istruzioni, di una serie di dati «in ingresso» (input) che realizza «in uscita» un risultato (output).

«Secondo questa caratterizzazione l'algoritmo in senso stretto è dotato delle seguenti proprietà:

Finitezza: l'algoritmo deve portare alla soluzione in un numero finito di passi.

Generalità: l'algoritmo non risolve solo un problema, ma una classe di problemi.

Non ambiguità: le istruzioni sono specificate univocamente, cosicché la loro esecuzione avviene sempre nello stesso modo, indipendentemente dall'esecutore.

Ripetibilità(determinismo): dati gli stessi dati in input l'algoritmo deve fornire gli stessi risultati in output»[15].

Fino a questo momento le nozioni di algoritmo analizzate o provengono dalla giurisprudenza, come nel caso della sentenza del Consiglio di stato, o dalla dottrina, come nel caso di Giovanni Sartor.

Ora passiamo a considerare la definizione di algoritmo proveniente dall'ambito anglosassone.

A partire dal 2020 il governo inglese ha avviato la National Data Strategy (NDS), che consiste in un quadro di riferimento delle azioni intraprese dal governo inglese in tema di uso dei dati[16]. Parte di questa strategia è l'Algorithm Transparency Standard, realizzato dal Central Digital Data Office. Esso ha la funzione di «helps public sector organisations provide clear information about the algorithmic tools they use, and why they're using them»[17]. L'Algorithm Transparency Standard riporta la seguente definizione del termine 'algorithm': «a set of step-by-step instructions». Lo scopo del governo inglese è creare una struttura pubblica il più possibile trasparente, cioè permettere ai cittadini di conoscere i processi tecnologici che animano il settore statale. È necessaria, quindi, una nozione semplice che consenta al cittadino medio di comprendere con facilità cosa si intenda per algoritmo.

Dalle definizioni di algoritmo elencate si evidenzia come non via sia alcun riferimento al concetto di azione autonoma. Infatti, tale concetto sembra oltrepassare i confini della semplice definizione di algoritmo. A dimostrazione di ciò, si può citare la definizione di sistema decisionale autonomo data dall'Algorithmic Accountability Act statunitense: «a computational process, including one derived from machine learning statistic, or other data processing or artificial techniques, that makes a decision or

[13] Cfr. G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione*, Torino, 2016.

[14] Cfr. Digital Centre and Data Office, *Algorithm Transparecy Standard*, 2021.

[15] Cfr. G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione*, cit., 85 ss.

[16] Cfr. Department for Digital, Culture, Media & Sport, *UK National Data Strategy*, 2020.

[17] *Ibid.*

facilitates human decision making, that impacts consumers». Con questa definizione il Congresso americano delinea un sistema in grado di prendere delle decisioni autonome o facilitare la decisione umana. Quindi nel concetto di sistema decisionale autonomo sembra ritrovarsi anche il concetto di azione autonoma che, invece, sembra estraneo alla definizione di algoritmo.
Da questa analisi sembra che la definizione di algoritmo non ricomprenda al suo interno il concetto di azione autonoma. Infatti, i concetti di azione autonoma e di sistema decisionale autonomo, delineato dal Congresso americano, sono più ampi rispetto al concetto di algoritmo.
Ciò indicherebbe che il ragionamento realizzato dalla Commissione di gara e dal Consiglio di stato non faccia riferimento al concetto di algoritmo ma si estenda a concetti più ampi rispetto allo stesso.

4. Esiste una relazione tra il concetto di azione autonoma e di algoritmo?

Tra gli informatici è consuetudine distinguere tra questi termini: algoritmo, codice, programma e software. Per "algoritmo" si intende una sequenza finita di istruzioni atte a risolvere un problema. Il termine "codice", invece, si riferisce a qualsiasi rappresentazione dell'algoritmo in un linguaggio di programmazione. A sua volta, il "programma" rappresenta l'esecuzione delle istruzioni dell'algoritmo come insieme di comportamenti descritti dal codice. E il "software" è l'insieme dei programmi, intesi come insieme di comportamenti, che sono eseguibili dal calcolatore.
In base a questa distinzione è possibile affermare che sia il Consiglio di stato sia il legislatore confondano il sistema che produce l'output, il software, con l'algoritmo: è il software, infatti, che permette all'algoritmo di realizzarsi. Il software è esattamente quella ware, ossia una macchina materiale ma dalla configurazione flessibile (soft) che istanzia l'algoritmo come un insieme di comportamenti. L'algoritmo, quindi, non esegue nulla ma si sostanzia semplicemente in una serie di istruzioni che sono finalizzate a risolvere un problema. Accogliendo questa distinzione, il concetto di algoritmo non può ricomprendere al suo interno il concetto di azione autonoma. Questo perché è il software che ricopre il ruolo di esecutore ed è sempre il software che realizza l'algoritmo.
Alla luce di queste considerazioni si può evidenziare come anche il bando di gara pecchi di imprecisione. Infatti «il criterio di valutazione algoritmo di prevenzione + algoritmo di trattamento» è impreciso: non è l'algoritmo che realizza gli interventi nel mondo fisico bensì il software. La Commissione di gara, così come il Consiglio di stato, confondono l'algoritmo con il software, ossia confondono l'algoritmo con la sua realizzazione (il software), intesa come macchina capace di modificare il mondo fisico.

Il nuovo perimetro di liceità per la pubblicazione di immagini di un atleta senza il suo consenso

Sabrina Peron

Corte di Cassazione, sez. II, civile, 16 giugno 2022, n. 19515

L'esimente prevista dall'art. 97 della l.633/1941 secondo cui non occorre il consenso della persona ritratta in fotografia quando, tra l'altro, la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, ricorre non solo allorché il personaggio noto sia ripreso nell'ambito dell'attività da cui la sua notorietà è scaturita, ma anche quando la fotografia lo ritrae nello svolgimento di attività a quella accessorie o comunque connesse, fermo restando, da un lato, il rispetto della sfera privata in cui il personaggio noto ha esercitato il proprio diritto alla riservatezza, dall'altro, il divieto di sfruttamento commerciale dell'immagine altrui, da parte di terzi, al fine di pubblicizzare o propagandare, anche indirettamente, l'acquisto di beni e servizi. **Parole chiave:** diritto all'immagine – riservatezza – personaggio pubblico – notorietà - divulgazione dell'immagine senza consenso

Sommario

1. Il caso. - 2. Brevi cenni sul diritto all'immagine. - 3. Il nuovo perimetro della deroga al consenso.

Keywords

diritto all'immagine - divulgazione dell'immagine senza consenso - notorietà - personaggio pubblico - riservatezza

1. Il caso

La casa editrice di un popolare quotidiano sportivo commercializzava, unitamente al quotidiano, una serie di prodotti riproducenti e/o contenenti le immagini di un calciatore molto noto ed amato dal pubblico (successivamente diventato anche un uomo politico). In particolare si trattava: di alcune medaglie riproducenti l'immagine dell'atleta; di nove supporti audio/video DVD, contenenti filmati di gioco e non, interviste e fotografie dell'atleta; e di un volume, contenente fotografie in momenti di gioco e non. A seguito della diffusione di tali prodotti, il calciatore conveniva l'editore avanti al

Tribunale di Milano, chiedendone la condanna per violazione sia del suo diritto d'immagine (art. 2 Cost.; art. 10 c.c.; artt. 1, 2 e 96, l. 633/1941), che del suo diritto alla protezione dei suoi dati personali, stante il difetto di previo consenso allo sfruttamento del suo diritto d'immagine a scopo commerciale.

In parziale accoglimento delle domande attoree, il Tribunale di Milano riteneva illecita la diffusione delle immagini fotografiche ritraenti l'attore non in azioni di gioco e quelle effigiate (sia pure in forma stilizzata) sulle medaglie e condannava la società convenuta al risarcimento dei danni liquidati in via equitativa in complessivi euro 50.000,00 (di cui euro 40.000,00 per danno patrimoniale ed euro 10.000,00 per danno non patrimoniale[1]).

La sentenza veniva confermata in secondo grado dalla Corte d'Appello di Milano, ad avviso della quale l'esimente *ex* art. 97, l. 633/1941 (che disciplina le ipotesi in cui l'immagine di una persona può essere riprodotta senza il suo consenso[2]) non poteva applicarsi per tutte quelle immagini che raffiguravano l'atleta in «scene di vita quotidiana e al di fuori del contesto calcistico in cui la sua notorietà trovava concretizzazione», ivi comprese le medaglie commemorative, sul presupposto che la stilizzazione evocava il calciatore con un alto grado di fedeltà.

Avverso tale sentenza l'editore ricorreva in Cassazione. Il ricorso era però limitato ai motivi di condanna inerenti all'accertamento dell'illiceità della pubblicazione delle fotografie del calciatore ritratto non in azione di gioco e senza la divisa della squadra ed alla conseguente quantificazione del danno[3]. Secondo il ricorrente, difatti, la sentenza era errata nella parte in cui aveva ritenuto illecita la pubblicazione delle fotografie in questione, sia perché erano state originariamente scattate con il consenso dell'atleta, sia perché non si trattava di immagini offensive o denigratorie, sia infine perché non erano state utilizzate a fini pubblicitari, soddisfacendo per contro finalità informative e didattico-culturali.

La Corte di Cassazione con la sentenza in commento ha accolto il ricorso con rinvio, disponendo l'applicazione del seguente principio: «L'esimente prevista dall'art. 97, l.633/1941, secondo cui non occorre il consenso della persona ritratta in fotografia quando, tra l'altro, la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, ricorre non solo allorché il personaggio noto sia ripreso nell'ambito dell'attività da cui la sua notorietà è scaturita, ma anche quando la fotografia lo ritrae nello svolgimento di attività a quella accessorie o comunque connesse, fermo restando, da un lato, il rispetto della sfera privata in cui il personaggio noto ha esercitato il proprio diritto alla riservatezza, dall'altro, il divieto di sfruttamento commerciale dell'immagine altrui, da parte di terzi, al fine di pubblicizzare o propagandare,

[1] Si noti che l'attore aveva richiesto la condanna al pagamento di circa euro 7.000,00 per il danno patrimoniale ed euro 5.000,00 per quello non patrimoniale.

[2] Più precisamente l'art. 97, l. 633/1941, costituisce norma derogatoria all'art. 96, l. 633/1941 (e art. 10 c.c.) e consente la riproduzione dell'immagine anche senza il consenso dell'interessato, quanto appaia giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, oppure, quando la riproduzione sia collegata a fatti di interesse pubblico o svoltisi in pubblico.

[3] Veniva invece prestata acquiescenza alla sentenza di secondo grado per la parte riguardante le immagini stilizzate nelle medaglie commemorative.

anche indirettamente, l'acquisto di beni e servizi».

2. Brevi cenni sul diritto all'immagine

La nozione d'immagine non concerne solo la rappresentazione e la riproduzione delle sembianze e dell'aspetto fisico di una persona, ma si estende sino a ricomprendervi il modo d'essere nelle relazioni sociali ove si esprime la propria personalità. Quest'ultima, a sua volta, formata da quell'insieme di valori (intellettuali, politici, sociali, religiosi, ideologici, professionali, etc.) che, insieme alle fattezze fisiche, concorrono a formarne l'identità personale.

La tutela del diritto all'immagine - considerato quale un diritto assoluto, personalissimo ed inalienabile, che trae il suo fondamento dall'art. 2 della Costituzione finisce così col lambire anche la tutela del diritto alla riservatezza: essendo l'immagine un modo d'essere dell'identità personale, è evidente che l'abuso dell'immagine altrui può sostanziarsi anche con intromissioni di terzi nella sfera privata. Non a caso, al riguardo, la normativa a tutela dei dati personali, prevede sempre il consenso dell'interessato al trattamento dei suoi dati (tra i quali pacificamente rientra l'immagine), con l'eccezione del trattamento effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle finalità d'informazione. In questo caso, tuttavia, è pur sempre necessario il rispetto dei criteri di verità, continenza ed essenzialità dell'informazione riguardo a fatti di interesse pubblico[4].

Come ricordato anche nella sentenza in commento le norme applicabili per la tutela del diritto all'immagine sono:

l'art. 10 c.c., dedicato all'abuso dell'immagine altrui, prevede che: «Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, possa disporre che cessi l'abuso, salvo il risarcimento dei danni»;

l'art. 96, l. 633/1941, che enuncia il principio generale in forza del quale: «Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il suo consenso, salve le disposizioni dell'articolo seguente»[5];

ossia l'art. 97, l. 633/1941, che consente la deroga alla necessità del consenso della persona ritratta «[…] quando la riproduzione dell'immagine è giustificata dalla notorietà o

[4] Secondo la giurisprudenza «l'essenzialità dell'informazione riguardo a fatti di interesse pubblico quale presupposto di liceità della condotta, in assenza del consenso dell'interessato, deve essere inquadrata nel generale parametro della continenza e, dunque, della indispensabile osservanza del limite di contemperamento tra la necessità del diritto di cronaca e la tutela della riservatezza del dato», così Cass. civ., sez. III, 23 marzo 2017, n. 7413, che richiama gli insegnamenti di Cass. pen., sez. V, 14 settembre 2016, n. 42987.

[5] Si ricorda che dopo la morte il consenso può essere dato o negato dai parenti del *de cuius* individuati dall'art. 93, c. 4, l. 633/1941, ossia il coniuge e i figli, o, in loro mancanza, i genitori e in mancanza di questi i fratelli e le sorelle, e, in loro mancanza, gli ascendenti e i discendenti fino al quarto grado.

dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico». Fermo restando che la riproduzione dell'immagine altrui è sempre considerata illecita quando rechi pregiudizio all'onore, alla reputazione o al decoro della persona ritrattata[6].

Con riferimento al consenso, giurisprudenza consolidata (richiamata anche nella sentenza in commento) si attiene al principio secondo il quale il consenso è «un negozio unilaterale, avente ad oggetto non il diritto, personalissimo ed inalienabile, all'immagine, ma soltanto il suo esercizio»;

e che sebbene possa essere «occasionalmente inserito in un contratto, da esso resta tuttavia distinto ed autonomo: con la conseguenza che esso è revocabile in ogni tempo, e anche in difformità di quanto pattuito contrattualmente, salvo, in questo caso, il diritto dell'altra parte al risarcimento del danno. Ma, se revoca (tempestiva, e cioè anteriore all'utilizzazione) non vi sia stata, il consenso precedentemente prestato resta efficace, e legittima l'uso che ne sia stato fatto in conformità alle previsioni contrattuali»[7].

Quanto invece alle ipotesi contemplate dall'art. 97, l. 633/1941 e valevoli quali eccezioni alla regola generale del consenso, queste, avendo carattere derogatorio del diritto all'immagine (che si ricorda è un diritto inviolabile della persona tutelato dalla costituzione) sono tutte di stretta interpretazione[8].

Ne segue, che in tutti i casi in cui la pubblicazione e la diffusione concernente un *homo publicus* non sia «finalizzata a fornire alla collettività un'informazione su fatti di una qualche utilità sociale, deve ritenersi vietata qualsiasi diffusione, senza il consenso, dell'immagine anche di persone note, le quali conservano intatto sia il diritto a che gli altri non abusino della loro immagine, sia il diritto a sfruttare economicamente la loro immagine, sia il diritto a vedere tutelata la sua sfera privata da illecite aggressioni»[9].

Il che ulteriormente significa che non si può prescindere dal consenso quando la divulgazione mira soltanto a fini puramente pubblicitari, commerciali, o comunque di lucro[10].

Inoltre, la presenza delle condizioni legittimanti l'esercizio del diritto di cronaca «non implica, di per sé, la legittimità della pubblicazione o diffusione anche dell'immagine delle persone coinvolte».

In questi casi, la liceità della diffusione delle immagini è subordinata (oltre che al ri-

[6] Cass. civ., sez. III, 27 agosto 2015, n. 17211: «l'esposizione o la pubblicazione dell'immagine altrui a norma dell'art. 10 c.c. e degli artt. 96 e 97 legge n. 633/1941 sul diritto d'autore, è abusiva non soltanto quando avvenga senza il consenso della persona o senza il concorso delle altre circostanze espressamente previste dalla legge come idonee ad escludere la tutela del diritto alla riservatezza (quali la notorietà del soggetto ripreso, l'ufficio pubblico dallo stesso ricoperto, la necessità di perseguire finalità di giustizia o di polizia, oppure scopi scientifici, didattici o culturali, o il collegamento della riproduzione a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico), ma anche quando, pur ricorrendo quel consenso o quelle circostanze, l'esposizione o la pubblicazione sia tale da arrecare pregiudizio all'onore, alla reputazione o al decoro della persona medesima».

[7] Cass. civ., sez. I, 29 gennaio 2016, n. 1748; 19 novembre 2008, n. 27506, in *Foro it.*, I, 10, 2009, 2728 ss.; 17 febbraio, 2004 n. 3014, in *De&G*, 21, 2004, 107 ss.

[8] Cass. civ., sez. III, 11 maggio 2010, n. 11353; Cass. civ., sez. I, 28 marzo 1990, n. 2527.

[9] Trib. Torino, 27 febbraio 2019, n. 940.

[10] Cass. civ., sez. I, 19 febbraio 2021, n. 4477, in *Foro it.*, I, 7, 2021, 2436 ss.

spetto delle prescrizioni contenute nelle norme sopra citate e da quelle previste a tutela della riservatezza dal GDPR (regolamento (UE) 2016/679) e dal Codice deontologico dei giornalisti), anche alla «verifica, in concreto della sussistenza di uno specifico ed autonomo interesse pubblico alla conoscenza delle fattezze dei protagonisti della vicenda narrata, nell'ottica della essenzialità di tale divulgazione ai fini della completezza e correttezza della informazione fornita»[11].

3. Il nuovo perimetro della deroga al consenso

Con particolare riguardo ai personaggi famosi, le immagini degli atleti, che in virtù delle loro gesta sono diventati beniamini del pubblico, hanno acquisito un valore ed un interesse via via crescente, anche in settori della vita civile estranei a quelli sportivi (ad esempio l'atleta *testimonial* di battaglie per i diritti civili[12]). In questo contesto è stato osservato come in alcuni tipi di sport «l'aspetto meramente ludico ed agonistico, conviva ormai con l'aspetto prettamente commerciale dell'attività, e ne sia anzi sovente travolto»[13].

Il mondo del calcio - sport molto popolare nel nostro Paese - è stato quello maggiormente interessato al fenomeno. Sull'argomento si ricorda che uno dei primi casi fu quello che coinvolse il calciatore Sandro Mazzola, del quale ne erano state riprodotte le sembianze in un pupazzo. In questa fattispecie la Corte di Cassazione statuì che «l'abbinamento dell'immagine di una persona nota senza il suo consenso alla vendita di un prodotto diverso dall'immagine a scopo di *reclame* di quest'ultimo», doveva considerarsi illecito, prescindendo dallo scopo di lucro, perché esulava da «tutte le ipotesi di deroga alla tutela dell'immagine previste dall'art. 97, l. 633/1941»[14]. Più altalenante, invece, la giurisprudenza formatasi in tema di commercializzazione di figurine di personaggi sportivi, dove la giurisprudenza ha oscillato tra: il ritenere che l'attività di produzione e vendita di figurine destinate ad esser collezionate in appositi album, rispondesse tanto ad esigenze informative, quanto a scopi didattici e culturali, con la conseguenza, pertanto, che l'utilizzazione delle immagini dei calciatori, come previsto dall'art. 97, non doveva subordinarsi al consenso dell'interessato[15]; e l'affermare la prevalenza dello scopo di lucro rispetto alla funzione informativa, così da escludere in radice l'operatività delle esimenti previste nella legge sul diritto d'autore[16].

---

[11] Cass. civ., sez. I, 9 luglio 2018, n. 18006; 22 luglio 2015, n. 15360.

[12] Si pensi ad esempio all'immagine di Colin Kaepernick, in ginocchio, durante l'inno americano, per protestare contro le ingiustizie subite dalla minoranza nera negli Usa.

[13] M. Cian, *Il diritto all'immagine degli atleti*, in *AIDA*, 2003, 260 ss.

[14] Cass. civ., sez. I, 10 novembre 1979, n. 5790, in *Foro it.*, I, 1980, 81 ss.

[15] Trib. La Spezia, ord., 30 giugno 1994, in *Dir. inf.*, 1995, 355 ss., con nota di A. Giampieri, *«Ce l'ho, ce l'ho, mi manca»: Ancora in tema di commercializzazione di figurine di personaggi sportivi*; App. Genova, 24 febbraio 1981, in *Riv. dir. sport.*, 1982, 563 ss.; App. Bologna, 21 aprile 1978, in *Foro pad.*, I, 1978, 295 ss., con nota di A. Pesce, *Figurine che passione! Spunti in tema di diritto all'immagine.*

[16] Si vedano: Trib. Milano, ord., 6 luglio 1994, in *Dir. inf.*, 1995, 358 ss., con nota di A. Giampieri, cit.; Trib. Torino, ord., 4 ottobre 1995, in *Dir. inf.*, 1996, 437 ss.; Trib. La Spezia, ord., 9 ottobre 1995, in *Dir. inf.*, 1996, 442 ss.; Trib. Modena, ord., 30 aprile 1996, in *AIDA*, 1997, 739 ss.

La società attuale che si nutre di moltiplicazioni ininterrotte d'immagini, rilanciate e moltiplicate on-line tra i più disparati social network, nel caso degli atleti, non solo porta alla riproduzione delle loro immagini tramite i mezzi più disparati, ma porta anche alla moltiplicazione degli oggetti da collezione, come nel caso in esame le medaglie commemorative (ma anche i calendari[17], i poster, e oggetti vari).

In questo contesto la sentenza in commento perimetra i confini dello spazio di operatività della deroga al consenso *ex* art. 97, l. 633/1941:

escludendo la possibilità di una lettura estensiva della norma che renderebbe lecita la diffusione delle immagini dei personaggi dello sport[18], «senza il loro consenso, anche in contesti del tutto avulsi da quelli che hanno reso noti tali personaggi»;

escludendo la liceità della diffusione di immagini scattate in occasioni private, senza «alcun collegamento, anche indiretto, con l'attività che ha determinato la celebrità e per le quali, del tutto lecitamente, il personaggio noto ha esercitato il diritto di ammantare di riservatezza, attraverso uno *jus excludendi alios*, la propria sfera privata»[19];

escludendo la liceità dell'utilizzo delle immagini per fini pubblicitari o propagandistici, agganciandola - anche suggestivamente - a un prodotto o a un servizio, al fine di incentivare i consumatori all'acquisto.

Ribaditi questi limiti, la Cassazione reputa tuttavia lecita la divulgazione delle immagini dei personaggi famosi «non solo allorché essi siano raffigurati nell'espletamento dell'attività specifica che li ha consegnati alla pubblica notorietà (vale a dire: per lo sportivo l'attività agonistica, per il cantante l'esibizione sul palco, per l'attore la recitazione in scena), ma anche quando la fotografia li ritrae nello svolgimento di attività accessorie e connesse, che rientrano nel cono di proiezione della loro immagine pubblica e quindi nella sfera di interesse pubblico dedicato dalla collettività alla loro attività».

La Corte di Cassazione sembrerebbe dunque porre al centro della sua attenzione la nozione di interesse pubblico. Questo viene inteso come interesse del pubblico non solo a conoscere e vedere le fotografie che ritraggono l'atleta nell'attimo del suo gesto sportivo, ma anche quelle che lo ritraggono «in partenza o al rientro per una competizione sportiva, o mentre esibisce un trofeo vinto, o nell'atto di rilasciare a un giornalista una intervista legata alla sua attività, o ancora insieme ad altri calciatori, per di più se in un ritiro organizzato dalla sua squadra». In tal modo è ammessa la liceità della riproduzione e divulgazione delle immagini di un'atleta, senza il suo consenso, tutte le volte in cui egli «pur non indossando la divisa e non praticando attualmente il proprio sport, viene raffigurato in stretta connessione con l'ambito di attività per cui

[17] Si ricorda in proposito: Trib. Torino, 13 aprile 1996, in *Dir. ind.*, 1996, 1007: «la pubblicazione (e distribuzione) di un calendario denominato Juventissima contenente le immagini dei dodici calciatori senza il consenso dei medesimi costituisce contraffazione del marchio Juventus di cui è titolare la società omonima e che viene da questa usato per commercializzare il calendario ufficiale della squadra e costituisce violazione del diritto dei calciatori sulla propria immagine».

[18] Ma non solo dei personaggi sportivi, ma in genere di tutti i personaggi famosi nel mondo del cinema o della musica o della moda etc.

[19] In proposito la sentenza in commento richiama il noto precedente della Cass. civ., sez. I, 23 gennaio 2019, n. 1875, concernente un caso in cui erano «state captate con strumenti tecnologici, e prolungati appostamenti, postazioni sopraelevate e utilizzo degli interstizi nelle siepi di recinzione, alcune immagini del noto attore con la compagna in ambiente privato e situazioni di vita quotidiana, per nulla disdicevoli o sconvenienti, ma private e riservate».

ha conseguito la notorietà, e in cui è oggetto di interesse da parte del pubblico proprio in quanto sportivo noto».

Cosicché, l'esimente dell'interesse pubblico *ex* art. 97, l. 633/1941, si estende sino a ricomprendere la conoscenza di come il personaggio sportivo, gioisce dei propri trionfi, si relaziona con la stampa, come si prepara alle partite e si rilassa dopo di esse, e interagisce con altri atleti famosi. Ragion per cui, i personaggi di tale calibro non possono poi pretendere di circoscrivere la loro «notorietà all'ambito originario da cui è germinata (nel caso il calcio)», così da escludere «situazioni in cui l'atleta viaggia, parla con altri calciatori, o appare in pubblico in abiti borghesi ma in connessione con la propria attività sportiva».

Ovviamente, dalla circostanza che l'editore della pubblicazione riproducente le immagini sia un soggetto avente natura imprenditoriale, non può desumersi automaticamente un utilizzo della stessa per fini pubblicitari e promozionali (per i quali è sempre necessario il consenso). Difatti, non deve confondersi la «natura professionale dell'attività di cronaca informativa e documentazione didattico-culturale, che comporta la pubblicazione di informazioni e di immagini, con le finalità di utilizzo dell'immagine in senso stretto. Altrimenti si finirebbe per interdire l'esercizio stesso della cronaca giornalistica». Fermo restando che «l'attività informativa, didattica e culturale, ben può essere rivolta anche con lo sguardo al passato, per raccontare e illustrare in modo organico vicende pregresse, e non solo con l'attenzione al presente per aggiornare sugli eventi in corso». E fermo restando altresì che le «finalità informative, didattiche o culturali, possano essere perseguite con la pubblicazione della fotografia nell'esercizio della circostanza esimente anche da un soggetto che agisca nell'esercizio di un'impresa e a fini di lucro, ove il profitto venga ricercato proprio per il tramite dell'attività informativa».

Internet e "standard della community" nella regolamentazione delle piattaforme online: sulla non vessatorietà delle clausole in materia di disinformazione

Matteo Gozzi

Tribunale di Varese, sez. I civile, ord. 2 agosto 2022

Non hanno carattere vessatorio, ove sussista un legittimo contemperamento tra i diritti costituzionali tutelati, le clausole contrattuali attraverso le quali i social network prevedano la sospensione degli account o la rimozione dei contenuti pubblicati comportanti disinformazione in ambito sanitario

Sommario

1. L'oggetto della decisione. – 2. Il necessario vaglio giurisdizionale sulla regolamentazione contrattuale. – 3. Il bilanciamento tra i diritti costituzionali. – 4. Conclusioni.

Keywords

Internet – codice del consumo - clausole vessatorie – disinformazione – manifestazione del pensiero.

1. L'oggetto della decisione

La sentenza annotata pone in luce e affronta in modo organico e attento un difficile problema giuridico, ossia i limiti entro i quali i cd. "standard della community" citati nella regolamentazione contrattuale di alcune piattaforme online possano giustificare la rimozione dei contenuti pubblicati dai singoli utenti.

Il punto centrale della motivazione riguarda l'inquadramento del diritto dell'*hosting provider* – previsto espressamente in una clausola contrattuale – di intervenire sopra l'account del singolo utente sospendendolo o inibendo l'accesso ad esso ove venissero ritenute violate, a giudizio del medesimo *hosting provider*, le relative condizioni contrattuali e, in particolare, i cd. "standard della community" tra i quali figura (a fianco di aspetti quali la lotta alle forme di violenza, la tutela della autenticità dei contenuti

oppure il rispetto della proprietà intellettuale) anche il contrasto alle campagne di disinformazione.

Tale profilo, per ciò che emerge dalla motivazione del provvedimento, si assesta tuttavia su un aspetto specifico oggetto di azione giudiziale, ossia l'ipotetica vessatorietà delle clausole ai sensi del codice del consumo e la legittimità della condotta dell'*hosting provider* sotto il profilo contrattuale.

Su questi punti, il Tribunale si pronuncia su alcuni aspetti di rilievo.

Il primo concerne il richiamo dei principi generali del codice civile e, precisamente, della disciplina dell'eccezione di inadempimento e l'esclusione della possibilità di inquadrare una tale previsione tra quelle tipizzate dal codice del consumo[1].

Tale precisazione appare a monte corretta perché, indipendentemente dall'esistenza di una precisa previsione contrattuale, la posizione dell'*hosting provider*, anche alla luce della recente giurisprudenza europea, non rende a mio avviso irragionevole – trattandosi anzi di una corretta informazione all'utenza – la precisazione contrattuale in merito all'esistenza di un potere immediato di intervento, quanto meno in presenza di contenuti che possano considerarsi illeciti e, a maggior ragione, ove gli stessi siano lesivi dell'onore e della reputazione di terzi soggetti[2] e ciò anche tenuto conto delle responsabilità che, sul piano risarcitorio, possono discendere da una posizione di inerzia[3].

---

[1] Correttamente il Tribunale osserva come l'indagine del Giudice debba valutare se la previsione implichi un significativo squilibrio nella posizione delle parti con riferimento alle posizioni contrattuali, ma sul punto si veda E. Bevilacqua-M.Labriola, *Codice del consumo: clausole vessatorie nei contratti di mutuo bancario ed intervento del notaio*, Consiglio Nazionale del Notariato, Studio n. 237-2006/C, in *Studi e Materiali CNN*, Milano, 2, 2006, 1332 ss. in cui si precisa che «il significativo squilibrio investe di fatto il giudice di notevole potere discrezionale nell'esame del caso concreto, dovendo questi ravvisare uno svantaggio del consumatore, nell'ambito delle posizioni contrattuali, di entità considerevole, dato non sempre agevolmente accertabile. In ogni caso dovrà trattarsi di uno squilibrio normativo (diritti ed obblighi del contratto) e non già di uno squilibrio economico, considerato che l'art. 34, comma 2, dispone che la valutazione del carattere vessatorio di una clausola non attiene all'adeguatezza del corrispettivo dei beni e servizi».

[2] Sul punto, come è noto, si è pronunciata la Corte di giustizia nella causa C-18/18, avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'art. 267 TFUE, dall'Oberster Gerichtshof (Corte Suprema, Austria) e che è stata decisa con sentenza del 25 ottobre 2017, pervenuta in cancelleria il 10 gennaio 2018, nel procedimento Eva Glawischnig-Piesczek contro Facebook Ireland Limited prevedendo che «alla luce di tutte le considerazioni che precedono, occorre rispondere alle questioni prima e seconda dichiarando che la direttiva 2000/31, in particolare il suo articolo 15, paragrafo 1, deve essere interpretata nel senso che essa non osta a che un giudice di uno Stato membro possa: - omissis - ordinare a un prestatore di servizi di hosting di rimuovere le informazioni oggetto dell'ingiunzione o di bloccare l'accesso alle medesime a livello mondiale, nell'ambito del diritto internazionale pertinente».

[3] Recentemente, la Corte di Cassazione ha osservato che «nell'ambito dei servizi della società dell'informazione, la responsabilità dell'hosting provider, prevista dal D.Lgs. 9 aprile 2003, n. 70, art. 16, sussiste in capo al prestatore dei servizi che non abbia provveduto alla immediata rimozione dei contenuti illeciti, nonché se abbia continuato a pubblicarli, pur quando ricorrano congiuntamente le seguenti condizioni: a) sia a conoscenza legale dell'illecito perpetrato dal destinatario del servizio, per averne avuto notizia dal titolare del diritto leso oppure aliunde; b) l'illiceità dell'altrui condotta sia ragionevolmente constatabile, onde egli sia in colpa grave per non averla positivamente riscontata, alla stregua del grado di diligenza che è ragionevole attendersi da un operatore professionale della rete in un determinato momento storico; c) abbia la possibilità di attivarsi utilmente, in quanto reso edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere».

2. Il necessario vaglio giurisdizionale sulla regolamentazione contrattuale

Quest'ultimo rilievo vale a introdurre il secondo punto di interesse che viene evidenziato nella decisione impugnata e che concerne l'ampiezza del concetto di disinformazione e il cui corretto inquadramento riflette i propri effetti sopra l'efficacia – nella valutazione di un eventuale squilibrio nella posizione dei contraenti – di una previsione contrattuale che disponga una limitazione dei diritti di manifestazione del pensiero in considerazione degli standard di comportamento condivisi e sottoscritti dagli aderenti a una piattaforma online.

La questione sarebbe di amplissimo respiro e non consente di essere adeguatamente trattata nell'ambito di un breve commento alla decisione atteso che il tema involge aspetti fondamentali del nostro ordinamento giuridico – sui quali la decisione in effetti si sofferma lungamente – quali il diritto di esprimere liberamente il proprio pensiero ai sensi dell'art. 21 della Costituzione.

La nostra riflessione può, tuttavia, muovere da un diverso punto di vista ossia il parallelismo con una diversa fattispecie in cui la sensibilità degli aderenti a una determinata formazione sociale può tradursi in norme vincolanti e, correlativamente, nelle conseguenti sanzioni.

Il riferimento è, in una prospettiva storica, all'organizzazione degli ordinamenti professionali nei quali le norme deontologiche di comportamento, in mancanza di una precisa regolamentazione da parte del legislatore, erano state originariamente inquadrate dalla nostra giurisprudenza di legittimità quali vere e proprie disposizioni contrattuali di comportamento[4].

L'attualità di questo paragone discende dagli sforzi che, da ultimo, sono stati posti in essere a livello europeo nell'incentivare, anche attraverso il recente Digital Services Act, l'adozione di codici di condotta da parte delle piattaforme operanti su internet e la sensibilizzazione rispetto ai rischi connessi alle campagne di disinformazione[5].

---

[4] Così, ad esempio in motivazione per il sistema disciplinare forense, v. Cass. civ., sez. un., 10 luglio 2003, n. 10842: «Deve, infatti, affermarsi che le disposizione dei codici deontologici predisposti dagli Ordini professionali, se non recepite direttamente da una norma di legge (ad esempio in materia di segreto professionale, tutelato anche nei confronti dell'autorità giudiziaria), non hanno né la natura né le caratteristiche di norme di legge, come tali assoggettabili al criterio interpretativo di cui all'art. 12 delle preleggi, ma sono espressione dei poteri di autorganizzazione degli Ordini (o Collegi) si da ripetere la loro autorità - come evidenziato in dottrina - oltre che da consuetudini professionali anche da norme che i suddetti Ordini (o Collegi) emanano per fissare gli obblighi di correttezza cui i propri iscritti devono attenersi e per regolare la propria funzione disciplinare. Alla stregua di quanto ora detto, quindi, le suddette disposizioni vanno interpretate nel rispetto dei canoni ermeneutici fissati dagli artt. 1363 c.c. e segg., sicché è denunziabile in Cassazione ex art. 360 c.p.c., n. 3 la violazione o falsa applicazione dei suddetti canoni - con la specifica indicazione di quelli tra essi in concreto disattesi - oltre che il vizio di motivazione ex art. 360 c.p.c., n. 5 non riscontrabile allorquando - come nel caso di specie - si intenda far prevalere sulla logica e coerente interpretazione seguita nel giudizio di merito una diversa opzione ermeneutica patrocinata dalla parte ricorrente».

[5] Così il considerando 88, del recente regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) all'interno del quale si precisa che «i motori di ricerca online di dimensioni molto grandi potrebbero aver bisogno di rafforzare i loro processi interni o la vigilanza sulle loro attività, in particolare per quanto riguarda il rilevamento dei rischi sistemici,

Il parallelismo, tuttavia, deve arrestarsi a questo piano generalissimo perché la successiva evoluzione normativa e giurisprudenziale ha riconosciuto il carattere pubblicistico della regolamentazione deontologica[6]; la relativa vincolatività su un piano giuridico anche in considerazione della funzione sociale alla quale assolvono i professionisti iscritti a un Albo professionale; il carattere amministrativo dei provvedimenti disciplinari[7] e, da ultimo, le specifiche finalità alle quali assolve la normativa deontologica a tutela della collettività nonché del decoro e della dignità professionali[8], con la correlativa esigenza di prevedere una disciplina che è ascrivibile a una fonte normativa secondaria legittimata da un apposito testo di legge.

Ebbene, al di là della impossibilità di poter ravvisare allo stato le medesime caratteristiche ora menzionate negli *standard* di comportamento di una pluralità indeterminata di soggetti che aderiscano a una piattaforma social – le quali allo stato non possono costituire altro che una regolamentazione pattizia – l'aspetto rilevante risiede nel fatto che, in entrambi gli ambiti, le norme paiono assolvere anche alla funzione di orientare i comportamenti al fine di tutelare la collettività e possono giustificare un controllo giurisdizionale[9].

---

e di effettuare valutazioni dei rischi più frequenti o mirate in relazione alle nuove funzionalità. In particolare, laddove i rischi siano condivisi tra diverse piattaforme online o motori di ricerca online, dovrebbero cooperare con altri prestatori di servizi, anche avviando codici di condotta o aderendo a codici di condotta esistenti o ad altre misure di autoregolamentazione. Dovrebbero inoltre prendere in considerazione azioni di sensibilizzazione, in particolare qualora i rischi siano connessi a campagne di disinformazione». In argomento v. recentemente, D. D'Alberti, *Google e le nuove autorità private: la metamorfosi dal fatto al diritto* in *Riv. Dir. Civ.,* 2021, 745 ss.

[6] Così, sempre con riferimento al sistema disciplinare forense, Cass. civ., sez. un., 29 dicembre 2017, n. 31227 secondo la quale: «Le deliberazioni con le quali il Consiglio nazionale forense procede alla determinazione dei principi di deontologia professionale e delle ipotesi di violazione degli stessi costituiscono regolamenti adottati da un'autorità non statuale in forza di autonomo potere in materia che ripete la sua disciplina da leggi speciali, in conformità dell'art. 3 disp. gen., comma 2, onde, trattandosi di legittima fonte secondaria di produzione giuridica, va esclusa qualsiasi lesione del principio di legalità, considerando altresì non tanto le tipologie delle pene disciplinari quanto l'entità delle stesse tra un minimo ed un massimo che ove graduabili, siano prestabilite dalla normativa statuale».

[7] Sul punto, v. da ultimo, R. Danovi, *Ordinamento forense e deontologia*, Milano 2023, 123, in cui si legge tra l'altro che «la giuridicità dell'ordinamento professionale e delle regole deontologiche è data anche dal fatto che la violazione di tali norme non comporta sanzioni morali ma sanzioni giuridiche, espressamente previste dall'ordinamento a conclusione di un procedimento disciplinare giurisdizionale (almeno nella seconda fase), con il controllo finale delle sezioni unite della Cassazione in sede di legittimità (tra l'altro per violazione di legge)».

[8] Recentemente, la Corte costituzionale ha evidenziato le ampie funzioni a cui assolvono le norme disciplinari precisando che «ben potendo in particolare le sanzioni disciplinari essere orientate, oltre che agli scopi di prevenzione generale e speciale, insiti in ogni tipo di sanzione, anche all'obiettivo di preservare l'integrità etica e l'onorabilità della professione, nonché a quello di assicurare la rimozione dalle funzioni di persone dimostratesi non idonee, o non più idonee, all'assolvimento dei propri doveri (sentenze n. 197 del 2018 e n. 161 del 2018), senza dover essere necessariamente finalizzate anche alla "rieducazione" della persona colpita dalla sanzione» (cfr. in materia notarile, Corte cost., 29 maggio 2019, n. 133).

[9] Così, proprio con riferimento alla compatibilità di una norma deontologica con i principi dettati dall'art. 21 Cost., v. recentemente e in motivazione Cass. civ., sez. un., 14 dicembre 2022, n. 36660: «Al riguardo va ribadito che, ai fini della responsabilità disciplinare dell'avvocato, le espressioni sconvenienti od offensive vietate dall'art. 20 del codice deontologico forense (nel testo applicabile "ratione temporis", oggi art. 52) rilevano di per sé, a prescindere dal contesto in cui sono usate e dalla veridicità dei fatti che ne sono oggetto (Cass. S.U. n. 11370 del 31/05/2016; Cass. S.U. n. 11370/2016), dovendosi escludere

E sotto tale profilo, appare corretta l'affermazione svolta nel provvedimento annotato secondo la quale l'autonomia privata esercitata nell'elaborazione di norme di comportamento alle quali gli utenti aderiscono non è illimitata, né insindacabile, essendo soggetta, oltreché al rispetto delle norme imperative, *ex* art. 1418 c.c., ai limiti che la legge impone alla autonomia contrattuale[10].

3. Il bilanciamento tra i diritti costituzionali

A ciò, il Tribunale aggiunge anche una riflessione in merito alla coerenza del contenuto degli standard rispetto ai valori costituzionali con specifico riferimento alla libertà di manifestazione del pensiero sancita dall'art. 21 Cost.
E anche a tale riguardo viene dettato un principio corretto, ossia quello secondo il quale lo strumento di internet – essendo rivolto a una pluralità indifferenziata di persone – è meritevole di ricevere le garanzie costituzionali previste dall'art. 21 Cost. per «ogni mezzo di diffusione» sicché, in linea astratta, anche ipotetiche limitazioni contrattuali a tale diritto dovrebbero essere recessive ove connesse alla attività di impresa, pur tutelata dall'art. 42 Cost., dell'*hosting provider*.
E, in effetti, anche in ambito deontologico una ipotetica limitazione del diritto costituzionale di esprimere il proprio pensiero (al pari di ogni limitazione di un diritto costituzionale) dovrebbe considerarsi illegittima ove imposta puramente e semplicemente da una norma professionale senza una precisa copertura costituzionale suscettibile di essere valutata in concreto dalla magistratura attraverso una delicata opera di bilancia-

che tale divieto, appunto previsto a salvaguardia della dignità e del decoro della professione, si ponga in contrasto con il diritto, tutelato dall'art. 21 Cost., di manifestare liberamente il proprio pensiero, il quale non è assoluto ma trova concreti limiti nei concorrenti diritti dei terzi e nell'esigenza di tutelare interessi diversi, anch'essi costituzionalmente garantiti (Cass. S.U. n. 13168 del 17/05/2021)».

[10] In questo senso, v. recentemente, G. Alpa, *Sul potere contrattuale delle piattaforme digitali*, in *Contr. e Impr.*, 2022, 721 ss., il quale osserva come «il potere normativo si estrinseca nella imposizione di clausole contrattuali relative al servizio reso. Esse sono disciplinate dal diritto interno e, per certi aspetti, dal diritto dell'Unione europea e dal diritto interno di derivazione europea. Pertanto, anche se le piattaforme sono considerate come soggetti privati che operano nell'ordinamento giuridico transnazionale, esse non si potranno sottrarre alla disciplina dell'Unione europea e alle regole del diritto interno di derivazione europea. Accanto alla disciplina del rapporto contrattuale, nel diritto interno (e sempre in connessione con il diritto dell'Unione europea) si sono considerati diversi settori in cui già sono state introdotte regole che producono effetti anche nei confronti delle (imprese che governano le) piattaforme, come la tutela del consumatore, la tutela della concorrenza, la tutela del diritto d'autore, la tutela del marchio, la tutela dei dati personali. Come ogni impresa, le piattaforme debbono rispettare i diritti fondamentali, e, se possiedono i requisiti stabiliti dalle leggi in materia, debbono predisporre il bilancio non finanziario e partecipare al programma degli obiettivi di ESG (Environmental Social Governance) predisposto dall'ONU con termine finale il 2030. Il fatto, dunque, di essere classificate come «private transnational legal orders» non le esime dall'osservare le regole del diritto privato degli ordinamenti nazionali e dell'Unione europea: dal punto di vista del diritto interno esse sono imprese multinazionali al pari di altre imprese che operano nel campo della produzione di beni e servizi o nel campo della distribuzione. Ovviamente, il loro peso specifico deve esser considerato anche dal punto di vista del diritto pubblico, e quindi nella costruzione della pubblica opinione, nella circolazione di idee ed opinioni, nella dialettica del gioco democratico, poiché la circolazione dei dati di ogni tipo, che esse provocano, si intreccia con la vita democratica di un Paese, così come l'uso degli elaboratori elettronici, di Internet e degli altri strumenti di comunicazione».

mento degli interessi coinvolti[11].

4. Conclusioni

La parte finale della decisione merita, invece, un supplemento di riflessione.
Nella stessa, il Tribunale analizza in concreto gli "standard della community" e giudica gli stessi come non vessatori in quanto coerenti rispetto ai valori costituzionali previsti dall'art. 21 Cost. perché volti a preservare una serie di diritti parimenti rilevanti e tutelati dalla legge, quali la sicurezza, la *privacy* e la dignità nonché, nel caso specifico e con riferimento al tema della disinformazione, la tutela della salute pubblica quale diritto avente sicura rilevanza costituzionale.
Da questo giudizio di compatibilità viene fatta quindi discendere la correttezza della decisione assunta dall'*hosting provider* e la proporzionalità dei provvedimenti concretamente adottati (rimozione del *post* e blocco del profilo dell'utente per il periodo di 30 giorni) non potendosi ravvisare nel caso di specie un rifiuto della prestazione non conforme a buona fede ai sensi dell'art. 1460 c.c.
Più nello specifico, in uno degli ultimi passaggi della decisione, il Tribunale ammette la pubblicazione come parzialmente legittima in quanto riconducibile al diritto di critica e, quindi, di manifestazione del pensiero, ma rileva per contro la presenza di alcuni contenuti vietati dagli "standard della community" (giudicati come coerenti con i principi del nostro ordinamento) e, pertanto, considera non contraria a buona fede la relativa rimozione e i provvedimenti assunti dall'*hosting provider*.
Senonché, e senza voler entrare nel merito della decisione sul caso concreto, a me pare che il ragionamento svolto suggerisca un ulteriore approfondimento.
I principi indicati nella decisione – pur con tutti i limiti di un commento che non ha a disposizione gli atti del processo – paiono costituire una risposta corretta ed equilibrata alle domande proposte nel corso del giudizio con riferimento al carattere asseritamente vessatorio delle clausole contrattuali[12].

[11] Fermo restando che la stessa non potrebbe essere denunciata autonomamente alla Corte costituzionale, ma sul punto v. recentemente Cass. civ., sez. un., 8 marzo 2022, n. 7501 secondo la quale «Manifesta è infine l'inammissibilità della eccezione di illegittimità costituzionale sollevata. Come si è sopra evidenziato, le norme del codice disciplinare forense costituiscono fonti normative integrative del precetto legislativo. Esse hanno dunque, per un verso, natura normativa (si consideri che dopo l'emanazione da parte del CNF, il codice disciplinare viene pubblicato sulla Gazzetta Ufficiale), per l'altro la loro precettività non è autosufficiente, in quanto è proiezione della norma legislativa che ne costituisce la fonte (L. n. 247 del 2012, art. 3, art. 35, comma 1, lett. d e art. 65, comma 5). Come rilevò Cass. Sez. U. n. 26810 del 2007, il precetto normativo risulta dalla norma di rinvio e dalla fonte che lo integra, la quale non avrebbe titolo per essere vincolante in mancanza della norma di rinvio. La disposizione del codice deontologico viene così ad acquistare la natura di norma interposta, necessaria per dare concretezza al precetto normativo che altrimenti resterebbe in bianco, secondo un fenomeno noto all'ordinamento giuridico. La denuncia di illegittimità costituzionale è stata proposta direttamente nei confronti della norma interposta, senza passare attraverso la denuncia di illegittimità della norma di rinvio che ne fonda la precettività giuridica. Assunta in modo solipsistico, la disposizione del codice deontologico costituisce atto privo della forza di legge, conseguendo tale forza solo all'integrazione del precetto legislativo. Di un atto privo della forza di legge non può essere predicata l'illegittimità sul piano costituzionale».

[12] Con la difficoltà, peraltro, di ammettere che la materia possa essere considerata *tout court* oggetto

A ciò si può aggiungere che la risposta data dal Tribunale, nel senso di ritenere legittima la rimozione preventiva di notizie giudicate come contrastanti con il canone contrattuale di evitare forme di disinformazione potenzialmente dannose per la salute pubblica, si inserisce nel solco del dibattito normativo e dottrinale in corso e appare in linea con le indicazioni programmatiche provenienti dall'Unione europea nel senso di promuovere un controllo attivo da parte delle grandi piattaforme online rispetto ai contenuti non veritieri o illeciti presenti in rete[13]. Si tratta, del resto, di indicazioni ed esigenze già note al nostro ordinamento – espresse normativamente ad esempio con riferimento all'esercizio della professione giornalistica ed ivi accompagnate anche da sanzioni di carattere disciplinare nella misura in cui si prevede un obbligo generale di rettificare le notizie che risultino inesatte e riparare gli eventuali errori[14] – in cui

di previsioni contrattuali cogenti anche perché l'eventuale vessatorietà delle clausole implicherebbe paradossalmente l'ammissibilità di una trattativa individuale, in argomento v. L. Valle, *L'inefficacia delle clausole vessatorie e il codice del consumo,* in *Contr. e Impr.,* 2006, 662 ss. secondo la quale «la disciplina delle clausole vessatorie nei contratti con i consumatori è fondata sul controllo dell'equilibrio della singola operazione contrattuale; tanto che lo squilibrio a danno del consumatore prodotto da una clausola potrebbe essere compensato dal contenuto favorevole al consumatore di un'altra clausola del contratto o di un contratto a questo collegato. Ed è altresì fondata sulla regolazione, e non sul divieto, dell'esercizio dell'autonomia privata, nel senso che, se la clausola sia frutto di una trattativa individuale condotta dal professionista con il consumatore, essa non è vessatoria (ex art. 1469 ter, comma 4°, art. 34, comma 4°, codice del consumo). Quest'ultimo carattere accomuna la disciplina delle clausole vessatorie nei contratti con il consumatore a quella generale data all'art. 1341. In ragione di queste sue caratteristiche si è appunto sottolineata la differenza dell'inefficacia delle clausole vessatorie nei contratti con il consumatore rispetto alle diverse discipline della nullità di singole clausole, che pure interessano i contratti con il consumatore e più in generale con il cliente (considerato parte debole del contratto). E se ne è invece individuata la comunanza di impostazione con le discipline della nullità del patto che realizza l'abuso della dipendenza economica e degli accordi gravemente iniqui sui termini di pagamento e sulle conseguenze del ritardato pagamento nelle transazioni commerciali».

[13] In questo senso, si può citare, ad esempio, la *Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the regions*, *Action Plan against Disinformation* della Commissione europea in cui si indica che «*Social media have become important means of spreading disinformation, including in some cases, like Cambridge Analytica, to target the delivery of disinformation content to specific users, who are identified by the unauthorised access and use of personal data, with the ultimate goal of influencing the election results. Recent evidence shows that private messaging services are increasingly used to spread disinformation. Techniques include video manipulation (deep-fakes) and falsification of official documents; the use of internet automated software (bots) to spread and amplify divisive content and debates on social media; troll attacks on social media profiles and information theft. At the same time, more traditional methods such as television, newspapers, websites and chain emails continue to play an important role in many regions. The tools and techniques used are changing fast – the response needs to evolve just as rapidly*» e come, tra i pilastri di intervento, le grandi piattaforme online dovrebbero "*should immediately (i) ensure scrutiny of adplacement and transparency of political advertising, based on effective due diligence checks of the identity of the sponsors, (ii) close down fake accounts active on their services and (iii) identify automated bots and label them accordingly. Online platforms should also cooperate with the national audio-visual regulators and with independent fact-checkers and researchers to detect and flag disinformation campaigns in particular during election periods and to make fact-checked content more visible and widespread*».

[14] Così l'art. 2 della legge 3 febbraio 1963, n. 69, recante "Ordinamento della professione di giornalista", la cui importanza è stata meritevolmente evidenziata all'art, 1 del Testo Unico dei doveri del giornalista adottato dal Consiglio Nazionale contenente le norme deontologiche applicabili e che riproduce, sotto la rubrica Libertà d'informazione e di critica che «l'attività del giornalista, attraverso qualunque strumento di comunicazione svolta, si ispira alla libertà di espressione sancita dalla Costituzione italiana ed è regolata dall'articolo 2 della legge n. 69 del 3 febbraio 1963: "È diritto insopprimibile dei giornalisti la libertà d'informazione e di critica, limitata dall'osservanza delle norme di legge dettate a tutela della personalità altrui ed è loro obbligo inderogabile il rispetto della verità sostanziale dei fatti, osservati sempre i doveri imposti dalla lealtà e dalla buona fede. Devono essere rettificate le notizie che risultino inesatte e riparati gli eventuali errori. Giornalisti e editori sono tenuti a rispettare il segreto professionale

la falsità delle notizie e delle pubblicazioni in generale costituisce il presupposto per forme di responsabilità operanti anche al di fuori dell'ambito contrattuale e che si sta affermando con maggiore incisività anche nella normativa europea[15].

In questo senso, e pur con l'auspicio di una presa di posizione precisa da parte del legislatore nazionale, il controllo operato dal Tribunale appare coerente con l'esigenza di contrastare situazioni potenzialmente lesive per la salute pubblica e appare in linea con l'insegnamento della Corte di giustizia, giustamente richiamato anche nella decisione in commento, secondo il quale le limitazioni alla libertà di pensiero alla stregua della CEDU non possono essere oggetto di restrizioni diverse da quelle che siano stabilite dalla legge e che costituiscono misure necessarie, in una società democratica, alla pubblica sicurezza, alla protezione dell'ordine, della salute o della morale pubblica, o alla protezione dei diritti e della libertà altrui[16].

sulla fonte delle notizie, quando ciò sia richiesto dal carattere fiduciario di esse, e a promuovere lo spirito di collaborazione tra colleghi, la cooperazione fra giornalisti e editori, e la fiducia tra la stampa e i lettori"».

[15] Sul punto, anche per ulteriori riferimenti, v. recentemente M. A. Astone, *Digital Services act e nuovo quadro di esenzione dalla responsabilità dei prestatori di servizi intermediari: quali prospettive?*, in *Contr. e Impr.*, 2022, 1050 la quale, con riferimento al recente regolamento europeo, osserva che «l'obiettivo è quello di intervenire sulla governance di internet, per tutelare gli utenti e per creare un mercato digitale articolato intorno a due linee di azione: l'inserimento dei servizi resi dalle piattaforme on line all'interno della più generale categoria dei servizi di hosting; la sicurezza della tecnologia e la protezione della persona umana da contenuti illegali e dannosi. L'obiettivo è, in particolare, quello di porre le basi per mercati equi e contendibili, come si evince dalla considerazione dell'altro Regolamento, quello sui mercati digitali, strettamente correlato al Digital services act, che nei servizi resi dalle piattaforme ricomprende quelli che presuppongono un ruolo attivo del gestore della piattaforma (per esempio motori di ricerca online; servizi di social network online; servizi di piattaforma per la condivisione di video). Ma soprattutto il DSA introduce uno statuto normativo più gravoso per le imprese di grandi dimensioni che gestiscono piattaforme - i c.d. Gatekeepers - sottoposti a stringenti obblighi riguardanti sia il trattamento dei dati personali, considerato che le loro dimensioni imprenditoriali e territoriali facilitano la trasmissione rapida e la circolazione delle informazioni, sia la prevenzione di squilibri contrattuali nei confronti degli utenti finali dei servizi di piattaforma di base. A tali obblighi si aggiungono pure divieti di pratiche sleali e di condizioni inique a presidio della concorrenza e della protezione del mercato digitale. Da tale statuto normativo emerge l'avvio di una nuova strategia. Infatti la tecnica utilizzata non è più fondata sulla riparazione, come nella direttiva 2000/31/CE, piuttosto sulla prevenzione e sulla responsabilizzazione dei fornitori di piattaforme on line; ciò si realizza con la previsione di obblighi di predisposizione di codici di condotta e della sottoscrizione di accordi di autoregolamentazione e di co-regolamentazione per lo svolgimento di una attività di moderazione dei contenuti, come già previsto dalla direttiva sui servizi media audiovisivi».

[16] Così, anche recentemente, CGUE, C-336/19, *Centraal Israëlitisch Consistorie van België e.a.* (2020).

NFT e proprietà intellettuale: problemi e prospettive*

Sveva Ruggiero

Tribunale di Roma, sez. Impresa, 20 luglio 2022

È illegittima la creazione di *NFT* riproducenti un calciatore nell'atto di indossare la maglia da gioco di una squadra calcistica, se quest'ultima non ha autorizzato allo scopo l'utilizzo del proprio marchio.
La circostanza che il calciatore abbia autorizzato lo sfruttamento della propria immagine non esclude infatti l'obbligo per la società autrice dei tokens di richiedere altresì alla società calcistica, di cui sono riprodotte le maglie da gioco, apposita autorizzazione al fine di poterne utilizzare il marchio. Infatti, la creazione e offerta in vendita di *non fungible tokens* costituisce un'operazione di carattere commerciale, sulla quale incide significativamente la notorietà dei club calcistici interessati dalla riproduzione digitale. Ne deriva che tale mancata autorizzazione determina un concreto rischio confusorio nel pubblico, indotto a credere che gli NFT immessi sul mercato provengano dalla società calcistica la cui maglia viene riprodotta o da società alla prima collegate.

Sommario

1. La pronuncia del Tribunale di Roma. - 2. Natura e funzione degli *NFT*. - 3. Gli *NFT* nel panorama americano. - 4. Gli interrogativi giuridici sollevati in materia di proprietà intellettuale.

Keywords

NFT - blockchain - marchi - diritto d'autore - proprietà intellettuale.

1. La pronuncia del Tribunale di Roma

Con ordinanza del 20 luglio 2022, un Tribunale italiano si è per la prima volta pronunciato su una vicenda legata all'uso e alla commercializzazione degli ormai famigerati *NFT* (*Non-Fungible tokens*). I fatti di causa si incentrano, in particolare, sull'avvenuta richiesta di inibitoria cautelare avanzata al Tribunale di Roma da parte della nota società calcistica Juventus S.p.A., volta ad impedire ogni ulteriore «produzione, commercializzazione, promozione e offerta in vendita, diretta e/o indiretta, in qualsiasi modo

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

e forma» degli *NFT* creati e commercializzati dalla società *Blockeras s.r.l.* raffiguranti l'ex calciatore Christian Vieri con indosso la maglia del club ricorrente e l'indicazione del nome della squadra. A detta della società Juventus tale condotta avrebbe costituito una lesione del marchio figurativo della società, costituito appunto dalla maglia a strisce verticali di colore bianco e nero con due stelle sul petto, simbolo della squadra torinese.

La ricorrente ha avanzato altresì richiesta al Tribunale di fissare una somma di denaro a titolo di *astreintes* per ogni giorno di ritardo nell'attuazione dei provvedimenti richiesti, oltre alla pubblicazione del provvedimento giurisdizionale su due celebri quotidiani italiani.

La società resistente, autrice degli *NFT* in questione, si è opposta deducendo la carenza dei presupposti del provvedimento cautelare, in particolare del *periculum in mora*, la sussistenza del proprio diritto all'utilizzo e alla commercializzazione dei *tokens,* nonché contestando la tutelabilità del marchio Juventus in ambito digitale, posto che lo stesso non risultava registrato nella categoria dei prodotti virtuali suscettibili di *download* di cui alla classe 9 della Convenzione di Nizza.

La pronuncia del giudice romano, disattendendo le menzionate contestazioni, ha accolto i motivi della ricorrente, affermando innanzitutto la sussistenza del *fumus boni iuris*, ossia la verosimile esistenza del diritto alla tutela del proprio marchio figurativo, oggetto di titolarità non contestata, e comunque dotato di notorietà generalizzata, tale da attribuirgli la tutela rafforzata di cui all'art. 20 del d.lgs 30/2005 (cd. Codice della proprietà industriale).

É infatti noto che, ai sensi del c. 1, lett. c), del citato articolo, il marchio registrato dotato di notorietà gode di una tutela particolarmente rafforzata, tale da impedire l'utilizzo di un segno identico o simile anche in relazione a prodotti non affini a quelli per cui il marchio risulta registrato, laddove l'uso indebito del segno consenta all'utilizzatore di trarre indebitamente vantaggio dal carattere distintivo del marchio notorio o di recare pregiudizio al legittimo titolare di quest'ultimo[1].

Ebbene, il Tribunale ha riconosciuto l'esistenza di un rischio confusorio legato all'illegittimo sfruttamento del marchio Juventus in relazione all'indebita apposizione dello stesso sugli *NFT* oggetto di esame, determinandosi la concreta possibilità che il pubblico «possa credere che i prodotti o servizi di cui trattasi provengano dalla stessa impresa o da imprese economicamente collegate». La Corte ha ulteriormente evidenziato come la circostanza dell'esistenza di un contratto tra la società autrice dei *tokens* e il calciatore Vieri, tale da autorizzare l'utilizzazione dell'immagine di quest'ultimo, non escludeva l'obbligo di richiedere altresì apposita e separata autorizzazione anche alla società Juventus, al fine di poterne utilizzare il relativo marchio.

Né, peraltro, ha osservato il Tribunale, la legittimità dell'operazione di commercializzazione dei *tokens* poteva ammettersi invocando l'art. 97 della legge sul diritto d'autore

[1] É noto come la tutela dei marchi registrati risulti particolarmente rafforzata, data la specifica disciplina del marchio dotato di rinomanza ai sensi degli artt. 12, c. 1, lett. e) e 20, c. 1, lett. c). Si tratta, in particolare, di una tutela che talvolta prescinde da una confondibilità in concreto basandosi, invece, su un accertamento, per così dire, "virtuale", ossia fondato su una presunzione di confondibilità, come accade ad esempio quando segni identici al marchio registrato vengano apposti su prodotti identici. Si veda sul punto A. Vanzetti – V. Di Cataldo – *Manuale di diritto industriale*, Milano, 2021, 240-242.

(l. 633/1941), ai sensi del quale non occorre il consenso della persona ritratta, qualora «la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico». E ciò non solo perché la finalità dell'operazione era unicamente commerciale, ma anche in quanto, come già osservato, la prestazione del consenso da parte del calciatore all'utilizzo della propria immagine non escludeva la necessità di richiedere separata autorizzazione alle squadre le cui maglie da gioco venivano rappresentate negli *NFT* e il cui marchio risultava così indebitamente utilizzato.
A fronte poi della contestazione proposta dalla società resistente per cui la tutela del marchio Juventus sarebbe stata preclusa in ambito digitale, non risultando il marchio registrato rispetto alla categoria relativa ai prodotti scaricabili, il Tribunale ha osservato ancora che il marchio in esame risulta registrato nella classe 9 relativa alle classi merceologiche indicate dalla Convenzione di Nizza[2], comprensiva altresì di prodotti non espressamente indicati, quali le pubblicazioni elettroniche scaricabili[3]. Pertanto, nemmeno da questo punto di vista il Tribunale ha rilevato impedimenti di sorta alla tutela del marchio.
La condotta della società autrice delle *cards* raffiguranti il calciatore è stata ritenuta illegittima dal Tribunale anche per un altro motivo, integrando un'ipotesi di concorrenza sleale, mediante uso non autorizzato del marchio altrui e conseguente appropriazione di pregi collegati al marchio indebitamente utilizzato.
Secondo la prospettiva dell'Autorità Giudicante, la condotta posta in essere dalla resistente ha infatti determinato una concreta possibilità di confusione nel pubblico, sfruttando la funzione distintiva del marchio Juventus in violazione dell'art. 2598 n. 1 c.c. (concorrenza sleale confusoria)[4], oltre a realizzare una illegittima appropriazione dei pregi riconducibili alla società ricorrente, in violazione dell'art. 2598 n. 2 c.c.
Così individuati i presupposti del *fumus boni iuris*, l'ordinanza in esame si sofferma infine sull'esistenza del *periculum in mora* che ritiene sussistente in relazione al rischio di volgarizzazione del marchio, oltre che alla lesione dei diritti di sfruttamento del marchio della ricorrente, suscettibili di cagionare alla stessa un danno di difficile quantificazione.
Pertanto il Tribunale ha accolto la domanda cautelare della ricorrente, ordinando l'inibizione di ogni ulteriore produzione e commercializzazione degli *NFT* indicati, oltre che l'utilizzo del marchio Juventus in ogni ulteriore forma e modalità. Il Tribunale ha altresì disposto il ritiro degli *NFT* presenti sui siti internet controllati dalla resistente

[2] La Classificazione Internazionale di Nizza prevede 34 classi di prodotti ed 11 classi di servizi, per un totale di 45 classi di prodotti e servizi. Ogni classe contiene, al suo interno, decine di prodotti e servizi.

[3] Tale approccio è conforme a quanto suggerito dall'Ufficio europeo (EUIPO) che, in data 23 giugno 2022, ha comunicato che i beni virtuali rientrano nella classe 9 poiché sono trattati come contenuti digitali o immagini.

[4] La tutela del marchio vede un'area di parziale sovrapposizione al divieto di concorrenza sleale confusoria di cui all'art. 2598, n. 1, c.c., ai sensi del quale «ferme le disposizioni che concernono la tutela dei segni distintivi e dei diritti di brevetto compie atti di concorrenza sleale chiunque: 1) usa nomi o segni distintivi idonei a produrre confusione con i nomi o i segni distintivi legittimamente usati da altri, o imita servilmente i prodotti di un concorrente, o compie con qualsiasi altro mezzo atti idonei a creare confusione con i prodotti e con l'attività di un concorrente».

attraverso i quali gli *NFT* erano offerti in vendita, fissando una penale per ogni giorno di ritardo nell'esecuzione del provvedimento cautelare emanato.

2. Natura e funzione degli *NFT*

La pronuncia esaminata rappresenta un punto di svolta nella perimetrazione dei diritti di proprietà intellettuale aventi ad oggetto una particolare categoria di beni ormai sempre più al centro della riflessione giuridica: gli *NFT*.

Gli *NFT*, acronimo di *Non-Fungible tokens*, sono dei certificati digitali basati sulla tecnologia *blockchain* volti a identificare in modo univoco, insostituibile e non replicabile la proprietà di un prodotto digitale[5].

In via generale, i *token* sono sequenze di informazioni registrate su *blockchain*, che rinviano in modo univoco al titolare delle informazioni medesime. Tali informazioni possono essere archiviate e trasmesse solo a soggetti autorizzati ad accedervi, così garantendo che i dati "tokenizzati" rimangano riservati.

Un *token* può essere "coniato" (dall'inglese "*minting*") sia in qualità di bene fungibile, sia con caratteristiche di infungibilità.

Nel primo caso, il *token* può essere scambiato con altro *token* dello stesso genere. Sono ad esempio *token* fungibili le criptovalute, dal momento che le stesse sono dotate di valore intrinseco e misurabile e possono essere utilizzate come mezzo di scambio sul mercato.

Nel secondo caso, invece, il *token* rappresenta beni infungibili: è questa l'ipotesi degli *NFT*, per l'appunto *Non-Fungible tokens*.

Gli *NFT* vengono utilizzati in relazione a contenuti digitali unici, quali immagini, video, opere d'arte. La memorizzazione degli stessi sulla rete *blockchain* consente di salvaguardare la paternità dei contenuti digitali che non possono essere rimossi o modificati proprio perché custoditi su tale rete. L'infungibilità degli *NFT* deriva dalla creazione di un numero limitato degli stessi da parte delle piattaforme che li generano (tra le varie *OpenSea, Rarible, Mintable*) o addirittura dalla loro creazione in edizione singola[6].

L'*NFT* rappresenta, in definitiva, un diritto su un bene digitale specifico. Tuttavia, l'acquisto di un *NFT* non comporta l'acquisizione della titolarità del bene materiale sottostante all'*asset* digitale, quanto la proprietà dell'*asset* digitale stesso, suscettibile

[5] Per maggiori approfondimenti si veda C. Trevisi – R. Moro Visconti – A. Cesaretti, *Non-Fungible Tokens (NFT): business models, legal aspects, and market valuation*, in questa *Rivista*, 1, 2022, 332 ss.

[6] Da questo punto di vista è possibile individuare in via generale due tipologie di *token*: a) l'LRC721, il *token* maggiormente utilizzato, è in grado di garantire l'unicità del bene o servizio compravenduto, assicurando al suo titolare la proprietà esclusiva del bene o del servizio acquistato. In tal senso, il proprietario esclusivo potrà invocare rispetto al bene acquistato tutte le forme di tutela da cui è assistita normalmente un'opera d'arte, garantendosi innanzitutto il diritto alla non riproducibilità dell'opera da parte di terzi. In questo caso ad un *token* viene associato un contratto, avente ad oggetto l'opera d'arte; b) l'altra tipologia di *token* utilizzabile è quello LRC 1155, che, al contrario del primo, associa un *token* a diversi contratti, in modo tale che l'opera risulta oggetto di diversi diritti di comproprietà, in una situazione analoga a quella che si avrebbe rispetto ad un'opera d'arte riprodotta in serie ma a tiratura limitata. É quanto accaduto, ad esempio, per l'opera di Andy Warhol "*14 small electric chairs*" del 1980, commercializzata sulla piattaforma *Maecenas* nel 2018 e associata a diversi *token*. Così P. Liberanome, *Criptoarte e nuove sfide alla tutela dei diritti autorali*, in *I Contratti*, 1, 2022, 93.

pertanto anche di essere trasferito a terzi.
Pare corretto affermare dunque che il *Non-Fungible Token* si limiti a certificare la titolarità di una delle poche copie digitali disponibili di un'opera originale.
In tal senso gli *NFT* ambiscono a traslare nel mondo digitale il concetto di "scarsità" di beni proprio del mondo fisico, rendendo uniche e irriproducibili rappresentazioni informatiche che per loro natura sarebbero al contrario replicabili all'infinito.
Alla luce della natura digitale, e dunque immateriale, del bene oggetto dell'*NFT*, si è resa necessaria l'implementazione di un sistema di autenticazione che consentisse di ricondurre univocamente la proprietà della copia digitale al suo esclusivo titolare: allo scopo, si è impiegata la già menzionata tecnologia *blockchain,* ossia un meccanismo che, sfruttando il sistema della crittografia, consente di convalidare la registrazione di molteplici transazioni su un registro immutabile, accessibile solo ai membri autorizzati della rete[7].
Nel caso degli *NFT*, all'interno della *blockchain* viene resa operante la tecnologia degli *smart contract*, ossia un protocollo di transazione computerizzato che esegue i termini di un contratto sulla base della ricezione di specifici *input*. Attraverso un contratto *smart* è possibile definire le condizioni per il trasferimento degli *NFT* attraverso le transazioni operate sulla rete *blockchain*.
Il meccanismo descritto risulta particolarmente significativo nell'ambito della circolazione di opere digitali, posto che lo stesso consente, ad esempio, di prevedere a favore dell'autore una percentuale risultante da ogni trasferimento dell'*NFT* successivo al primo. In questo modo l'autore dell'*NFT* si garantisce il diritto di ricevere ulteriori ricavi da ogni rivendita successiva della propria opera, al contrario di quanto normalmente avviene rispetto al trasferimento materiale dei beni, in cui gli artisti non ottengono ricavi aggiuntivi dopo aver trasferito la proprietà delle loro opere.
Il processo di "tokenizzazione" di beni materiali infungibili, quali opere d'arte, video o brani musicali, solleva una serie di interrogativi in ordine ai diritti di proprietà intellettuale facenti capo agli autori materiali dei lavori riprodotti in forma di *NFT*.
L'ordinanza cautelare analizzata affronta proprio tale questione, esaminandola dal punto di vista della tutela del marchio registrato, indebitamente utilizzato dai creatori dell'*NFT* "incriminato".

3. Gli *NFT* nel panorama americano

I predetti interrogativi stanno animando anche oltre oceano la discussione degli operatori del diritto, come si evince da due recenti controversie aventi ad oggetto l'indebito utilizzo di marchi registrati nella creazione di *NFT*, nonché di una ulteriore disputa legale connessa alle interferenze della vendita di *NFT* con il diritto d'autore[8].

[7] Per una descrizione tecnica del meccanismo di funzionamento della *blockchain* si veda *What is blockchain technology?,* in *ibm.com.*

[8] Per l'analisi del caso in esame si rimanda a *casetext.com*. La vicenda vede contrapporsi la nota casa di produzione *Miramax* al regista Quentin Tarantino. La prima sostiene che i diritti riservati del regista in relazione al film "*Pulp Fiction*" non sarebbero tali da giustificare la creazione e commercializzazione, da parte del regista, di *NFT* riproducenti bozze inedite della sceneggiatura originale del film, rispetto alla

In materia di *NFT* e tutela del marchio, la prima delle pronunce in esame vede protagonista l'azienda Nike contro la piattaforma di *reselling StockX,* in relazione alla vendita non autorizzata di «Valut NFT» riferiti a calzature materialmente offerte in commercio da *StockX* e riportanti il celebre marchio, simile ad una virgola capovolta, dell'azienda americana.

Quest'ultima, ritenendo tale operazione illecita, ha contestato l'indebito utilizzo del proprio marchio da parte del rivenditore, che lo avrebbe sfruttato decettivamente al fine di ottenere indebiti profitti, con ulteriore rischio di diluizione del marchio Nike, oltre che di indebita appropriazione di pregi.

La difesa di *StockX* si è basata sull'argomento per cui la stessa, lungi dal commercializzare *asset* digitali, si fosse limitata ad una rivendita autorizzata di modelli materiali di calzature Nike, descrivendo i relativi *NFT* come semplici "chiavi" per accedere al bene materiale conservato presso il rivenditore. Pertanto *StockX* ha negato che l'*NFT* fosse dotato di valore intrinseco, rappresentando un semplice strumento di accesso al bene fisico oggetto di offerta sul mercato[9].

Corre l'obbligo di osservare che, se è vero che gli *NFT* in contestazione sono collegati a modelli di calzature reali, dando all'acquirente il diritto di accedere al prodotto fisico custodito da *StockX*, gli stessi possono tuttavia circolare autonomamente in qualità di beni digitali, qualora il "riscatto" del bene materiale non venga esercitato.

In attesa della decisione della corte ci si chiede pertanto se i *Vault NFT* messi in circolazione da *StockX* rappresentino una sorta di ricevuta digitale connessa ad un bene materiale, e dunque espressione di un ordinario processo di vendita, o piuttosto siano prodotti a se stanti la cui circolazione comporta, pertanto, un indebito utilizzo del marchio altrui.

Altro caso connesso ad una vicenda di sfruttamento illecito del marchio altrui in relazione all'emissione di *NFT* si è avuto rispetto al caso *Hermès vs Mason Rothschild*[10].

La vicenda ha visto la casa di moda *Hermès* – titolare del marchio *Birkin* volto a designare le iconiche borse simbolo della *maison* – citare in giudizio l'artista *Mason Rothschild* per la commercializzazione di *NFT* connessi ad immagini di borse riportanti il marchio *MetaBirkin* e aventi caratteristiche simili a quelle proprie delle borse della celebre casa di moda francese, rivisitate nel materiale utilizzato (pelliccia).

Hermès ha quindi citato l'artista autore degli *NFT MetaBirkin* dinanzi al Tribunale Federale di New York, accusandolo di violazione e diluizione del marchio, *cybersquatting* e lesione della propria reputazione commerciale, e chiedendo, oltre all'ordine di inibizione di ogni ulteriore utilizzo del proprio marchio, il risarcimento dei danni subiti, comprensivi dei profitti realizzati mediante la vendita degli *NFT*.

L'artista si è difeso invocando il diritto alla libertà di espressione, sancito dal primo emendamento della Costituzione americana, in nome del quale egli avrebbe avuto diritto di utilizzare gli *NFT* delle *Meta Birkin* quale strumento di critica rispetto alla

quale sarebbe la *Miramax*, nella sua prospettazione, a detenere i relativi diritti.

[9] Si veda sul punto *stockx.com/lp/nfts/* in cui tale concetto è espresso indicando che «*Each Vault NFT is tied to a physical product (as depicted on the NFT), which is stored in our brand new, climate-controlled, high-security vaults*».

[10] Per una precisa descrizione dei fatti di causa si veda *castext.com.*

pratica di utilizzo di pellicce di animali per la produzione di borse e altri accessori di moda. In ciò avrebbe pertanto fatto uso legittimo del marchio *Hermès Birkin*.
Il Tribunale di New York, con una recente decisione del maggio 2022, si è preliminarmente pronunciato affermando che, se è vero che gli *NFT Meta Birkin* rappresentano opere d'arte digitale dotate di carattere espressivo, alle quali risulta pertanto applicabile la tutela del primo emendamento, d'altra parte l'uso del nome *MetaBirkin* presenta in ogni caso carattere ingannevole rispetto all'origine delle opere, idoneo ad ingenerare nel pubblico l'illegittima percezione della loro provenienza dalla casa di moda francese[11].
La vicenda è ancora pendente, ma dal preliminare pronunciamento della Corte pare potersi intravedere anche oltreoceano la tendenza a tutelare in maniera rafforzata i titolari di diritti di privativa industriale, a fronte del dilagante fenomeno degli *NFT*.

4. Gli interrogativi giuridici sollevati in materia di proprietà intellettuale

Si è visto come gli *NFT* rappresentino un fenomeno recente, rispetto al quale manca allo stato un quadro giuridico di riferimento.
Se negli USA alcune pronunce hanno iniziato ad esplorare il tema, in Italia non si hanno ancora decisioni, fatta eccezione per la commentata ordinanza del Tribunale di Roma, che rappresenta certamente un importante punto di partenza in materia.
Occorre pertanto interrogarsi sugli strumenti che il diritto offre per tutelare i soggetti coinvolti dall'emissione dei *Non-Fungible Tokens*, in particolare laddove tali strumenti minaccino di ledere i loro diritti di proprietà intellettuale.
Il primo interrogativo da cui partire, peraltro risolto dall'ordinanza del luglio 2022, si pone rispetto alla tutela del marchio registrato.
Ebbene, si è visto che non vi è nessun ostacolo rispetto alla tutela del marchio, laddove lo stesso sia violato dalla creazione di un *NFT* che ne faccia indebitamente uso.
Il problema – anch'esso in realtà risolto dall'ordinanza – si pone semmai soltanto laddove tale marchio non copra le classi relative a prodotti e servizi digitali.
Come osservato da alcuni commentatori[12], si nota come per superare tale ostacolo, sempre più marchi vengano depositati estendendo la registrazione del marchio anche a tali categorie di beni o servizi, per esempio, ai file multimediali suscettibili di *download* ricompresi nella Classe 9[13].

[11] Per il contenuto della decisione si veda *images.law.com.*

[12] M. Tavella, *Il parere del professionista – La creazione di un NFT in violazione di diritti di proprietà intellettuale altrui* in *Il diritto industriale*, 4, 2022, 394.

[13] Nella già citata comunicazione EUIPO del giugno 2022 si legge infatti che gli *NFT*, in quanto classificabili come "merci virtuali" sono ricompresi nella Classe 9, ferma restando la necessità di doverne meglio specificarne il contenuto all'atto della registrazione: «*The Office is increasingly receiving applications containing terms relating to virtual goods and non-fungible tokens (NFTs). This is the approach that the Office is taking for classification purposes. Virtual goods are proper to Class 9 because they are treated as digital content or images. However, the term* virtual goods *on its own lacks clarity and precision so must be further specified by stating the content to which the virtual goods relate (e.g. downloadable virtual goods, namely, virtual clothing). The 12th Edition of the Nice Classification will incorporate the term downloadable digital files authenticated by non-fungible tokens in*

Si è già visto come peraltro il problema assuma una portata più limitata laddove si tratti di marchi dotati di rinomanza, rispetto ai quali viene assicurata una più ampia tutela, venendo gli stessi protetti anche nei casi in cui il marchio non sia stato registrato per prodotti identici o affini (art. 20, c. 1, lett. c), c.p.i.).

Un secondo profilo rispetto al quale la creazione di *NFT* è suscettibile di creare conflitti, si ha rispetto al diritto d'autore.

Si è visto come non di rado gli *NFT* siano connessi a opere dell'ingegno umano (opere d'arte, immagini, video, musica); si realizza pertanto un conflitto nei casi in cui l'autore dell'*NFT* non sia altresì il creatore del prodotto sottostante, il cui diritto d'autore viene di conseguenza leso dalla creazione della copia digitale della propria opera d'ingegno.

Non vi è infatti dubbio che nei casi in cui la creazione di un *NFT* abbia quale necessario presupposto l'opera di un diverso autore, essa equivalga ad una forma di riproduzione della stessa, che come tale rientra tra i diritti esclusivi dell'autore[14].

Infine, connessa al tema della responsabilità degli autori di *NFT* per violazione dei diritti di proprietà intellettuale altrui, un'ultima considerazione merita la possibilità di chiamare a rispondere le stesse piattaforme attraverso le quali gli *NFT* vengono creati e commercializzati.

Tale considerazione risulta ancor più significativa alla luce della recente approvazione da parte del Parlamento Europeo del *Digital Services Act*[15], che, tra gli altri obiettivi, stabilisce nuovi standard in materia di responsabilità delle piattaforme *online* per quanto riguarda contenuti illegali o dannosi.

In particolare, le piattaforme tramite le quali vengono creati e commercializzati *NFT*, paiono riconducibili a piattaforme di *hosting*, rispetto alle quali il nuovo *DSA* prevede un obbligo di rimozione dei contenuti illegali (ad esempio degli *NFT* coniati in violazione del diritto d'autore), non appena la piattaforma ne venga a conoscenza mediante indagini volontarie o notifiche sufficientemente precise ricevute da persone o enti, tali da consentire ad un operatore economico diligente di individuare e contrastare efficacemente i presunti contenuti illegali (cd. *notice and take down*).

A fronte di siffatta condotta, il *DSA* prevede l'esonero di responsabilità della piattaforma di *hosting*; è possibile dunque affermare *a contrario* la responsabilità della piattaforma nel caso in cui tale condotta non venga invece realizzata.

Ai sensi del successivo par. 24 resta in ogni caso fermo che le esenzioni di responsa-

*Class 9. NFTs are treated as unique digital certificates registered in a blockchain, which authenticat**e** digital items but are distinct from those digital items. For the Office, the term non fungible tokens on its own is not acceptable. The type of digital item authenticated by the NFT must be specified. Services relating to virtual goods and NFTs will be classified in line with the established principles of classification for service».*

[14] É quanto si evince dal combinato disposto degli artt. 12 e 13, l. 633/1941 sulla protezione del diritto d'autore. Ai sensi dell'art. 12 infatti «l'autore ha il diritto esclusivo di pubblicare l'opera. Ha altresì il diritto esclusivo di utilizzare economicamente l'opera in ogni forma e modo originale, o derivato, nei limiti fissati da questa legge, ed in particolare con l'esercizio dei diritti esclusivi indicati negli articoli seguenti (…)». Nell'elencazione di tali diritti, l'art. 13 dispone che: «Il diritto esclusivo di riprodurre ha per oggetto la moltiplicazione in copie diretta o indiretta, temporanea o permanente, in tutto o in parte dell'opera, in qualunque modo o forma, come la copiatura a mano, la stampa, la litografia, l'incisione, la fotografia, la fonografia, la cinematografia ed ogni altro procedimento di riproduzione».

[15] Si veda il regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, par. 22.

bilità lasciano impregiudicate i provvedimenti inibitori emanati da autorità giurisdizionali o amministrative volte a porre fine alle violazioni contestate, anche mediante rimozione dei contenuti illegali o disabilitazione dell'accesso a tali contenuti.
Nel caso degli *NFT*, il contenuto non può essere materialmente cancellato dalla rete *blockchain*, quanto piuttosto inviato ad un indirizzo della stessa che funge da "buco nero" per i certificati digitali di cui ci si voglia liberare[16].
In conclusione, dalle riflessioni svolte sembra potersi ricavare che la novità della tecnologia impiegata rispetto agli *NFT* non mette in discussione i meccanismi di tutela approntati dal diritto industriale e della proprietà intellettuale.
Il fenomeno degli *NFT* consente di riflettere su come il progresso digitale venga letto e governato dalla lente del diritto che, sebbene con difficoltà, cerca di rimanere al passo con i tempi, adeguandosi al fine di proporre rimedi adatti a governare una realtà sempre più complessa e foriera di nuove sfide.

[16] Per una guida pratica sul punto si rimanda a *How do I delete or burn my NFTs?*, in *docs.mintable.app*.

Cronache

La digitalizzazione nell'UE: una sfida costituzionale

Giuseppe Muto

Abstract

Nell'ambito del *Digital Europe Programme*, l'Unione europea ha adottato un approccio antropocentrico, secondo cui le moderne tecnologie devono essere sia al servizio delle persone, sia in linea con i principi, i valori e i diritti fondamentali dell'Unione stessa. In questa prospettiva, la creazione degli *European Digital Innovation Hub*, sul modello degli *Hub* innovativi nella *Silicon Valley*, si pone non solo il fine di implementare il livello di digitalizzazione degli Stati membri, ma soprattutto sfruttare la tecnologia, al fine di garantire l'effettività di alcuni principi di rilevanza costituzionale.

Within the Digital Europe Programme, the European Union has adopted an anthropocentric approach, according to which modern technologies need to be both at the service of people and in line with the principles, values and fundamental rights of the Union itself. In this perspective, the creation of European Digital Innovation Hubs, modelled on the innovation hubs in Silicon Valley, aims not only to implement the level of digitization of the Member States, but mainly to harness technology in order to ensure the effectiveness of some principles of constitutional relevance.

Sommario

1. La digitalizzazione: una sfida fondamentale per l'UE. – 2. Il *Digital Europe Programme*. – 3. Il modello degli *Hub* nella *Silicon Valley* e primi esemplari in Europa. – 4. Gli *European Digital Innovation Hub*. – 5. La rilevanza costituzionale del programma *Europe Digital* e degli *European Digital Innovation Hub*.

Keywords

Unione europea – Digital Europe Programme – Digital Hub – Digitalizzazione – Politiche digitali

1. La digitalizzazione: una sfida fondamentale per l'UE

Pur non volendo assegnare a J.W. Goethe doti profetiche, il quale nel *Faust* affermava che «e così ci sarà un pensatore, che costituirà un cervello che sappia pensare esatta-

mente»[1], appare corretto ritenere che lo sviluppo delle tecnologie, tra di queste anche l'intelligenza artificiale, richieda uno sforzo teorico a tutti i cultori delle scienze sociali, in particolare ai giuristi. In Italia, già nel 1968 si era soliti distinguere "il diritto artificiale" da "il diritto naturale", ripercorrendo l'antitesi già proposta dai greci tra *physis*, ossia la natura, e la *techne*, cioè la creazione artificiale, evidenziando, in questo modo, la particolare inclinazione dei giuristi italiani verso il cd. "diritto artificiale"[2]. «Le possibilità di applicazione della tecnologia, intesa come processo di razionalizzazione operativa, costituiscono una nuova fisionomia spirituale, così che la mentalità tecnologica diventa una sua seconda, rinnovata natura.»[3]

In questo contesto, l'UE, per mezzo della Commissione, ha occupato l'avamposto di quanto concerne la regolamentazione giuridica delle piattaforme digitali, ponendo attenzione a non volere rallentare lo sviluppo tecnologico, bensì ad adeguarlo ai valori fondanti dell'Europa. In questo spirito, si è proceduto alla codificazione del *General Data Protection Regulation, GDPR* e della *Digital Single Market Strategy*, di cui fanno parte il *Data Governance Act*, il *Digital Services Act*, il *Digital Markets Act* e la *Cybersecurity Strategy*.[4]

La comunicazione emanata dalla Commissione europea il 9 marzo 2021 "*2030 Digital Compass: the European way for the Digital Decade"* evidenzia «l'incidenza del digitale nel tessuto socio-economico europeo, esaltandone la rilevanza strategica per garantire la resilienza dell'Europa»[5]. Questa circostanza è emersa in maniera dirompente durante la fase acuta dell'emergenza epidemica da Covid-19, quando tutte le attività sociali ed economiche si sono trasferite sulle piattaforme digitali, e si è affermata anche successivamente con l'affermarsi dei *Big Data*, della *Blockchain* e dell'intelligenza artificiale. Tuttavia, la Commissione ha individuato quale fattore di particolare vulnerabilità, la forte dipendenza del Vecchio Continente dalle tecnologie sviluppate e prodotte in paesi non democratici. Per questa ragione, «il programma di lavoro della Commissione ribadisce il termine del 2030 quale orizzonte temporale per il completamento della trasformazione digitale europea, basata su tecnologie affidabili, sicure ed antropocentriche»[6]. Al fine di rendere concreta questa ambizione, la Commissione europea ha individuato quattro obiettivi[7] da raggiungere entro il termine temporale prefissato:

a digitally skilled population and highly skilled digital professionals: assicurare ad almeno l'80% della popolazione adulta il possesso di competenze digitali di base;

secure and performant sustainable digital infrastructures: costruire infrastrutture digitali idonee a garantire l'accesso per tutti i cittadini ai servizi digitali;

digital transformation of businesses: prevedere che almeno i tre quarti delle imprese faccia-

---

1 J. W. Goethe, *Faust*, atto II, versi 6869 – 6870.

2 *Amplius* in T.E. Frosini, *L'orizzonte giuridico dell'intelligenza artificiale*, in *Il diritto dell'informazione e dell'informatica*, 1, 2022, 7.

3 V. Frosini, *Cibernetica diritto e società*, Milano, 1968, 14.

4 Sul tema A. Bradford, *Effetto Bruxelles. Come l'Unione Europea regola il mondo,* Milano, 2021.

5 A. Palladino, *Europa digitale 2030, la Commissione propone la "Bussola" per la sovranità digitale,* in *irpa.eu*, 27 aprile 2021.

6 Servizio Studi Senato della Repubblica – Ufficio rapporti con l'Unione europea Camera dei deputati, *Il programma dell'Unione Europea per il 2022*, Documentazione per le Commissioni, 14 giugno 2022, 17.

7 Così come riportati da A. Palladino, *Europa digitale 2030, la Commissione propone la "Bussola" per la sovranità digitale*, cit.

no uso di *cloud computing*, *big data* ed intelligenza artificiale;
digitalisation of public services: garantire l'accessibilità online a tutti i principali servizi pubblici e l'utilizzo dell'identificazione digitale.
Per le finalità sopra menzionate vengono in considerazione, in particolare[8]:
la proposta di direttiva relativa a misure per un livello comune elevato di cybersicurezza dell'Unione (cd. NIS 2 – *Security of network and information systems*), già oggetto di accordo tra il Parlamento europeo e il Consiglio dell'UE (concluso il 13 maggio 2022);
la proposta di modifica del regolamento (UE) 910/2014 in materia di identità digitale europea;
la legge sull'intelligenza artificiale, che, oltre a tutelare i diritti fondamentali, promuova «il ricorso a spazi di sperimentazione normativa volti a creare un ambiente controllato per testare tecnologie innovative per un periodo limitato, oltre all'accesso ai poli dell'innovazione digitale e a strutture di prova e sperimentazione, con l'obiettivo di sostenere le imprese innovative, le PMI e le *start-up*.»[9].

2. Il *Digital Europe Programme*

L'Unione europea ha, dunque, adottato un approccio antropocentrico[10], in relazione al quale le moderne tecnologie devono essere sia al servizio delle persone, sia in linea con i principi, i valori e i diritti fondamentali dell'Unione stessa.
Per questa ragione, l'UE, accanto agli strumenti previsti dal *Recovery Fund* e dal *Green Deal* europeo, ha adottato il *Digital Europe* (Programma Europa Digitale).
«Gli obiettivi generali del programma sono i seguenti: sostenere e accelerare la trasformazione digitale dell'economia, dell'industria e della società europee, permettere ai cittadini, alle pubbliche amministrazioni e alle imprese di tutta l'Unione di beneficiare dei suoi vantaggi, nonché migliorare la competitività dell'Europa nell'economia digitale mondiale contribuendo a ridurre il divario digitale in tutta l'Unione e rafforzando l'autonomia strategica dell'Unione tramite un sostegno globale, intersettoriale e transfrontaliero e un maggiore contributo dell'Unione».[11]
Infatti, ai sensi dell'art. 173 TFUE, l'Unione e gli Stati membri si adoperano per assicurare le condizioni necessarie per garantire la competitività dell'industria e, a tal fine, accelerare l'adattamento dell'industria alle trasformazioni strutturali, nonché favorire un migliore sfruttamento del potenziale industriale delle politiche d'innovazione, di ricerca e di sviluppo tecnologico. Il par. 3, nello specifico, prevede la possibilità di adottare misure peculiari per consentire agli Stati membri di raggiungere questi obiettivi.

[8] Così come esposte in Servizio Studi Senato della Repubblica – Ufficio rapporti con l'Unione europea Camera dei deputati, *Il programma dell'Unione Europea per il 2022*, Documentazione per le Commissioni, 14 giugno 2022, 17.

[9] *Ibidem*.

[10] Definizione presente in Commissioni Riunite IX (Trasporti, poste e telecomunicazioni) e X (Attività produttive, commercio e turismo) della XVIII Legislatura, *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione. COM(2021) 206 final e Allegati*, Allegato 1, 13 aprile 2022, 7.

[11] Art. 3, par. 1, regolamento (UE) 2021/694.

Inoltre, già nel vertice di Tallinn sul digitale del settembre 2017, si è evidenziata l'opportunità per l'Unione di «investire nella digitalizzazione delle proprie economie e far fronte al divario di competenze se vuole mantenere e arricchire la propria competitività e la propria innovazione, la qualità della vita e il tessuto sociale»[12].

Approfondendo ulteriormente, i cinque pilastri considerati prioritari nel programma *Digital Europe* sono[13]:

calcolo ad alte prestazioni[14]: l'utilizzo dei cd. supercomputer è ritenuto strategico sia per la PA sia per le imprese; a questo fine si evidenzia la necessità di implementare in modo adeguato l'infrastruttura di dati. Parte dei fondi stanziati dall'UE per questo programma confluiranno nell'impresa comune[15] EuroHPC, con il fine di finanziare progetti di ricerca ed innovazione sul calcolo ad alte prestazioni;

intelligenza artificiale: «è l'abilità di un macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività»[16]. Si tratta di una delle tecnologie più attraenti per il futuro economico e sociale di ciascuno Stato membro; lo sviluppo sarà rilevante non solo nell'ambito dei prodotti digitali, ma anche nella vita quotidiana dei cittadini europei. Per questa ragione, il programma ha intenzione di implementare l'utilizzo dell'intelligenza artificiale, sia da parte degli operatori economici, sia da parte delle amministrazioni pubbliche, al fine di assicurare al cittadino l'accesso sicuro a tali servizi e di archiviare ingenti quantità di dati ed algoritmi. L'approccio regolativo della Commissione[17], così come espresso nel Libro Bianco sull'Intelligenza artificiale, si basa su un sistema a piramide ascendente, che mira a ridurre al minimo i rischi per la sicurezza e i diritti fondamentali. In relazione al grado di rischio, sono richiesti requisiti minimi di trasparenza (come nel caso di *chatbot* o *deep fake*) o sono ricollegate misure di attenuazione o divieti (ad esempio, per l'identificazione biometrica remota);

cybersicurezza: le tecnologie digitali determinano il sorgere di nuovi rischi, tra cui l'aumento di frodi e furti di dati. L'UE reagisce a queste sfide, sia adottando misure normative *ad hoc*, sia per mezzo di investimenti, volti a sostenere l'acquisto di attrezzature, infrastrutture e strumenti avanzati;

competenze digitali: la digitalizzazione produce importanti benefici, solamente se un numero sufficientemente alto di utenti è in grado di utilizzarle. Per utenti deve intendersi non solamente studenti e professionisti, ma anche imprese e lavoratori;

capacità digitale ed interoperabilità: le soluzioni digitali interoperabili delle Pubbliche Amministrazioni si propongono di facilitare lo svolgimento di attività burocratiche in ambiti di pubblico interesse, quali la salute, e di agevolare l'accesso per le PMI alla tecnologia.

---

12 Considerando 9, regolamento (UE) 2021/694.

13 *Amplius* A. Bonifazi, *Fondi per la digitalizzazione delle PMI: lo strumento per uscire dalla crisi (parte II)*, in *Finanziamenti su misura*, 3, 2021, 7.

14 La dizione degli specifici obiettivi è riportata nell'art. 3, par. 2, regolamento (UE) 2021/694.

15 A. Bonifazi, *Fondi per la digitalizzazione delle PMI*, cit., 7, nt. 2.

16 Ufficio Rapporti con l'Unione europea Camera dei deputati, *Legge sull'intelligenza artificiale,* Dossier n. 57, 12 novembre 2021, 2

17 Così come sintetizzato *ibidem.*

Al fine di assolvere alle *missions* appena descritte, il programma *Digital Europe* prevede anche l'istituzione di un *network* di *European Digital Innovation Hub* (Poli europei di Innovazione Digitale), che offrono accesso ad incubatori di sviluppo tecnologico e supporto alla trasformazione digitale per le organizzazioni pubbliche e private europee, incluse quelle governative a livello nazionale, regionale e locale.[18] Pertanto, l'obiettivo che si pone il legislatore europeo è quello di creare degli incubatori di tecnologia, mettendo a sistema tutte le risorse del territorio, che erogano vantaggi per le stesse realtà economiche radicate in quell'area geografica.

3. Il modello degli *Hub* nella *Silicon Valley* e primi esemplari in Europa

Si cerca, dunque, di ricalcare il modello estremamente virtuoso della *Silicon Valley*, il cui segreto si basa sull'esistenza di un ambiente innovativo. Non è possibile individuare un solo fattore per cui alcuni giganti del tech, tra cui Google, Apple, Xerox, Cisco, abbiano deciso di stabilire i propri centri di sviluppo in questa area, bensì occorre analizzare le sinergie esistenti tra la storia dell'area, la presenza di ingenti capitali di rischio, l'esistenza di centri accademici (Stanford e UC Berkley) e di ricerca eccellenti (la NASA) e di un alto livello di ambizione delle migliori giovani menti, per le quali niente è impossibile. Non si è mai generato un eguagliabile ecosistema di innovazione in Europa, perché le imprese europee sono generalmente meno inclini alla cultura del cambiamento, ma anche non è sufficientemente diffusa la cultura del fallimento. Innovare vuol dire scoprire qualcosa di nuovo e la scoperta può anche produrre un fallimento. Inoltre, il posizionare i laboratori di ricerca e sviluppo al di fuori delle strutture aziendali, quali la burocrazia e gli altri processi interni, permette al personale selezionato per l'hub di poter effettivamente innovare, senza dover osservare i limiti di quello che è necessario per l'azienda. Consideriamo l'esempio di Google, che ha stabilito il suo *innovation hub* (Google X) al di fuori degli uffici dove è normalmente realizzata l'attività d'impresa quotidiana. In quel luogo, infatti, i dipendenti sviluppano tecnologie diverse dagli attuali segmenti di produzione, al fine di occupare sempre una posizione di vantaggio rispetto ai *competitor*. L'integrazione con il territorio è evidente: Google testa i propri nuovi prodotti con reali clienti ed in relazione agli esiti generati da questi *early-stage* decide se tenere, modificare o abbandonare completamente quel prodotto.[19]

Nel 2016 l'Unione europea, al fine di riprodurre questo modello virtuoso anche nel Vecchio Continente, ha avviato il programma "Digitalizzazione dell'industria europea" (*Digitising European Industry*, DEI), che si poneva l'obiettivo di rafforzare la competitività dell'UE nelle tecnologie digitali, cosicché da garantire ad ogni impresa la

[18] European Commission, *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme – European Digital Innovation Hubs for 2021 – 2023*, in *ec.europa.eu*, 3.

[19] Per un approfondimento sugli *innovation hub* presenti nella *Silicon Valley* si rinvia a A. Berger – A. Brem, *Innovation Hub How-To: Lessons From Silicon Valley*, in *Global Business and Organizational Excellence*, 35, 2016, 58 ss.

possibilità di sfruttare le innovazioni. Le risorse economiche stanziate erano pari a 50 miliardi, provenienti da investimenti sia pubblici che privati per il quinquennio successivo. Nell'ambito di questo programma si prevedeva anche la costituzione di poli dell'innovazione digitale (*Digital Innovation Hub,* DIH), che avevano il fine di coadiuvare le imprese nella rivoluzione tecnologica, offrendo a queste supporto tecnico, e di creare un ecosistema virtuoso. Le caratteristiche[20] di questi DIH erano: partecipare ad una iniziativa regionale, nazionale o europea di digitalizzazione dell'industria; essere un'organizzazione senza finalità di lucro; essere fisicamente presente nella regione e disporre di un sito internet aggiornato che illustrasse chiaramente le attività del DIH e i servizi forniti, fornire almeno tre esempi di modalità con cui il polo ha aiutato una impresa ad attuare la trasformazione digitale. Nel 2017 la Commissione ha creato un catalogo online con il fine di favorire la creazione di una rete, nel quale erano registrati 498 DIH, di cui 309 operativi e 189 in preparazione[21].

La Corte dei Conti europea ha verificato se la Commissione avesse adeguatamente coadiuvato gli Stati membri nella definizione della strategia di digitalizzazione dell'industria. Tuttavia, è stata individuata una falla nel processo di rendicontazione alla Commissione della attività svolte dagli Stati, a causa della mancata definizione degli effetti attesi, indicatori di risultato e valori-obiettivo. Infatti, l'istituzione del programma, a metà del periodo di programmazione 2014-2020, aveva impedito l'emanazione di disposizioni giuridiche che obbligassero gli Stati membri ad adoperarsi in maniera proattiva per il monitoraggio dei progetti. La Corte, pertanto, ha affermato che: «le attività negli Stati membri visitati sono state modeste. Quattro anni dopo l'avvio dell'iniziativa DEI, i DIH avevano ancora un limitato accesso ai fondi: in base a quanto rilevato dalla Corte, in alcuni casi questi non erano stati costituiti in modo coordinato e, fatta eccezione per le attività finanziate da Orizzonte 2020, non esiste ancora un quadro dettagliato per il monitoraggio dei DIH a livello UE.»[22]

4. Gli *European Digital Innovation Hub*

Nonostante lo sviluppo delle tecnologie, le imprese incontrano ancora difficoltà nel comprendere su quali tecnologie investire e come adeguarsi alla trasformazione digitale.

L'Unione europea, in considerazione della necessità di stimolare la diffusa adozione delle tecnologie avanzate per lo sviluppo sia delle imprese, in particolare delle PMI, sia per la digitalizzazione della PA e constatando il parziale fallimento degli DIH, prevede la costituzione di nuovi Poli europei di Innovazione Digitale, inserendo questo obiettivo nel Programma *Digital Europe*.

Infatti, l'art. 2, n. 5), del regolamento (UE) 2021/694 definisce un Polo europeo di

[20] Così come riportate in Corte dei Conti europea, *Digitalizzazione dell'industria europea: iniziativa ambiziosa il cui successo dipende dal costante impegno dell'UE, delle amministrazioni e delle imprese*, in *eca.europa.eu*, 33.

[21] Dati aggiornati al 31 dicembre 2019.

[22] Corte dei Conti europea, *Digitalizzazione dell'industria europea: iniziativa ambiziosa il cui successo dipende dal costante impegno dell'UE, delle amministrazioni e delle imprese*, in *eca.europa.eu*, 5.

Innovazione Digitale come «un soggetto giuridico selezionato a norma dell'articolo 16 per svolgere i compiti previsti dal Programma, in particolare fornire direttamente o assicurare l'accesso a competenze tecnologiche e strutture di sperimentazione, come attrezzature e strumenti software, allo scopo di rendere possibile la trasformazione digitale dell'industria, nonché agevolare l'accesso ai finanziamenti; è aperto alle imprese di ogni forma e dimensione, in particolare alle PMI, alle società a media capitalizzazione e alle scale-up, nonché alle pubbliche amministrazioni di tutta l'Unione».

Dunque, la base normativa comunitaria deve ritrovarsi nell'art. 16 del regolamento (UE) 2021/694 e nella decisione della Commissione europea C/2021/7911 del 10 novembre 2021, concernente l'adozione del programma di lavoro pluriennale dei Poli europei di Innovazione Digitale per il periodo 2021-2023.

Questi nuovi soggetti giuridici dovrebbero stimolare l'adozione delle tecnologie digitali più avanzate da parte dell'industria, in particolare le PMI e le altre realtà che occupano al massimo 3000 persone, le organizzazioni pubbliche e il mondo accademico. «I poli europei dell'innovazione digitale dovrebbero fungere da sportelli unici per accedere a tecnologie provate e convalidate e promuovere l'innovazione aperta. Essi dovrebbero inoltre fornire sostegno nel settore delle competenze digitali avanzate, ad esempio coordinandosi con i responsabili dell'istruzione per offrire attività di formazione a breve termine per i lavoratori e tirocini per gli studenti. La rete dei poli europei dell'innovazione digitale dovrebbe assicurare un'ampia copertura geografica in tutta Europa e dovrebbe favorire la partecipazione delle regioni ultraperiferiche al mercato unico digitale.»[23]

Più nello specifico, ai sensi dell'art. 16, par. 2, regolamento (UE) 2021/694, gli Stati membri, per mezzo di una procedura aperta e competitiva, in conformità con le proprie procedure interne, individuano i soggetti candidati alla seconda fase di selezione, che avverrà in sede europea, conformandosi ai seguenti criteri:

- competenze adeguate all'esperimento delle funzioni ad esse assegnate (§ *infra*);
- capacità di gestione, personale ed infrastrutture adeguate allo svolgimento delle attività;
- mezzi operativi e giuridici idonei all'applicazione delle norme amministrative, contrattuali e finanziarie dell'Unione; e
- adeguata sostenibilità finanziaria.

Inoltre, ai sensi dell'art. 16, par. 6, regolamento (UE) 2021/694, i Poli europei di Innovazione Digitale devono svolgere le seguenti attività a vantaggio dell'industria (PMI ed imprese a media capitalizzazione), nonché del settore pubblico:

- sensibilizzare e fornire competenze, *know-how* e servizi di trasformazione digitale;
- assistere le imprese, in particolare le PMI e le start-up, le organizzazioni e le amministrazioni pubbliche, affinché diventino più competitive e migliorino i loro modelli di business attraverso l'uso delle nuove tecnologie contemplate dal Programma;
- agevolare il trasferimento di competenze e *know-how* tra le regioni […], incoraggiare gli scambi di esperienze e competenze, le iniziative congiunte e le buone prassi;
- fornire servizi tematici, in particolare quelli correlati all'IA, all'HPC e alla cybersicurezza e alla fiducia, o garantirvi l'accesso, alle pubbliche amministrazioni, alle

[23] Così come affermato nel considerando 17, regolamento (UE) 2021/694.

organizzazioni del settore pubblico, alle PMI o alle imprese a media capitalizzazione; e

- erogare sostegno finanziario a terzi nell'ambito dell'obiettivo specifico 4 (*i.e.* implementare le competenze digitali nei diversi utenti).

Nel contesto italiano, lo sviluppo di questi *hub* è stato integrato nel Piano Nazione di Ripresa e Resilienza[24], il quale[25] pone l'obiettivo, entro il 2025, di costituire 42 nuovi Poli (che si aggiungono agli 8 già esistenti), distinti in centri di competenza e la rete dei poli di innovazione sul campo. I primi sono partenariati pubblico-privati e sono individuati in relazione alla loro capacità di proporre strumenti innovativi ed efficaci nella trasformazione digitale delle imprese. I partner devono essere individuati in istituzioni come università, centri di ricerca ed imprese private tecnologiche di punta. Differentemente, la rete dei poli di innovazione sul campo propone servizi come: sensibilizzazione, formazione, intermediazione tecnologica, accesso ai finanziamenti per l'innovazione tecnologica, audit tecnico e banchi di prova[26]. Infine, si dispone che entro il medesimo periodo temporale, i centri devono fornire servizi per una quantità di risorse pari ad almeno 600 milioni di euro e siano beneficiari di tali prestazioni almeno 4500 piccole e medie imprese. In particolare, così come previsto dal Working Programme[27] della Commissione, ciascun polo deve erogare i servizi di test e sperimentazione (*test before invest*), formazione e sviluppo di competenze digitali avanzate, sostegno all'accesso a meccanismi di finanziamento e ecosistemi dell'innovazione e networking. La rilevanza di questi poli per il tessuto sociale ed economico del Paese è chiaramente espressa dal Ministro dello Sviluppo Economico, On. Giancarlo Giorgetti, in occasione dell'emanazione del Decreto Ministeriale del 11 aprile 2022: «Puntiamo sugli investimenti in manifattura 4.0 per accompagnare la transizione digitale delle filiere produttive, soprattutto in settori strategici per l'economia del paese. Con questo obiettivo abbiamo deciso di investire su una rete nazionale di Poli di trasferimento tecnologico in cui il fattore umano gioca un ruolo decisivo per il futuro del settore manifatturiero, rafforzando la capacità di incontro tra il mondo della ricerca e le imprese nell'applicazione di tecnologie all'avanguardia»[28]

[24] Così come approvato con Decisione del Consiglio ECOFIN del 13 luglio 2021, notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21 del 14 luglio 2021.

[25] Nello specifico ci riferiamo alla Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'Impresa" – Investimento 2.3 "Rafforzamento ed estensione settoriale/territoriale dei centri per il trasferimento tecnologico per i segmenti di industria".

[26] Come esposto nel Decreto Ministeriale del Ministro dello Sviluppo Economico del 11 aprile 2022.

[27] European Commission, *Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme – European Digital Innovation Hubs for 2021 -2023*, cit.

[28] Ministero dello Sviluppo Economico, *Al via network nazionale di Poli di trasferimento tecnologico*, in *mise.gov.it*, 21 aprile 2022.

5. La rilevanza costituzionale del programma *Europe Digital* e degli *European Digital Innovation Hub*

Con riguardo al digitale, la letteratura costituzionale ha affrontato principalmente i rischi connessi alla tutela di alcuni valori di rilevanza costituzionale (si pensi alla tutela della proprietà intellettuali o dei dati personali) e, conseguentemente, si è sempre soffermata sullo studio delle regole che potessero garantire un adeguato bilanciamento tra i diritti e le libertà coinvolte. Per questa ragione, ci si interroga se le regole del costituzionalismo digitale europeo possano essere capaci di proporre un approccio digitale sostenibile, che si discosti dal contrasto dicotomico tra imperialismo costituzionale e protezionismo costituzionale, emancipando il dibattito costituzionale dalla prospettiva dominante, limitata alla privacy e alla proprietà intellettuale.[29]

Infatti, come sostiene De Gregorio riguardo all'intelligenza artificiale, «Di fronte al bivio normativo della quarta rivoluzione industriale, l'Unione sembra aver scelto un percorso verso lo sviluppo di un ambiente sostenibile per l'intelligenza artificiale, piuttosto che concentrarsi semplicemente sulla promozione dell'innovazione per sfruttare le potenzialità di queste tecnologie o limitarsi ad ostacolarne lo sviluppo per proteggere i diritti fondamentali e i valori democratici».[30] Infatti, lo sviluppo tecnologico ha offerto l'enorme possibilità di potenziare l'esercizio e l'effettività dei diritti fondamentali e dei valori democratici. Tuttavia, la tradizionale nozione di legge, come espressione di un pubblico potere, è oggi messa in crisi dall'emergere di norme autoprodotte da altri sottosistemi, quali le imprese, che detengono il monopolio del digitale. Non è possibile, pertanto, consentire che una delle modalità di esercizio dei principi costituzionali sia schiava di attori privati.

«Gli approcci neoliberali che rifiutano il ruolo degli attori pubblici nella protezione dei diritti fondamentali e dei valori democratici possono scontrarsi con le caratteristiche del costituzionalismo europeo. I diritti fondamentali e i valori democratici non possono essere lasciati nelle mani di poteri *unaccountable* che, anche se privati, prendono decisioni che influenzano la vita quotidiana al di fuori dei circuiti democratici. […] Un'espressione più matura del costituzionalismo digitale mirerebbe a contrastare le soluzioni tecno-deterministe e contribuirebbe a promuovere i valori europei come modello costituzionale sostenibile per lo sviluppo delle tecnologie automatizzate nel contesto globale».[31]

In questo senso, deve essere interpretato il fine che l'Unione si è posta con l'adozione del *Digital Europe* ed, in particolare, la costituzione degli *European Digital Innovation Hub*: assicurare l'esercizio dei valori costituzionali, sfruttando la tecnologia.

Infatti, è proprio il preambolo alla Carta di Nizza che, tra i suoi scopi, si pone la tutela dei diritti fondamentali alla luce degli sviluppi scientifici e tecnologici.[32] È possibile

[29] O. Pollicino, *Foreword,* in G. De Gregorio, *Digital Constitutionalism in Europe,* Cambridge, 2022, XIV.

[30] G. De Gregorio, *Digital Constitutionalism in Europe,* Cambridge, 2022, 316.

[31] Ivi, 317.

[32] Preambolo Carta di Nizza 2000/C 364/ 08: «A tal fine è necessario, rendendoli più visibili in una Carta, rafforzare la tutela dei diritti fondamentali alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici».

ritenere che la costituzione di questi poli nel nostro Paese abbia il fine ultimo di contribuire alla rimozione di quegli ostacoli di ordine economico e sociale, che impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione alla vita economica e sociale del Paese, di cui all'art. 3 Cost., nonché promuovere lo sviluppo della cultura e della ricerca scientifica e tecnica, così come stabilito dall'art. 9 Cost. Inoltre, è possibile ritenere che la particolare struttura prevista per questi enti dal regolamento (UE) 2021/694, così aperta a tutte le eccellenze del territorio in cui è inserita, ben si allinea con il dettato di cui all'art. 45 Cost., nel quale si afferma che la Repubblica riconosce la funzione sociale della cooperazione a carattere di mutualità e senza fini di speculazione privata.

Più nello specifico, così come riportato nella conclusione del Consiglio europeo del 19 ottobre 2017, la creazione di un'Europa digitale non può che accompagnarsi ad una alfabetizzazione mediatica[33] e digitale, che preveda la diffusione di competenze essenziali idonee a permettere un'efficace relazione dei cittadini con i media, nonché sviluppare un pensiero critico e capacità di apprendimento a lungo termine. All'uopo, questo Programma deve coordinarsi con gli altri che perseguono simili finalità (*i.e.* FSE+, FESR, Erasmus+, Horizon). Con riferimento al contesto nazionale, la relazione programmatica del Governo, di cui all'art. 13 c. 1 l. 234/2012 e trasmessa al Parlamento il 16 maggio 2022, pone quale priorità l'accrescimento delle competenze digitali e la riduzione del *digital divide*, prevedendo, nell'iniziativa Repubblica digitale, una forte accelerazione alla dotazione digitale delle scuole. È possibile, pertanto, ritenere che il Programma *Digital Europe* si ponga il fine di garantire l'effettività del diritto all'istruzione, così come formulato dall'art. 14 della Carta di Nizza e dagli artt. 33 e 34 Cost.

Inoltre, lo sviluppo dell'attività d'impresa, art. 16 della Carta di Nizza e artt. 4 e 41 Cost., inevitabilmente trae un vantaggio dalla costituzione dei Poli, così come illustrato *supra* § 4.

Per la crescita a lungo termine dell'Europa e la creazione di valore aggiunto nella società della conoscenza, le competenze digitali avanzate devono accompagnarsi alla piena inclusione. Infatti, nella risoluzione sulla digitalizzazione dell'industria europea, il Parlamento europeo ha chiesto che «l'equilibrio di genere sia integrato in tutte le iniziative digitali sottolineando la necessità di affrontare il divario di genere nel settore delle tecnologie dell'informazione»[34]. Ancora, «la digitalizzazione può agevolare e migliorare l'accessibilità senza barriere per tutti, compresi gli anziani, le persone a mobilità ridotta o con disabilità, e le persone che vivono in zone remote o rurali»[35]. Proprio riguardo agli abitanti di terre remote è sintomatico come il legislatore abbia esplicitamente stabilito l'applicabilità del Programma anche nelle cd. regioni ultraperifiche ai sensi degli artt. 349 e 355 TFUE. È la stessa Carta di Nizza che dispone «L'Unione […] cerca di promuovere uno sviluppo equilibrato e sostenibile» e ribadisce questo principio anche all'art. 26. Questa peculiarità ben si concilia anche con il dettato dell'art. 38, c. 3, Cost.

In aggiunta, come dichiarato nella dichiarazione di Tallinn sull'e-government da parte dei ministri delegati per la specifica materia, il progresso digitale sta profondamente

[33] Così come espressamente dichiarato nei considerando 40 e 41, regolamento (UE) 2021/694.

[34] Considerando 42 e 43, regolamento (UE) 2021/694.

[35] Considerando 46, regolamento (UE) 2021/694.

trasformando le loro società, ponendo davanti alla pubblica amministrazione nuove sfide per rispondere in modo adeguato alle attese dei cittadini. Infatti, dal momento che la qualità della PA ha un impatto diretto sull'ambiente economico ed è assolutamente necessario favorire la produttività, la crescita sostenibile e l'occupazione, la digitalizzazione della PA rappresenta una priorità fondamentale per la costituzione di un efficace mercato unico digitale. Diversamente, si creerebbero barriere elettroniche transfrontaliere, generando una frammentazione dei servizi pubblici europei a detrimento delle libertà fondamentali e del riconoscimento reciproco dei servizi nell'Unione.[36] Pertanto, la digitalizzazione della PA appare essere, oltre che un'esigenza di ragione economica, l'attuazione di principi di rilevanza costituzionale, come l'art. 41 della Carta di Nizza ed il buon andamento dell'amministrazione della PA.

Infine, il grado di sviluppo delle nuove tecnologie giunge perfino a coinvolgere i valori costituzionali descritti nella Parte II "Ordinamento della Repubblica" della nostra Costituzione. Si registra che il dibattito pubblico si è massicciamente spostato sulle piattaforme *social*, rendendo necessario non solo una loro regolamentazione da parte di autorità pubbliche (tema al centro di copiose discussioni), ma anche implementazione della consapevolezza degli utenti. Gli algoritmi tendono a mostrare sempre contenuti simili a quelli con i quali si è interagito precedentemente, mortificando l'ambiente aperto ad un dibattito pluralistico e giungendo ad un'estrema polarizzazione del dibattito politico, che potrebbe produrre, in casi estremi, una reale manipolazione delle elezioni.[37]

In conclusione, la digitalizzazione dell'Unione, fine perseguito dal Programma *Europe Digital* e, in particolare, dalla creazione degli *European Digital Innovation Hub*, non produrrà esclusivamente benefici di tipo economico, bensì contribuirà a garantire l'effettività di diritti e libertà costituzionali per il cittadino, se ben integrato nel nuovo mondo digitale.

[36] Considerando 50, 51, 52, 53, regolamento (UE) 2021/694.

[37] Ufficio Rapporti con l'Unione europea Camera dei deputati, *Legge sull'intelligenza artificiale*, cit., 4.

Diritto all'oblio. Prime riflessioni sull'introduzione dell'art. 64-*ter* disp. att. c.p.p.

Margherita Pisapia - Carlotta Cherchi

Abstract

Il d.lgs. 150 del 2022 (c.d. Riforma Cartabia) ha introdotto tra le disposizioni di attuazione del codice di procedura penale l'art. 64-*ter*, rubricato «Diritto all'oblio degli imputati e delle persone sottoposte ad indagini». L'art., dopo una breve panoramica sul rapporto tra processo penale e media e sull'evoluzione giurisprudenziale del diritto all'oblio, si sofferma sugli strumenti introdotti dalla norma, sui possibili risvolti pratici e sulle criticità sinora ravvisabili.

The Legislative Decree 150 of 2022 (so called Cartabia Reform) has introduced article 64-ter, entitled «Right to be forgotten of defendants and persons under investigation». The paper, after a brief overview on the relationship between criminal proceedings and the media and on the jurisprudential evolution of the «right to be forgotten», focuses on the tools introduced by the law, on the possible practical implications and on the critical issues that have been identified so far.

Sommario

1. Introduzione. – 2. Processo penale e media. – 3 Dal diritto all'oblio tradizionale al diritto all'oblio digitale. – 4 Il neo introdotto art. 64-*ter* disp. att. c.p.p. – 5 Conclusioni.

Keywords

diritto all'oblio - Cartabia - deindicizzazione - media - motori di ricerca.

1. Introduzione

Tra le novità introdotte dalla Riforma Cartabia, merita attenzione il nuovo art. 64-*ter* delle disposizioni di attuazione del codice di procedura penale, rubricato «diritto all'oblio degli imputati e delle persone sottoposte ad indagini».
Con l'inserimento dell'art. 64-*ter* disp. att. c.p.p. è stata data attuazione all'art. 1, c. 25, della legge delega n. 134 del 2021, che dava mandato al Governo di «prevedere che il decreto di archiviazione e la sentenza di non luogo a procedere o di assoluzione costituiscano titolo per l'emissione di un provvedimento di deindicizzazione che, nel

rispetto della normativa dell'Unione europea in materia di dati personali, garantisca in modo effettivo il diritto all'oblio degli indagati o imputati».
La norma neo introdotta prevede ora che la persona nei cui confronti siano stati pronunciati una sentenza di proscioglimento o di non luogo a procedere, ovvero un provvedimento di archiviazione, può richiedere che sia preclusa l'indicizzazione o che sia disposta la deindicizzazione sul web dei dati personali riportati nella sentenza o nel provvedimento.
Nel caso di richiesta volta ad ottenere una preclusione dell'indicizzazione, la cancelleria del giudice che ha emesso il provvedimento appone sullo stesso e sottoscrive un'annotazione del seguente tenore: «ai sensi e nei limiti dell'art. 17 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, è preclusa l'indicizzazione del presente provvedimento rispetto a ricerche condotte sulla rete internet a partire dal nominativo dell'istante» (art. 64-*ter* disp. att. c.p.p., c. 2).
Qualora venga invece richiesta la deindicizzazione la cancelleria appone e sottoscrive l'annotazione, anch'essa espressamente richiamata dalla norma, secondo cui «il presente provvedimento costituisce titolo per ottenere, ai sensi e nei limiti dell'art. 17 del regolamento(UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, un provvedimento di sottrazione dell'indicizzazione, da parte dei motori di ricerca generalisti, di contenuti relativi al procedimento penale, rispetto a ricerche condotte a partire dal nominativo dell'istante» (art. 64-*ter* disp. att. c.p.p., c. 3).

2. Processo penale e media

Il rapporto tra processo penale, informazione e privacy «è tra i più complessi del nostro sistema giuridico»[1]: la narrazione della vicenda giudiziaria, espressione dell'irrinunciabile funzione di controllo esercitata sull'amministrazione della giustizia, espone inevitabilmente coloro che ne sono (loro malgrado) coinvolti, a un grave pregiudizio reputazionale.
Se il processo penale ha per sua natura un effetto desocializzante, la sua mediatizzazione rischia, infatti, di creare uno stigma indelebile in chi la subisce, con ricadute negative sulla sfera personale, professionale e sociale del soggetto[2].-
E ciò sia per le modalità con cui viene raccontata la vicenda giudiziaria, sia per le caratteristiche degli odierni mezzi di informazione.
Sotto il primo profilo è un dato ormai incontestato che oggi l'attenzione dei media – vuoi per il disallineamento tra i tempi dell'informazione e quelli del processo, vuoi per

[1] Così il Presidente del Garante della Privacy, dott. Pasquale Stanzione, nel discorso del Garante in occasione della relazione annuale 2021, consultabile all'indirizzo *garanteprivacy.it*.

[2] Sul tema dei rapporti tra informazione e processo penale, *ex multis*, G. Giostra, *Riflessi della rappresentazione mediatica sulla giustizia «reale» e sulla giustizia «percepita»*, in *lalegislazionepenale.eu*, 17 settembre 2018; G. Caneschi, *Processo penale mediatico e presunzione di innocenza: verso un'estensione della garanzia?* in *Archivio Penale*, 3, 2021; F. Palazzo, *Note sintetiche sul rapporto tra giustizia penale e informazione giudiziaria*, in *Diritto Penale Contemporaneo*, 3, 2017, 139 ss.; A. Riviezzo, *L'ingiusto processo mediatico*, in questa *Rivista*, 3, 2018, 62 ss.; V. Manes, *La vittima del processo mediatico: misure di carattere rimediale*, in *Diritto Penale Contemporaneo*, 3, 2017, 114 ss.

il *fil rouge* tra inquirenti e giornalisti – si concentri sulla fase delle indagini preliminari, seguite con spasmodico interesse e con toni sensazionalistici, per poi scemare con il passare del tempo.

Con due evidenti conseguenze. Da una parte, avendo come fonte informativa gli atti di indagine, la cronaca giudiziaria tende ad appiattirsi sull'ipotesi accusatoria della Procura, che viene acriticamente presentata al lettore come dato di fatto, così inevitabilmente alimentando un giudizio anticipato di colpevolezza da parte dell'opinione pubblica[3].

Dall'altra, proprio per la discrasia tra l'esigenza di celerità della notizia e i tempi del processo, l'eventuale sentenza di assoluzione, intervenuta magari dopo anni, non solo non suscita alcun interesse informativo (meritando al più un trafiletto di poche righe), ma spesso, non riesce comunque a superare il pregiudizio precedentemente formatosi. Come ha ben stigmatizzato autorevole dottrina, nel comune sentire, il solo fatto di essere indagato è raccontato e percepito come «inequivoco indizio di colpevolezza», che non viene superato neppure da un successivo proscioglimento[4].

Se a ciò si aggiunge la potenza diffusiva del web e la sua capacità di archiviazione di dati, che amplificano e cristallizzano il pregiudizio dell'opinione pubblica nei confronti di chiunque sia sottoposto a processo penale, si comprende la complessità e la gravità del fenomeno[5].

Invero, qualsiasi notizia diffamante pubblicata *online* diventa potenzialmente sempre attuale, essendo in qualsiasi momento immediatamente reperibile da parte di chiunque, rendendo così di fatto impossibile per l'utente di internet "dimenticare" e per chi è finito sotto i riflettori dei media a causa di una vicenda giudiziaria, liberarsi da quello stigma.

In questo contesto non si può che accogliere con favore un intervento normativo che ha la dichiarata finalità «di garantire in modo effettivo il diritto all'oblio degli indagati o imputati» il cui procedimento si sia concluso con esito a loro favorevole[6].

La norma sembra inscriversi nel più ampio percorso intrapreso dal nostro legislatore – su spinta comunitaria – di rafforzamento della tutela dei diritti dell'indagato/imputato in un'ottica extra-processuale.

Se in passato l'attenzione del legislatore si concentrava sulle distorsioni che si verificano all'interno del processo e su eventuali correttivi processuali, si assiste recentemente a una maggiore sensibilità per gli effetti pregiudizievoli sui diritti dell'indagato che, seppur connessi al processo, si manifestano al di fuori dello stesso e spesso perman-

[3] Si vedano i risultati dell'indagine svolta dall'Osservatorio sull'Informazione giudiziaria dell'Unione delle Camere Penali Italiane, raccolti nel volume *L'informazione giudiziaria in Italia. Libro bianco sui rapporti tra mezzi di comunicazione e processo penale,* Pisa, 2016.

[4] G. Giostra, *Un catechismo per atei. Una prima lettura del d.lgs n. 188 del 2021,* in questa *Rivista*, 1, 2022, 11 ss.

[5] E. Currao, *Diritto all'oblio, stigma penale e cronaca giudiziaria: una memoria indimenticabile*, in *Diritto Penale Contemporaneo*, 6, 2019, 157 ss.

[6] Così l'art. 1, c. 25, della legge delega n. 134 del 2021. All'indomani dell'introduzione dell'art. 64-*ter* disp. att. c.p.p., l'onorevole Enrico Costa – fautore dell'emendamento – dichiarava: «dal 1° gennaio 2023 sarà vigente la mia proposta sull'oblio per gli assolti […]. Basta innocenti marchiati a vita da indagini finite nel nulla».

gono indipendentemente dal suo esito.
Ciò che si vuole tutelare è la percezione sociale della persona sottoposta ad indagini o imputata che «non deve trovarsi diminuita – socialmente, moralmente e fisicamente – nei confronti degli altri cittadini»[7].
In questo senso il primo significativo intervento è stato senza dubbio l'attuazione della direttiva (UE) 343/2016 sulla presunzione di innocenza che ha finalmente riconosciuto una portata extra-processuale al principio di cui all'art. 27 della Costituzione: non è solo nel processo, ma è nella rappresentazione pubblica, che la persona indagata o imputata ha diritto ad essere considerato innocente fino alla sentenza definitiva di condanna[8].
Nella stessa direzione sembra oggi inscriversi anche il riconoscimento del «diritto all'oblio degli imputati e delle persone sottoposte ad indagini» di cui si proporrà un'analisi nei paragrafi che seguono.

3. Dal diritto all'oblio tradizionale al diritto all'oblio digitale

Senza alcuna pretesa di esaustività, ci pare utile una breve panoramica del diritto all'oblio, al fine di tratteggiarne i contorni e fissare alcuni punti che ci aiuteranno nell'analisi della nuova norma.
Comunemente definito come il «diritto ad essere dimenticato», il diritto all'oblio può essere più correttamente inteso come il diritto dell'individuo a una rappresentazione corretta e aggiornata della propria identità.
Si ritiene che il primo riconoscimento del diritto all'oblio sia avvenuto nel caso *Melvin v. Reid*[9], deciso dalla Corte d'appello della California nel 1931: un'ex prostituta, accusata di omicidio e poi assolta, agì in giudizio contro un produttore cinematografico che, diversi anni dopo, quando la donna si era rifatta una vita, costruendosi una nuova identità, aveva girato un film sulla sua storia, utilizzando il suo vero nome e rivelando così la sua precedente occupazione e le accuse al tempo mosse nei suoi confronti.
La Corte diede ragione alla donna, riconoscendole il diritto, «una volta riabilitata» e inserita nella società come donna «rispettabile e virtuosa»[10], a non vedere distrutta la sua nuova reputazione a causa della rievocazione «*unnecessary and indelicate*»[11] di un evento

[7] V. Manes, *Giustizia mediatica. Gli effetti perversi sui diritti fondamentali e sul giusto processo,* Bologna, 2022, 131.

[8] Per un'analisi approfondita del d.lgs. n. 188 del2021, si veda C. Melzi d'Eril (a cura di), *L'attuazione della direttiva europea sulla presunzione di innocenza*, in questa *Rivista*, 1, 2022.

[9] *Melvin v. Reid*, 112 Cal. App. 285, 297 (1931).

[10] Così testualmente la sentenza, *ivi,* 292, che sottolinea il fatto che la donna, dopo l'assoluzione, «… *abandoned her life of shame and became entirely rehabilitated. She then married Bernard Melvin and commenced the duties of caring for their home, and thereafter at all times lived an exemplary, virtuous, honorable and righteous life. She assumed a place in respectable society».*

[11] *Ibid.* In realtà, la Corte di Appello americana parla di diritto alla privacy e diritto alla felicità. Secondo i Giudici, la rievocazione dopo anni di un evento della vita passata della ricorrente «*was a direct invasion of her inalienable right to pursue and obtain happiness*».

passato ormai dimenticato.
Al di là dei toni moralizzanti dell'epoca utilizzati in motivazione, la Corte americana, per la prima volta, affermava il diritto del singolo ad «essere lasciato in pace», a non essere pregiudicato dalla rievocazione, a distanza di tanto tempo, di «incidenti» del passato.
Anche in Italia, i primi casi relativi al diritto all'oblio affrontati dalla Corte di Cassazione (circa mezzo secolo più tardi) riguardavano la ripubblicazione, a distanza di tempo, di vicende passate e affrontavano l'argomento sotto il profilo del rapporto esistente tra il diritto di cronaca, privacy e il «giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata»[12].
Dal punto di vista normativo, la disciplina di riferimento nei casi citati, era la legge n. 675 del 1996 (cd. Legge sulla Privacy), poi sostituita dal d.lgs. n. 196 del 2003 (Codice della Privacy). In particolare, l'art. 25 della Legge sulla Privacy – recepito poi dall'art. 137 del d.lgs. n. 196 del 2003[13] – stabiliva il principio della libertà del trattamento dei dati personali nell'ambito dell'attività giornalistica (per il quale non è necessario il consenso dell'interessato), a condizione che la diffusione della notizia risponda ad un criterio di essenzialità dell'informazione riguardo a fatti di interesse pubblico e avvenga nel rispetto delle regole deontologiche volte a contemperare i diritti fondamentali della persona con il diritto all'informazione[14]. Tra i criteri indicati dal Codice deontologico del 1998, si richiamavano, per quel che qui rileva, quello dell'interesse pubblico e dell'essenzialità dell'informazione previsti dagli artt. 5 e 6, in relazione all'art. 8 sulla tutela della dignità delle persone.
Alla luce del quadro normativo sinteticamente tracciato, la giurisprudenza nazionale procedeva a valutare la legittimità della diffusione di una notizia già oggetto di precedente divulgazione mediante un'interpretazione rigorosa dei requisiti legittimanti l'esercizio del diritto di cronaca - l'interesse pubblico alla conoscenza della notizia, la verità dei fatti narrati e la continenza espositiva - a cui aggiungeva il criterio dell'attualità.
Secondo la Suprema Corte, in caso di rievocazione di una notizia in qualche modo lesiva della reputazione del soggetto che ne è stato protagonista, non è sufficiente che la stessa fosse stata in precedenza legittimamente diffusa, ma occorre una nuova valutazione, al fine di verificare l'attualità di tali criteri.
Il trascorrere del tempo può infatti incidere sulla permanenza dei presupposti della

[12] Cass. civ., sez. III, 9 aprile 1998, n. 3679, *Il Foro Italiano,* 1998, 1833 ss.; sullo stesso tema anche Cass. civ., sez. I, 25 giugno 2004, n. 11864; Cass. civ., sez. III, 5 aprile 2012 n. 5525; Cass. civ., sez. III, 26 giugno 2013, n. 16111; Cass. civ, sez. I, 24 giugno 2016 n. 13161, in *Il Foro Italiano*, 9, 2016, 2730 ss., con nota di R. Pardolesi, *Diritto all'oblio, cronaca in libertà vigilata e memoria storica a rischio di soppressione.*

[13] Norma tuttora vigente seppur modificata dapprima dal d.lgs. n. 101 del 2018 e, più recentemente, dalla l. 205/2021.

[14] Il Codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica è stato emanato per la prima volta in data 29 luglio 1998 con provvedimento del Garante per la protezione dei dati personali e poi ribadito con il provvedimento del 29 novembre 2018 della medesima Autorità, sulla scia delle numerose modifiche introdotte dal decreto legislativo 10 agosto 2018, n. 101. Con riferimento alla normativa di settore, deve essere poi citato il Testo unico dei doveri del giornalista che il Consiglio nazionale dell'ordine ha approvato in data 27 gennaio 2016 e che ha recepito i precedenti documenti deontologici.

scriminante del diritto di cronaca: una notizia ritenuta in passato di interesse pubblico, perde con il passare del tempo la sua rilevanza e finanche la sua verità, allorché ad esempio la stessa non sia aggiornata e nel frattempo siano intervenuti nuovi fatti.
Alla luce di tali considerazioni, la Suprema Corte enucleava le condizioni in presenza delle quali il diritto di cronaca prevale su quello all'oblio: tra queste «il contributo arrecato dalla diffusione della notizia ad un dibattito di interesse pubblico, l'interesse effettivo e attuale alla diffusione, la grande notorietà del soggetto rappresentato»[15].
In assenza di tali condizioni, prevale il diritto dei singoli «alla riservatezza rispetto ad avvenimenti del passato che li feriscano nella dignità e nell'onore dei quali si sia ormai spenta la memoria collettiva»[16].
Riservatezza che, come stabilito in una recente pronuncia sulla base delle regole deontologiche sopra richiamate, deve essere in ogni caso preservata, anche qualora il fatto rivesta un effettivo interesse pubblico, garantendo laddove possibile, l'anonimato di colui che ne è stato protagonista[17].
Come visto, il diritto all'oblio sancito dalla Corte americana negli anni Trenta e poi ripreso dalla giurisprudenza nazionale, ha a che fare con gli effetti pregiudizievoli della riproposizione sui media di una notizia riguardante una vicenda passata e risulta intimamente connesso ai diritti della personalità, quali il diritto alla riservatezza, il diritto all'immagine, il diritto alla reputazione e il diritto all'identità personale.
Con l'avvento di Internet e con l'evolversi della società digitale, il diritto all'oblio assume un'ulteriore e diversa connotazione, legata alla capacità di conservazione nella rete di notizie pubblicate molto tempo prima, alla loro accessibilità e alla protezione dei dati personali[18].
Nel mondo iperconnesso e globale di internet, tutti sono esposti e tutti sono visibili: le miriadi di informazioni presenti in rete non solo non subiscono l'effetto erosivo del tempo, restando disponibili pressoché per sempre, ma sono altresì *facilmente* accessibili a tutti[19].
Si è così affermato, a livello giurisprudenziale, il diritto dell'individuo a una rappresentazione corretta e attuale della propria "identità digitale", inteso come giusta aspettativa del singolo a non essere permanentemente collegato - e di conseguenza identificato – con una notizia che sarebbe stata altrimenti dimenticata[20]; interesse da bilanciare con

---

15 Cass. civ., sez. I, ord. 20 marzo 2018, n. 6919, *Il Foro Italiano,* 2018, 1151 ss.

16 Cass. civ., sez. un., 22 luglio 2019, n. 19681.

17 *Ibid.* La Corte preliminarmente rileva che «quando si parla di riproposizione di una notizia precedentemente divulgata, non si ha a che fare con il diritto di cronaca (che riguarda il racconto di un fatto presente), ma più correttamente di "diritto alla rievocazione storica di quei fatti" che non gode della stessa garanzia costituzionale e che retrocede rispetto al diritto dei singoli […] Con la conseguenza che, se è pur vero che non può essere messa in discussione la scelta editoriale di procedere alla rievocazione storica di fatti ritenuti importanti – espressione della libertà di stampa e di espressione, essa deve svolgersi in forma anonima quando non vi sia un interesse qualificato alla diffusione dei nomi dei protagonisti, per la notorietà degli stessi o per il ruolo pubblico rivestito».

18 F. Di Ciommo, *Quello che il diritto non dice. Internet e oblio*, in *Danno e responsabilità,* 12, 2014, 1101 ss.

19 Come ha osservato recentemente Cass. civ., sez. I, 8 febbraio 2022, n. 3952: «nel mondo segnato dalla presenza di internet, le notizie sono sempre reperibili a distanza di anni dal verificarsi degli accadimenti che ne hanno imposto o comunque suggerito la prima diffusione».

20 Cass. civ., sez. III, 5 maggio 2012, n. 5525, in cui la Corte riconosce «il diritto soggettivo

il diritto della collettività ad essere informata e con l'esigenza di preservare la memoria storica collettiva.

Mentre il diritto all'oblio cd. tradizionale prevede quali strumenti di tutela a disposizione del singolo soltanto la rettifica e il risarcimento del danno cagionato, il diritto all'oblio nella sua accezione moderna prevede un ventaglio molto più ampio di rimedi, grazie ai nuovi strumenti a disposizione nel contesto digitale.

Accanto alla possibilità di ottenere la rettifica (e il risarcimento), l'interessato può chiedere l'aggiornamento della notizia, l'anonimizzazione, la de-indicizzazione delle pagine web, fino alla cancellazione dei propri dati personali[21].

Senza volere in questa sede ripercorrere le singole pronunce, è interessante notare come, dapprima a livello europeo e poi nazionale, si è andata via via cristallizzando l'idea che, tra i diversi rimedi azionabili dai singoli, la deindicizzazione sia lo strumento più adeguato a garantire un corretto bilanciamento tra diritti e interessi contrapposti, in quanto meglio di altri preserva la completezza delle fonti storiche senza pregiudicare il diritto all'oblio dell'individuo[22].

Quando si parla di deindicizzazione si intende la possibilità da parte dell'interessato di chiedere a un motore di ricerca di eliminare dall'elenco dei risultati che appare a seguito di una ricerca effettuata partendo dal nome della persona, i *link* verso pagine *web* contenenti informazioni relative a questo individuo.

I dati personali, quindi, non vengono cancellati e rimangono pubblicati online e visibili da chiunque, semplicemente non compariranno più nei risultati di ricerca effettuata a partire dal nome dell'interessato.

Il diritto all'oblio diventa pertanto il diritto a che una notizia non sia così facilmente reperibile online (*right not to be found easily*).

Anche recentemente la Corte di Cassazione ha ribadito che «la deindicizzazione dei contenuti presenti sul web rappresenta, il più delle volte, l'effettivo punto di equilibrio tra gli interessi in gioco. Essa integra, infatti, la soluzione che, a fronte della prospettata volontà, da parte dell'interessato, di essere dimenticato per il proprio coinvolgimento in una vicenda del passato, realizza il richiamato bilanciamento escludendo le estreme soluzioni che sono astrattamente configurabili: quella di lasciare tutto com'è e quella di cancellare completamente la notizia dal web, rimuovendola addirittura dal sito in cui è localizzata»[23].

La consacrazione del diritto del singolo a pretendere dal motore di ricerca la deindicizzazione dei propri dati personali si ha con la nota sentenza *Google Spain* della Corte di giustizia del 2014[24].

---

dell'individuo a che le informazioni che lo riguardano presenti in un archivio on line siano costantemente contestualizzate e aggiornate, a tutela della fedele rappresentazione dell'identità personale e sociale nel suo dinamico divenire».

[21] G.E. Vigevani, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *federalismi.it,* 19 settembre 2014.

[22] CEDU, *Biancardi c. Italy*, ric. 77419/16 (2021); *Hurbain c. Belgium,* ric. 57292/16 (2021); *M.L. and W.W. c. Germany*, ricc. 60798/10 e 6599/10 (2018). Per un'analisi approfondita, si veda M.R. Allegri, *Dimenticare, rievocare, rappresentare: dove conduce la via* dell'oblio, in questa *Rivista,* 2, 2022.

[23] Cass. civ., sez. I, 8 febbraio 2022, n. 3952.

[24] CGUE, C-131/12, *Costeja* (2014).

La Corte «preso atto che l'attività di un motore di ricerca può incidere, in modo rilevante, sui diritti personali al rispetto della vita privata e alla protezione dei dati personali, dal momento che facilita notevolmente l'accessibilità di tali informazioni a qualsiasi utente di internet», attribuisce all'interessato il diritto di rivolgersi direttamente al gestore del motore di ricerca per chiedere la deindicizzazione dei propri dati.
Secondo la Corte, i diritti della persona interessata prevalgono non solo sugli interessi economici del gestore del motore di ricerca, ma di norma anche sull'interesse degli utenti di Internet ad avere accesso alle informazioni; è tuttavia necessario ricercare il giusto equilibrio tra tali interessi confliggenti. Equilibrio che può dipendere «dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a ricevere tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica».
La Corte di giustizia europea attribuisce al gestore del motore di ricerca il compito di valutare la fondatezza delle richieste, precisando tuttavia che «qualora il responsabile del trattamento non dia seguito a tali domande, la persona interessata può adire l'autorità di controllo o l'autorità giudiziaria affinché queste effettuino le verifiche necessarie e ordinino a detto responsabile l'adozione di misure precise conseguenti».
Tra le critiche rivolte alla sentenza, la principale è stata quella di avere affidato a società private, quali sono i gestori dei motori di ricerca, un eccessivo potere discrezionale in sede di valutazione delle richieste, a cui si aggiungono – come ben osservato - la mancanza di trasparenza del procedimento applicato, l'assenza di un effettivo contraddittorio e di qualsiasi intervento per gli editori dei contenuti[25].
A seguito della pronuncia della Corte di giustizia, nel 2014 il Gruppo di lavoro "Articolo 29" (Art. 29 WP)[26] ha creato delle linee guida prevedendo dei criteri condivisi per la valutazione della fondatezza delle richieste di deindicizzazione[27].
Poco dopo, nel regolamento (UE) 2016/679 sulla protezione dei dati personali (GDPR) è stato formalmente recepito l'orientamento giurisprudenziale, con l'inserimento del «diritto all'oblio»[28] nell'art. 17.
Nel 2019 la Corte di giustizia europea è tornata a pronunciarsi nei confronti di Google[29], affrontando il tema del trattamento da parte del gestore del motore di ricerca di particolari categorie di dati, tra i quali – per quel che qui interessa - i dati relativi a reati e condanne[30].

---

[25] Così M.R. Allegri, *Dimenticare, rievocare, rappresentare: dove conduce la via dell'oblio*, cit., 99.

[26] Il gruppo di lavoro europeo indipendente, oggi confluito nel European Data Protection Board.

[27] Consultabili all'indirizzo *garanteprivacy.it.*

[28] A dire il vero, l'art. 17 ha contenuto più ampio del diritto sancito dalla sentenza *Costeja*, prevedendo anche il diritto alla cancellazione tout court dei dati personali e avendo quali destinatari tutti i titolari del trattamento e non soltanto il gestore del motore di ricerca. L'art. 17 per quel che qui più interessa, individua, al primo comma i motivi che un interessato può invocare per chiedere la cancellazione (o la deindicizzazione) dei dati e al terzo comma le eccezioni opponibili dal titolare del trattamento. Fra questa rileva soprattutto quella previsto sub a) cioè quando il trattamento dei dati sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione.

[29] CGUE, C-136/17, *CG et al. V. CNIL* (2019).

[30] La Corte chiarisce anzitutto che nel campo di applicazione dell'art. 8, par. 5, nella categoria dei

Ai fini dell'accoglimento della richiesta di deindicizzazione di pagine internet contenenti dati relativi a procedimenti penali, il motore di ricerca deve tenere conto di una serie di elementi, quali in particolare «la natura e la gravità del reato, lo svolgimento e l'esito di tale procedura, il tempo trascorso, il ruolo rivestito dalla persona coinvolta e il suo comportamento nel passato, l'interesse pubblico al momento della richiesta, il contenuto e la forma della pubblicazione, le ripercussioni della pubblicazione per tale persona» e sulla base di tutte le circostanze del caso, deve verificare se l'inserimento di detto link nei risultati di ricerca a partire dal nome dell'interessato, si riveli strettamente necessario per proteggere la libertà di informazione degli utenti di internet.
E anche nel caso in cui sia necessario mantenere quei contenuti indicizzati, il gestore è tenuto in ogni caso ad aggiornare l'elenco dei risultati collegati al nome della persona, affinché compaiano per primi i link verso pagine con informazioni più recenti in modo da riflettere la situazione giudiziaria attuale[31].
Per quel che attiene all'ordinamento interno, i principi stabiliti dalla Corte di giustizia europea a partire dalla sentenza *Costeja* sono stati pienamente recepiti dalle pronunce della Cassazione e del Garante della Privacy che, coerentemente con il quadro sopra tratteggiato, riconoscono la deindicizzazione quale principale strumento a garanzia del diritto all'oblio del singolo.

4. Il neo introdotto art. 64-*ter* disp. att. c.p.p.

È nel *parterre* giurisprudenziale e normativo sopra richiamato che si inscrive l'introduzione dell'art. 64-*ter* disp. att. c.p.p.[32], rubricato «diritto all'oblio degli imputati e delle persone sottoposte alle indagini».
Come emerge dal testo della norma, l'ex indagato o l'ex imputato nei cui confronti sia stata emessa una sentenza di proscioglimento o di non luogo a procedere, ovvero un provvedimento di archiviazione[33], può attivarsi per ottenere: a) un'inibitoria dell'in-

«dati relativi a infrazioni o condanne penali» vanno ricomprese anche le informazioni sull'apertura di inchieste giudiziarie o su indagini penali, a prescindere dall'esistenza di una condanna.

[31] *Ibid.*

[32] Quanto alla collocazione sistematica, la legge delega prevedeva di incidere sulle disposizioni attuative del codice di procedura penale in materia di comunicazione della sentenza. L'art. 64-*ter* disp. att. c.p.p. è stato inserito nel capo V "disposizioni relative agli atti", dopo l'art. 64-*bis* disp. att. c.p.p. che disciplina la comunicazione degli atti tra differenti giudici o pubblici ministeri. In un'ottica meramente sistematica, si evidenzia che sarebbe stato forse più aderente al criterio di delega l'inserimento della norma nel capo XI recante «disposizioni relative al dibattimento», e in particolare dopo l'art. 154-*ter* che disciplina le modalità di comunicazione della sentenza penale emessa nei confronti di un lavoratore dipendente di un'amministrazione pubblica. Trattasi infatti dell'unica norma che, nell'ambito delle disposizioni di attuazione, disciplina una forma di comunicazione del provvedimento all'esterno, e non solo tra differenti autorità giudiziarie, e per cui è stabilita un'autonoma competenza della cancellaria del giudice che ha emesso il provvedimento.

[33] In merito al presupposto che legittima l'attivazione del singolo interessato, l'art. 64-*ter* disp. att. c.p.p. richiama una serie di provvedimenti "favorevoli" quali titoli per richiedere la deindicizzazione o la preclusione dell'indicizzazione che non coincidono con quelli indicati nella legge delega (che si riferiva esclusivamente al decreto di archiviazione e alla sentenza di non luogo a procedere o di assoluzione). Come emerge dalla Relazione illustrativa, trattasi di una scelta ponderata del legislatore, che ha optato per «una formula armonizzatrice» più estesa poiché «non avrebbe senso, da un lato, includere i decreti

dicizzazione del provvedimento emesso nei suoi confronti e non ancora diffuso (ex ante); b) un titolo di *delisting* dei dati relativi al procedimento penale a suo carico già oggetto di divulgazione (ex post).

4.1. L'inibitoria dell'indicizzazione

La tutela di cui all'art. 64-*ter,* c. 2, disp. att. c.p.p., si traduce in un divieto di indicizzazione preventivo e originario del provvedimento «rispetto a ricerche condotte sulla rete internet a partire dal nominativo dell'istante».
Si tratta di una tutela che sulla carta appare di sicura portata innovativa, poiché introduce per la prima volta un istituto di carattere preventivo, applicabile prima della divulgazione della notizia. Per tale motivo, nei pochi commenti dottrinali sinora apparsi, il divieto di indicizzazione è stato definito estraneo al diritto all'oblio in senso tradizionale, che presuppone ontologicamente la dimenticanza di qualcosa che si conosce[34].
L'istituto, coerentemente con la finalità di prevenire un danno reputazionale da processo, è stato costruito sulla falsariga dell'oscuramento di cui all'art. 52, c. 1, Codice della Privacy[35].
Come evidenziato dal Garante della Privacy, l'inibitoria dell'indicizzazione costituisce una cautela volta a circoscrivere preventivamente gli effetti della pubblicità del provvedimento giudiziale[36].
Quanto alle modalità, vi deve essere un'espressa richiesta dell'interessato (si ritiene anche per il tramite del difensore), non potendosi ipotizzare attivazioni d'ufficio del Giudice che emette il provvedimento, né a maggior ragione della cancelleria, alla quale la norma attribuisce la competenza in merito al rilascio dell'annotazione.

ed escludere le ordinanze di archiviazione; dall'altro, includere le sentenze dibattimentali di assoluzione (art. 530) ed escludere quelle dibattimentali di non doversi procedere (artt. 529 e 531), quando le archiviazioni e le sentenze di non luogo a procedere vengono menzionate abbracciando qualunque "formula"».

[34] M. Marini, *Oblio, deindicizzazione e processo penale: dal diritto eurounitario alla Riforma Cartabia*, in *Sistema Penale*, 1, 2023, 5 ss.

[35] Si riporta il testo dell'art. 52 del d.lgs n. 196 del 2003 (come modificato dal d.lgs n. 101 del 2018): «1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento. 2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.
3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: 'In caso di diffusione omettere le generalità e gli altri dati identificativi di …' […]».

[36] Garante della Privacy, *Parere sullo schema di decreto legislativo di attuazione della legge 27 settembre 2021 n. 134, recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari,* Roma, 2022.

Dal tenore letterale della norma non sembra neppure ipotizzabile alcun preventivo vaglio da parte dell'autorità giudiziaria che ha emesso il provvedimento, sulla fondatezza dell'istanza, come invece accade per la richiesta di oscuramento di cui all'art. 52, c. 1, del Codice della Privacy.

La scelta di riservare la competenza alla cancelleria se da una parte risponde a esigenze di celerità tipiche dell'istituto, dall'altra non tiene conto di situazioni particolari di non immediata definizione: si pensi al caso di sentenze con plurimi capi di imputazione che abbiano assolto soltanto su alcuni e condannato su altri; in tali ultimi casi ci si domanda come debba comportarsi la cancelleria di fronte a un'istanza di inibizione, apparendo difficilmente ipotizzabile il rilascio di un'annotazione nei termini prescritti dalla norma.

L'art. 64-*ter* disp. att. c.p.p., inoltre, non specifica se esiste un termine per presentare l'istanza. Il fatto che si parli di provvedimento già emesso sembra escludere che si possa presentare in udienza prima della decisione, contrariamente a quanto invece previsto dall'art. 52, c. 1, Codice della Privacy; tuttavia, la finalità preventiva del divieto di indicizzazione, induce a ritenere che la richiesta da parte dell'interessato debba essere presentata in tempi contenuti, quantomeno fino a quando il provvedimento è ancora nella materiale disponibilità della cancelleria e non è stato oggetto di comunicazione all'esterno.

Stando al tenore letterale della norma, il divieto di indicizzazione riguarda esclusivamente «il provvedimento», vale a dire la sentenza di proscioglimento o di non luogo a procedere o il decreto (o ordinanza) di archiviazione.

Se si può comprendere la scelta del legislatore di garantire una sorta di anonimato anche sui provvedimenti positivi, dal momento che, come visto in premessa, il solo fatto di essere stato indagato può comportare un pregiudizio reputazionale, indipendentemente dall'esito assolutorio[37]; lascia alquanto perplessi la scelta di limitare l'inibitoria al solo provvedimento. In relazione a tale aspetto, il Garante della Privacy aveva suggerito di estendere la portata dell'attestazione preventiva ai contenuti e non solo al provvedimento in quanto tale, per far sì che tale forma di tutela potesse avere reale capacità innovativa.

In effetti, riflettendo su una possibile applicazione pratica dell'istituto, riteniamo che il divieto di indicizzazione del solo provvedimento non appaia realmente idoneo a tutelare il diritto alla riservatezza dell'ex imputato o ex indagato: difficilmente si assiste infatti alla diffusione del provvedimento in quanto tale, se non in siti istituzionali o su banche dati specialistiche, sulle quali tendenzialmente non si forma l'opinione pubblica. In tale contesto, l'oscuramento già previsto dall'art. 52, c. 1, del Codice della Privacy rimane comunque uno strumento più efficace nella tutela della riservatezza rispetto all'inibitoria, che rende possibile reperire il provvedimento, con tutti i dati in esso contenuti, a partire da ricerche formulate diversamente.

La prassi rivela inoltre che i maggiori danni reputazionali derivano dalla narrazione mediatica della vicenda giudiziaria e non certo dalla pubblicazione del provvedimento in sé. Motivo per il quale sarebbe stato opportuno estendere l'inibitoria, come solle-

[37] Si pensi ad esempio alla figura giornalistica dell'"ex-inquisito", espressione carica di un significato dispregiativo e stigmatizzante.

citato dal Garante, ai dati relativi al procedimento penale, così come previsto per la deindicizzazione.
In accoglimento della richiesta presentata dall'interessato, la cancelleria rilascia, come evidenziato in premessa, la seguente annotazione «ai sensi e nei limiti dell'art. 17 del regolamento (UE) 2016/679 […], è preclusa l'indicizzazione del presente provvedimento rispetto a ricerche condotte sulla rete internet a partire dal nominativo dell'istante». Si tratta di una formulazione piuttosto ambigua: infatti, se la locuzione «è preclusa» induce a ipotizzare il carattere perentorio del divieto, il richiamo «ai sensi e nei limiti» dell'art. 17 del regolamento lascia desumere una discrezionalità in capo al gestore del motore di ricerca nel non dare seguito all'annotazione, opponendo una delle plurime ragioni in base alle quali il trattamento di quei dati è da ritenere necessario (es: esercizio del diritto di informazione, adempimento di un obbligo giuridico, motivo di interesse pubblico).
Sul punto il Garante della Privacy aveva evidenziato che il richiamo dell'art. 17 del regolamento nella sua interezza, oltre ad apparire poco compatibile con una misura di carattere inibitorio, «sembra radicare, in capo al titolare del trattamento (o, in caso di sua inerzia, al Garante o all'autorità giudiziaria eventualmente aditi) un margine di discrezionalità valutativa in ordine all'inibitoria che contrasta con la ratio della norma, volta a precostituire un titolo (in questo caso insindacabile) per la sottrazione del provvedimento all'indicizzazione»[38]. In tal senso, invitava dunque il legislatore a valutare l'opportunità di espungere il riferimento a tale disposizione, nell'ambito della formulazione prescritta per l'attestazione preventiva. Tale monito è rimasto inosservato (cfr. Parere preventivo Garante Privacy).
In merito alla fase successiva al rilascio dell'attestazione, dal dato testuale non si evince cosa debba essere fatto dalla parte. Visto il carattere preventivo dell'istituto, quello che ci si può immaginare è che qualsiasi gestore del sito che voglia pubblicare il provvedimento dovrà astenersi dal farlo nel rispetto dell'annotazione. Non è invece plausibile ipotizzare un'attivazione da parte del singolo che di fatto, trasmettendo il provvedimento con la relativa annotazione, finirebbe comunque per divulgarlo.
La disciplina in esame non prevede rimedi specifici per un'eventuale inottemperanza o ritardo della cancelleria nel rilascio dell'attestazione, né chiarisce quale sia l'iter da seguire qualora il motore di ricerca non si adegui alla preclusione e indicizzi il provvedimento a partire dal nome dell'interessato. Certo è che, in tale ultimo caso, rimarrebbe attivabile il rimedio della deindicizzazione.

4.2. La deindicizzazione

La tutela di cui all'art. 64-*ter*, c. 3, disp. att. c.p.p., si traduce invece in un'attestazione della idoneità del titolo ad ottenere la deindicizzazione, da parte dei motori di ricerca generalisti, di contenuti relativi al procedimento penale rispetto a ricerche condotte a partire dal nominativo dell'istante. Si tratta di una forma di tutela successiva, utilizzabile dal singolo interessato una volta che l'indicizzazione è già avvenuta.

[38] Ivi, 6.

Come chiarito nei paragrafi che precedono, la deindicizzazione non comporta una cancellazione totale della notizia, ma rende semplicemente più difficoltoso il reperimento della stessa. Di fatto digitando il nome della persona non verranno più fuori le notizie riguardanti i procedimenti penali a suo carico che si sono conclusi positivamente.
Anche in questa ipotesi, la competenza è della cancelleria del giudice che ha emesso il provvedimento che, di fronte alla richiesta dell'interessato e in presenza dei presupposti, rilascerà l'annotazione senza alcun vaglio sul merito dell'istanza.
Non sono stabiliti termini, il che fa ritenere che non vi sia alcuna decadenza.
Una volta ottenuta l'attestazione da parte della cancelleria, l'interessato dovrà rivolgersi direttamente al motore di ricerca per richiedere la sottrazione dell'indicizzazione dei contenuti relativi al procedimento penale, rispetto a ricerche condotte a partire dal suo nominativo.
Anche in tal caso l'annotazione richiama «ai sensi e nei limiti» l'art. 17 del regolamento.
Su quest'ultimo aspetto, la relazione illustrativa chiarisce che «il rinvio all'art. 17 del regolamento senza ulteriori specificazioni appare in grado di meglio evocare - in modo recettizio - l'istituto del diritto all'oblio nella sua interezza, anche a fronte di future modifiche della disciplina U.E.»[39].
A differenza delle considerazioni relative al divieto di indicizzazione, nel caso di specie, la soluzione è stata ritenuta dal Garante «coerente, del resto, con la tassonomia dei vari interessi giuridici suscettibili di venire in rilievo nelle fattispecie concrete e […] conforme al vincolo al rispetto della disciplina di protezione dati contenuto nel criterio di delega»[40].
Dalla scelta effettuata per un rinvio mobile, anziché fisso, si desume che si tratta di una presunzione relativa di fondatezza dell'istanza e non assoluta e che pertanto rimane un margine di discrezionalità in capo al gestore del motore di ricerca di dar seguito alla deindicizzazione; in secondo luogo è ipotizzabile che, ai fini di un bilanciamento in concreto, rimanga impregiudicata, in caso di mancato adempimento da parte del motore di ricerca, la facoltà dell'interessato di adire il Garante della Privacy.

5. Conclusioni

Da quanto sinora osservato, risulta chiaro l'intento del legislatore di recepire il favor della giurisprudenza, soprattutto di carattere sovranazionale, rispetto all'istituto della deindicizzazione. Si tratta di un'operazione sicuramente importante dal punto di vista

[39] La Relazione illustrativa chiarisce che «il rinvio vuole garantire il rispetto della disciplina comunitaria, imposto dalla delega (e che) non si è ritenuto opportuno effettuare un rinvio maggiormente specifico, mediante espressa menzione dell'art. 17, comma 1, lett. e) e dell'art. 19 del Regolamento: ciò non perché si ritenga che dette norme non siano applicabili, ma all'opposto perché il rinvio all'art. 17 del Regolamento senza ulteriori specificazioni appare in grado di meglio evocare - in modo recettizio - l'istituto del diritto all'oblio nella sua interezza, anche a fronte di future modifiche della disciplina U.E.», *Relazione illustrativa aggiornata al testo definitivo del d.lgs. 10 ottobre 2022, n.* 150, Gazzetta Ufficiale (Serie Generale n. 245 del 19 ottobre 2022 - Suppl. Straordinario n. 5).

[40] *Ibid.*

simbolico. Così come appare indiscutibilmente innovativa l'introduzione di una tutela di carattere preventivo, azionabile prima che il soggetto sia stato esposto agli effetti distorsivi della giustizia mediatica.

Tuttavia, la formulazione della norma – sia per quel che dice, ma anche e soprattutto per quel che tace – presenta diverse criticità che ci inducono a dubitare dell'effettiva capacità di preservare il diritto all'oblio digitale degli imputati e delle persone sottoposte alle indagini.

Con riferimento al divieto di indicizzazione, come già evidenziato, la scelta di limitare l'oggetto della tutela al solo provvedimento e di stabilire un rinvio mobile all'art. 17 del regolamento, si è di fatto tradotta in un importante depotenziamento dell'istituto. In tal senso non ci paiono ipotizzabili nella prassi reali effetti dirimenti, o comunque più incisivi di quelli sinora prodotti dall'istituto dell'oscuramento di cui all'art. 52, c. 1, Codice della Privacy.

A ciò si aggiunga che la mancanza di chiare indicazioni in merito ad eventuali termini per la presentazione della richiesta, alla procedura da seguire una volta ottenuta l'annotazione, e ai rimedi nelle ipotesi di inottemperanza della cancelleria, anche in caso di sentenze parzialmente assolutorie, crea allo stato una grande senso di incertezza sull'applicazione dell'istituto e, conseguentemente, sulla sua efficacia nel concreto.

Intervistato sul punto, l'onorevole Costa, fautore dell'emendamento che ha portato all'introduzione dell'art. 64-*ter*, ha chiarito che «la legge Cartabia prevede […] la possibilità, insomma, di emanare decreti correttivi o integrativi. Magari può essere quella la sede per avviare una opportuna riflessione sui motori di ricerca»[41].

Riteniamo pertanto auspicabile che il legislatore intervenga sulla norma neo-introdotta, se non per correggerne le storture evidenziate sopra, quantomeno per colmare le lacune procedurali ad oggi presenti.

Con riferimento alla deindicizzazione, è innegabile che l'annotazione possa di fatto tradursi in un titolo rafforzativo delle istanze, che potrebbe facilitarne l'accoglimento da parte del motore di ricerca. Una prassi di questo tipo contribuirebbe indubbiamente a consolidare definitivamente l'orientamento, proveniente dall'Ufficio del Garante della Privacy, secondo cui le pronunce favorevoli costituiscono un valido presupposto normativo per ottenere la deindicizzazione.

Tale efficacia non è tuttavia scevra da criticità: se realmente l'istituto non dovesse trovare applicazione retroattiva, così come da alcuni sinora sostenuto[42], ci si domanda se in relazione ai procedimenti conclusi prima del 30 dicembre 2022, i motori di ricerca saranno più restii ad accogliere le istanze di deindicizzazione non accompagnate dalle annotazioni provenienti dalla cancelleria. Stessa prospettazione potrebbe ipotizzarsi per tutte quelle richieste che, pur avendo ad oggetto procedimenti conclusi a seguito dell'entrata in vigore della Riforma Cartabia, vengono presentate direttamente al motore di ricerca, senza una preventiva istanza ai sensi dell'art. 64-ter disp. att. c.p.p..

In tal caso sarebbe vanificato l'intento del legislatore di riconoscere una tutela su più

[41] Intervista rilasciata da Enrico Costa in *giornalettismo.com*, 3 gennaio 2023.

[42] Vedi sul punto F. Sarzana, *Diritto all'oblio per gli assolti. Ora è (finalmente) in vigore*, in *ildubbio.news*, 2 gennaio 2023.

livelli: l'annotazione finirebbe per porsi come strumento esclusivo, imponendo al singolo di doverla necessariamente richiedere, pur non conoscendo allo stato i tempi di risposta della cancelleria, gli eventuali rimedi azionabili in caso di inerzia della stessa e, soprattutto, non essendo certo dell'accoglimento dell'istanza da parte del motore di ricerca. Rimane infatti, come visto, lo stesso margine di discrezionalità in capo a quest'ultimo che potrebbe ritenere necessario, per tutti i motivi di cui al terzo comma dell'art. 17, mantenere l'indicizzazione dei dati personali dell'interessato.

Anche su tali ultimi aspetti sarebbe stata auspicabile l'approvazione di una disciplina transitoria che prevedesse l'applicazione retroattiva della norma, almeno con riferimento ad una finestra temporale ravvicinata in cui è ipotizzabile che l'interessato non si sia ancora attivato per domandare la deindicizzazione.

In conclusione, alla luce di tutte le considerazioni svolte e in attesa di conoscere l'effettivo impatto dei due istituti nella pratica, riteniamo che la norma non soddisfi appieno l'apprezzabile intento del legislatore di tutelare in sede extra-processuale i diritti di colui che è stato ingiustamente indagato o imputato, con il rischio che rimanga *inutiliter data*.

Il contrasto legislativo ai *socialbot* e le soluzioni avanzate nella Repubblica di Singapore e nella Repubblica d'Irlanda*

Alessandro Tedeschi Toschi - Giampaolo Berni Ferretti

Abstract

L'utilizzo dei *social media* ha permesso a chiunque di diffondere il proprio pensiero con una velocità ed una capillarità che eclissano quelle dei grandi organi di stampa tradizionali. All'interno di queste "piazze virtuali" operano anche i cosiddetti "*social bot*", dei programmi che, una volta forniti delle credenziali di accesso di un *account*, sono in grado di gestirlo in autonomia dando, però, l'impressione di essere una persona vera. La loro rapidità e precisione di reazione sui *social network* rendono questi "strumenti digitali" pericolosamente utili per la diffusione di contenuti favorevoli od ostili. Il recente impiego dei *socialbot* all'interno del dibattito elettorale e politico di diverse nazioni e le sue conseguenze hanno spinto i legislatori di diversi Stati ad intervenire contro questo fenomeno. Vengono qui prese in considerazione le riforme – e le proposte di riforma – avanzate nella Repubblica di Singapore e nella Repubblica d'Irlanda che specificamente mirano a contrastare l'uso di *social bot* con intenti malevoli o fuorvianti.

The use of social media has allowed anyone to spread their thoughts with a speed and a capillarity that eclipse those of the large traditional press companies. Within these "virtual squares" also operate the so-called "*social bot*," programs that, once provided with the login credentials of an account, can manage it independently, but giving the impression of being a real person. Their rapidity and precision of reaction on social networks make these "digital tools" dangerously useful for the dissemination of favourable or hostile content. The recent use of *socialbots* within the electoral and political debate of different nations and its consequences have prompted the legislators of various States to act against this phenomenon. We took into consideration here the reforms – and reform proposals – made in the Republic of Singapore and in the Republic of Ireland which specifically aim to counter the use of social bots with malicious or misleading intent.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Sommario

1. I *social bot* all'interno dei *social media*: diffusione e pericoli. – 2. I tentativi di riforma legislativa nel mondo. – 2.1. Il *Protection from Online Falsehoods and Manipulation Act* della Repubblica di Singapore. – 2.2. La *Online Advertising and Social Media (Transparency) Bill* 2017 della Repubblica d'Irlanda. – 3. Conclusioni.

Keywords

social network - automazione - *bot* - propaganda computazionale - disinformazione.

1. I *social bot* all'interno dei *social media*: diffusione e pericoli

La recente diffusione dell'utilizzo dei *social media* come strumenti di comunicazione e di divulgazione delle proprie opinioni ha portato a dei veri e propri sconvolgimenti nei modi e nei tempi di propagazione del pensiero. Grazie alle architetture digitali sviluppate negli ultimi anni e ospitate su infrastrutture capaci di gestire in autonomia e con perfetta precisione l'immensa mole di dati generati dalle azioni e dalle interazioni dei loro utenti (si calcola, ad esempio, che nel solo corso dell'agosto 2021 siano stati pubblicati 575.000 *tweet* ogni minuto)[1], la diffusione di contenuti e idee avviene oggi con una velocità ed una capillarità che eclissano quelle dei grandi organi di stampa tradizionali. Tuttavia, negli ultimi anni essi sono diventati anche un terreno fertile per la propaganda ed il proselitismo di tutti coloro che ne hanno compreso le potenzialità e hanno un minimo di cognizione del loro funzionamento[2].

Ad attrarre l'attenzione verso questi strumenti di comunicazione anche di soggetti pubblici e politici sono stati la facilità e la gratuità del loro utilizzo, il loro crescente impiego da parte delle persone come fonte di notizie ed il parallelo declino della carta stampata[3], nonché il conseguente avvicinamento dei *mass media* tradizionali a queste

[1] I dati statistici sono disponibili in S. Dixon, *Media usage in an online minute 2022*, in *statista.com*, 4 ottobre 2022.

[2] Si vedano, *ex multis*, S. Utz, *The (Potential) Benefits of Campaigning via Social Network Sites*, in *Journal of Computer-Mediated Communication*, 14(2), 2009, 221 ss.; S. Stieglitz – L. Dang-Xuan, *Social media and political communication: a social media analytics framework*, in *Social Network Analysis and Mining*, 3(4), 2013, 1277 ss.; G.S. Enli – E. Skogerbø, *Personalized Campaigns in Party-centred Politics Twitter and Facebook as Arenas for Political Communication*, in *Information, Communication & Society*, 16(5), 2013, 757 ss.; G.S. Enli, *Twitter as arena for the authentic outsider: exploring the social media campaigns of Trump and Clinton in the 2016 US presidential election*, in *European Journal of Communication*, 32(1), 2017, 50 ss.; B. Mclaughlin – T. Macafee, *Becoming a Presidential Candidate: Social Media Following and Politician Identification*, in *Mass Communication and Society*, 22(5), 2019, 584 ss.

[3] Si vedano, *ex multis*, S.A. Myers – A. Sharma – P. Gupta – J. Lin, *Information network or social network? The structure of the Twitter follow graph*, in *Proceedings of the 23rd International Conference on World Wide Web*, 2014, 493 ss.; H. Allcott – M. Gentzkow, *Social media and fake news in the 2016 election*, in *Journal of economic perspectives*, 31(2), 2017, 211 ss.; K. Shu – H.R. Bernard – H. Liu, *Studying fake news via network analysis: detection and mitigation*, in N. Agarwal – N. Dokoohaki – S. Tokdemir (a cura di), *Emerging research challenges and opportunities in computational social network analysis and mining*, Berlino, 2019, 43 ss. Inoltre, anche il *Digital News Report* del 2016 redatto dal Reuters Institute in collaborazione con l'Università di Oxford ha sottolineato la crescente importanza dei *social media* come fonte di notizie. Il rapporto è liberamente

piattaforme. A tali ragioni, poi, si aggiunge il fatto che essi garantiscono una forma di interazione non mediata ed istantanea con il pubblico, la quale permette di evitare verifiche puntigliose dei fatti, contestualizzazioni e valutazioni sulla fondatezza delle rivendicazioni da parte di critici, esperti e professionisti. Per di più, l'architettura fisica di qualsiasi *social network* non è quella di una grande infrastruttura "ministeriale", dove migliaia di persone devono coordinarsi assiduamente tramite una minuziosa ed intricata burocrazia per far sì che anche un solo slogan possa giungere ad una vasta platea di ascoltatori. Essa consiste, invece, unicamente in una rete di *server* connessi tra loro e capaci di svolgere in autonomia miliardi di operazioni in una frazione di secondo.
Soprattutto negli ultimi anni, in particolare durante la campagna referendaria sulla permanenza del Regno Unito di Gran Bretagna e Irlanda del Nord nell'Unione europea e le elezioni presidenziali negli Stati Uniti d'America del 2016, il ruolo che queste piattaforme hanno avuto come catalizzatori e motori del dibattito all'interno della società civile è risultato particolarmente evidente[4]. Dopo l'approvazione della Brexit e l'elezione di Donald J. Trump, l'ampio catalogo di studi sull'incidenza sulle dinamiche sociali – e perfino sulle votazioni politiche – delle discussioni e delle interazioni che avvengono sui *social network* ha posto anche in luce come attività ben studiate ed organizzate di creazione e condivisione di contenuti sulle piattaforme siano in grado di creare l'illusione di un ampio consenso su argomenti che in realtà non sono così popolari all'interno della società per così dire "non digitale"[5]. In particolare, riguardo al referendum britannico alcuni studi hanno messo in evidenza come il ruolo dei *social media* nella determinazione del suo esito sia stato marginale e allo stesso tempo fondamentale, data una suddivisione delle preferenze dei votanti abbastanza vicina alla parità[6]. Inoltre, il dibattito sviluppatosi *online* circa l'evento referendario d'oltremanica

disponibile in *Digital News Report 2016*, in *reutersinstitute.politic.ox.ac*, 2016.

[4] Si vedano, *ex multis*, M. Hänska – S. Bauchowitz, *Tweeting for Brexit: how social media influenced the referendum*, in J. Mair – T. Clark – N. Fowler – R. Snoddy – R. Tait (a cura di), *Brexit, Trump and the Media*, Bury St Edmunds, 2017, 31 ss., in cui gli autori fanno anche riferimento ad uno studio del 2015 condotto dalla Ofcom (l'autorità indipendente per la regolazione delle società di comunicazione del Regno Unito), dal quale è risultato che il 43% di coloro che consultavano notizie su Internet lo facevano tramite i *social media*, e ad uno del 2017 dal quale è risultato che della fascia d'età 16-24 anni il 61% degli appartenenti usava i *social* come primaria–ma non unica–fonte d'informazione; W. Hall – R. Tinati – W. Jennings, *From Brexit to Trump: Social Media's Role in Democracy*, in *Computer*, 51(1), 2018, 18 ss.; L. Luceri – A. Deb – S. Giordano – E. Ferrara, *Evolution of bot and human behavior during elections*, in *firstmonday.org*, 2019; N. Grinberg – K. Joseph – L. Friedland – B. Swire-Thompson – D. Lazer, *Fake news on Twitter during the 2016 US presidential election*, in *Science*, 363(6425), 2019, 374 ss.; Y. Gorodnichenko – T. Pham – O. Talavera, *Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #Uselection*, in *European Economic Review*, 136, 2021, 103772.

[5] Si vedano, *ex multis*, M. Hänska – S. Bauchowitz, *Tweeting for Brexit: how social media influenced the referendum*, cit.; N. Persily, *The 2016 U.S. Election: Can Democracy Survive the Internet?*, in *Journal of Democracy*, 28(2), 2017, 63 ss.; J.A. Tucker – Y. Theocharis – M.E. Roberts – P. Barberá, *From liberation to turmoil: social media and democracy*, in *Journal of Democracy*, 28(2), 2017, 46 ss.; S. Sanovich – D. Stukal – J.A. Tucker, *Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia*, in *Comparative Politics*, 50(3), 2018, 435 ss.; J.A. Tucker – A. Guess – P. Barberá – C. Vaccari – A. Siegel – S. Sanovich – D. Stukal – B. Nyham, *Social media, political polarization, and political disinformation: A review of the scientific literature*, in *ssrn.com*, 2018, in cui gli autori svolgono un'approfondita rassegna degli studi compiuti sull'argomento; Y. Gorodnichenko – T. Pham – O. Talavera, *Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #Uselection*, cit.

[6] Il "*Leave*" ha ottenuto il 51,8% dei voti mentre il "*Remain*" il 48,2%. I dati statistici sono stati

è stato anche il palcoscenico di un'estesa e strutturata operazione di propaganda sui *social* messa in atto da soggetti che di certo non avevano il diritto di esprimere il proprio voto nel corso della consultazione[7]: è stato ampiamente – ma solo successivamente – riportato come oltre 150.000 *account* localizzati all'interno della Federazione Russa abbiano pubblicato su Twitter contenuti inerenti alla Brexit, diffondendo tra gli elettori britannici informazioni non veritiere e dissimulandone la provenienza[8].

Insomma, queste "piazze digitali", ossia dei gruppi di *server* governati da *software* acritici e volti a permettere ai loro utenti la condivisione del maggior numero possibile di contenuti, hanno consentito a soggetti in possesso di capitali relativamente ridotti e di un certo grado di conoscenza del loro funzionamento di raggiungere una platea di proporzioni altrimenti inarrivabili e di crearsi, così, un seguito sempre pronto a promuovere e a condividere i contenuti che essi pubblicano sui *social*.

Quella che a prima vista pare una schiera di fedelissimi seguaci profondamente convinti della validità delle opinioni espresse da questi soggetti può, però, non essere effettivamente composta da esseri umani assiduamente presenti su queste piattaforme. Può trattarsi, invece, dei cosiddetti "*social bot*" o nella vulgata più comune – criticata da diversi ricercatori per la sua portata confusiva all'interno del dibattito – semplicemente "*bot*" (dalla contrazione delle parole *software robot*)[9], ossia dei programmi *software* autonomi progettati per agire su di un *social medium* simulando il modo in cui un utente umano si comporta su di esso. Tra questi vi è anche chi distingue la sottocategoria dei cosiddetti "*socialbot*" (una parola unica), spesso chiamati "*sybil*", ossia dei programmi *software* autonomi progettati per agire su di un *social medium* che, dissimulando la propria natura ed identità, si infiltrano nelle comunità *online* di utenti umani per diffondere contenuti (spesso mistificatori ed ingannevoli)[10].

L'utilizzo dei *socialbot* come strumenti di propaganda sui *social network*, oltre a giovarsi delle già viste caratteristiche di diffusione accelerata dei contenuti insite nell'architettura stessa di queste piattaforme, beneficia anche di un'altra importantissima caratte-

ottenuti consultando il sito della *Electoral Commission* britannica, l'ente indipendente di verifica dei risultati elettorali del Regno Unito, e sono disponibili in *Results and turnout at the EU referendum*, in *electoralcommission.org.uk*, 16 luglio 2019.

7 P.N. Howard – B. Kollanyi, *Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum*, in *ssrn.com*, 2016; M. Del Vicario – F. Zollo – G. Caldarelli – A. Scala – W. Quattrociocchi, *Mapping social dynamics on Facebook: The brexit debate*, in *Social Networks*, 50, 2017, 6 ss.; Digital, Culture, Media and Sport Committee della House of Commons, *Disinformation and 'fake news': Final Report*, HC1791, 2019; Y. Gorodnichenko – T. Pham – O. Talavera, *Social Media, Sentiment and Public Opinions: Evidence from #Brexit and #Uselection*, cit.

8 C. François, *Actors, Behaviours, Content: A Disinformation ABC*, in *Algorithms*, 2020; D. Wolchover – A. Robinson, *Is Brexit a Russia-backed Coup?*, in *New Law Journal*, 2020; J. Horder, *Online Free Speech and the Suppression of False Political Claims*, in *ILSA Journal of International and Comparative Law*, 2021.

9 Per un'accurata analisi della terminologia impiegata nella descrizione di questi particolari programmi *software* si veda quanto riportato in A. Tedeschi Toschi – G. Berni Ferretti, *Il contrasto legislativo ai socialbot e le soluzioni avanzate negli Stati Uniti d'America a livello federale e statale*, in *Diritto di Internet*, 3, 2022, 451 ss.

10 Y. Boshmaf – I. Muslukhov – K. Beznosov – M. Ripeanu, *The Socialbot Network: When Bots Socialize for Fame and Money*, in *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC '11)*, 2011, 93 ss.; L. Alvisi – A. Clement – A. Epasto – S. Lattanzi – A. Panconesi, *Sok: The evolution of sybil defense via social networks*, in *2013 IEEE symposium on security and privacy*, 2013, 382 ss.; O. Varol – E. Ferrara – C. Davis – F. Menczer – A. Flammini, *Online human-bot interactions: Detection, estimation, and characterization*, in *Proceedings of the international AAAI conference on web and social media*, 11(1), 2017, 280 ss.

ristica comune alla maggior parte delle tecnologie digitali: la ripetibilità[11]. Infatti, una volta creato un *socialbot* – un programma piuttosto "leggero" per le capacità di calcolo dei moderni computer – è possibile copiarlo e dare al suo clone le credenziali di un altro *account* nel giro di pochissimi minuti, creando così un secondo *follower*, che, come il primo, sarà un fedelissimo sostenitore di qualsiasi profilo sia programmato a seguire. Questo processo può essere quindi ripetuto un'altra volta e un'altra ancora, tanti quanti sono i profili che si hanno a disposizione, creando così folle oceaniche di sostenitori artificiali di chiunque possa permettersi di finanziare questo procedimento.

L'aspetto più problematico di un tale processo è il fatto che, come accennato, chiunque abbia o sia in grado di reperire un capitale adeguato (magari anche grazie all'aiuto di gruppi di interesse stranieri)[12] sarà in grado di crearsi una rete di fedelissimi seguaci artificiali programmati per osannarlo e per ripetere prontamente qualunque cosa dica, senza che questa sia effettivamente convincente, veritiera o anche solo rispettosa dei più basilari principi del rispetto della persona (finendo, così, col configurare questi seguaci sintetici come dei *socialbot*)[13], e che diano ai meno esperti l'illusione che sia invece il grande pubblico a condividere e a seguire le sue opinioni[14].

Oltre all'insidioso aspetto della dilatazione artificiale dell'apprezzamento esibito sui *social media* per alcuni soggetti (sia pubblici che politici), è stato osservato come i *socialbot* agiscano anche nell'alterazione dei temi e delle discussioni *online* tramite modalità meno celebrative dei loro "padroni" e delle dichiarazioni che questi fanno. Una parte non indifferente delle attività di questi agenti *software* viene, infatti, occupata dalla propagazione o dal supporto di contenuti, interpretazioni od opinioni legati a temi al

[11] O. Varol – E. Ferrara – C. Davis – F. Menczer – A. Flammini, *Online human-bot interactions: Detection, estimation, and characterization*, cit.; L. Luceri – A. Deb – S. Giordano – E. Ferrara, *Evolution of bot and human behavior during elections*, cit., in cui gli autori fanno anche riferimento a B. Mønsted – P. Sapiezynski – E. Ferrara – S. Lehmann, *Evidence of complex contagion of information in social media: An experiment using twitter bots*, in PLoS *ONE*,12, 2017, e0184148; O. Boichak – S. Jackson – J. Hemsley – S. Tanupabrungsun, *Automated diffusion? bots and their influence during the 2016 us presidential election*, in *International Conference on Information*, 2018, 17 ss.; C. Shao – G.L. Ciampaglia – O. Varol – K.C. Yang – A. Flammini – F. Menczer, *The spread of low-credibility content by social bots*, in *Nature communications*, 9(1), 2018, 47 ss.

[12] A questo riguardo si veda, in particolare, quanto accuratamente descritto in T.C. Helmus – E. Bodine-Baron – A. Radin – M. Magnuson – J. Mendelsohn – W. Marcellino – A. Bega – Z. Winkelman, *Russian social media influence: Understanding Russian propaganda in Eastern Europe*, Santa Monica, 2018; F. Giglietto – N. Righetti – G. Marino, *Understanding coordinated and inauthentic link sharing behavior on Facebook in the run-up to 2018 general election and 2019 European election in Italy*, in *osf.io*, 20 settembre 2019.

[13] Si veda a questo proposito l'analisi sul rischio di lesioni irreparabili della reputazione amplificate dall'uso di *socialbot* compiuta in A. Tedeschi Toschi – G. Berni Ferretti, *Social media, profili artificiali e tutela della reputazione. Come l'avvento dei social bot per la gestione dei profili social possa rappresentare una grave minaccia per la reputazione delle persone e quali potrebbero essere le risposte a tale pericolo*, in *Rivista Italiana di Informatica e Diritto*, 3(2), 2021, 107 ss.

[14] Y. Xie – F. Yu – Q. Ke – M. Abadi – E. Gillum – K. Vitaldevaria – J. Walter – J. Huang – Z.M. Mao, *Innocent by association: Early recognition of legitimate users*, in *Proceedings of the 2012 ACM Conference on Computer and Communications*, 2012, 353 ss.; D. Westerman – P.R. Spence – B. Van Der Heide, *A social network as information: The effect of system generated reports of connectedness on credibility and health care information on Twitter*, in *Computers in Human Behavior*, 28(1), 2012, 199 ss.; M. Forelle – P.N. Howard – A. Monroy-Hernández – S. Savage, *Political bots and the manipulation of public opinion in Venezuela*, in *ssrn.com*, 1 ss.; E. Ferrara – O. Varol – C. Davis – F. Menczer–A. Flammini, *The Rise of Social Bots*, in *Communications of the ACM*, 59(7), 2016, 96 ss.; S.C. Woolley, *Automating power: Social bot interference in global politics*, in *First Monday*, 21(4), 2016; D. Guilbeault, *Growing Bot Security: An Ecological View of Bot Agency*, in *International Journal of Communication*, 10, 2016, 5003 ss.

centro dell'interesse pubblico senza dare l'impressione che siano emanazione diretta di un determinato soggetto ma, invece, di un gruppo più o meno ampio e spontaneo. Questo approccio alla diffusione potenziata di determinati contenuti al centro del dibattito può essere spiegato dal fatto che, come già mostrato da alcuni importanti studi compiuti a metà del secolo scorso[15], la formazione del pensiero politico degli individui è influenzata da più reti interpersonali di natura diversa (come amicizie, colleghi di lavoro e famiglia), che essi tendono a prestare attenzione a ciò che sembra popolare e a fidarsi delle informazioni che circolano all'interno del loro contesto sociale[16] e che oggigiorno anche le cerchie virtuali di connessioni giocano un ruolo importante nella formazione delle convinzioni personali e delle opinioni politiche[17]. Così, l'uso dei *socialbot* è divenuto per tutti coloro che ne siano entrati in possesso grazie all'impiego di capitali propri o di terzi, da alcuni soprannominati anche «*augmented humans*» (ossia «umani potenziati»)[18], un valido strumento di sviamento del naturale orientamento delle discussioni *online* tra utenti ed un ancor più valido mezzo per indirizzare le persone attive sui *social* verso le loro posizioni, dando, però, l'illusione che queste siano popolari e condivisibili per via di una loro intrinseca validità e non a causa di un'intensa e ben finanziata campagna propagandistica.

Di fatto, quindi, chi sappia creare e ben orchestrare – oppure, più semplicemente, sia in grado di comprarsi – queste folle di utenti artificiali ben potrebbe fingersi un semplice interprete dei sentimenti delle masse attive *online*, anche se in verità ne sta dettando gli orientamenti in maniera unilaterale, o anche apparire completamente estraneo agli umori e alle direzioni presi da esse, pur essendone in realtà l'unico vero direttore. In altre parole, grazie ai *socialbot*, i soggetti in possesso delle giuste conoscenze possono presentarsi come dei moderni vati della società, quando in realtà, per usare le parole di Ferrara, Varol, Davis, Menczer e Flamini[19], sono dei burattinai che muovono a proprio piacimento i fili di migliaia di pupazzi digitali, liberi di orientarli nella direzione che più gli aggrada.

---

[15] P.F. Lazarsfeld – B. Berelson – H. Gaudet, *The People's Choice. How the Voter Makes Up His Mind in a Presidential Campaign*, New York, 1944; B.R. Berelson – P.F. Lazarsfeld – W.N. Mcphee, *Voting: a study of opinion formation in a presidential campaign*, Chicago, 1954; E. Katz – P.F. Lazarsfeld, *Personal influence: The part played by people in the flow of mass communications*, Glencoe, 1955.

[16] Y. Jun – R. Meng – G.V. Johar, *Perceived social presence reduces fact-checking*, in *Proceedings of the National Academy of Sciences*, 114(23), 2017, 5976 ss.; K.C. Yang – O. Varol – C. Davis – E. Ferrara – A. Flammini – F. Menczer, *Arming the public with artificial intelligence to counter social bots*, in *Human Behavior and Emerging Technologies*, 1(1), 2019, 48 ss.

[17] D. Centola, *The spread of behavior in an online social network experiment*, in *Science*, 329(5996), 2010, 1194 ss.; R.M. Bond – C.J. Fariss – J.J. Jones – A.D. Kramer – C. Marlow – J.E. Settle – J.H. Fowler, *A 61-million-person experiment in social influence and political mobilization*, in *Nature*, 489(7415), 2012, 295 ss.; L. Muchnik – S. Aral – S.J. Taylor, *Social influence bias: A randomized experiment*, in *Science*, 341(6146), 2013, 647 ss.; C. Becatti – G. Caldarelli – R. Lambiotte – F. Saracco, *Extracting significant signal of news consumption from social networks: the case of Twitter in Italian political elections*, in *Palgrave Communications*, 5(1), 2019, 1 ss., in cui gli autori fanno anche riferimento a G. Caldarelli, *Scale-Free Networks: Complex Webs in Nature and Technology*, Oxford, 2007; M.E.J. Newman, *Networks: an introduction*, New York, 2010.

[18] M. Stella – M. Cristoforetti – M. De Domenico, *Influence of augmented humans in online interactions during voting events*, in *PLoS ONE*, 14(5), 2019, e0214210, in cui gli autori usano questi termini per "*per indicare specificamente quegli* account *umani che sfruttano i* bot *per aumentare artificialmente, cioè* potenziare*, la loro influenza nel mondo digitale*".

[19] O. Varol – E. Ferrara – C. Davis – F. Menczer – A. Flammini, *The Rise of Social Bots*, cit., 103.

2. I tentativi di riforma legislativa nel mondo

Di fronte alle conseguenze delle influenze straniere sperimentate sui *social media* ed ai risultati concreti – soprattutto in ambito elettorale – di cui sono stati testimoni, i governi di diverse nazioni hanno istituito commissioni di indagine per comprendere a fondo quali fossero state le dinamiche all'interno delle reti sociali *online* che avevano avuto un'ascendente su questi risultati[20]. Le conclusioni a cui queste sono giunte si sono accompagnate, poi, ad un impegno da parte degli organi legislativi ad adottare delle riforme volte ad ostacolare le attività di disinformazione e di mistificazione avvenute sulle piattaforme digitali e che, come detto, avevano avuto riflessi incontrollati anche sulla società *off-line*. Un breve spazio di intervento legislativo è stato anche dedicato specificamente al contrasto delle attività di diffusione di contenuti compiute dai *socialbot* con, tuttavia, un'effettiva incidenza sul fenomeno che da alcuni è stata messa in dubbio[21].

Tra le poche nazioni a reagire attivamente – e legislativamente – alle attività di questi agenti *software* si sono distinti gli Stati Uniti d'America, i quali, però, nonostante la profondità degli effetti che la propaganda digitale di nazioni ad essi avverse aveva avuto sul loro tessuto sociale e politico, non sono ancora riusciti ad approvare una normativa federale[22]. Anche la piccola Repubblica di Singapore ha adottate alcuni provvedimenti di riforma del proprio ordinamento al fine di contrastare la diffusione – e soprattutto la credibilità – di contenuti fuorvianti, mistificatori o semplicemente falsi tramite Internet, i *social media* ed anche i *socialbot*. Invece, nella Repubblica d'Irlanda è in discussione al Dáil Éireann (la camera bassa del Parlamento) una proposta di legge per «garantire la trasparenza nella divulgazione delle informazioni nella pubblicità politica online». Avendo già in altra sede compiuto un esame delle normative statunitensi proposte od approvate di regolamentazione dell'uso di *social bot* e *socialbot*[23], di seguito vengono analizzate le disposizioni contenute nel *Protection from Online Falsehoods and Manipulation Act 2019* della Città dei Leoni e nell'*Online Advertising and Social Media (Transparency) Bill 2017* della repubblica dell'Isola di Smeraldo.

[20] Si vedano, ad esempio, le conclusioni a cui è giunta la U.S. Senate Select Committee on Intelligence sulle interferenze della Federazione Russa nelle elezioni presidenziali americane del 2016, la relazione (divisa in cinque parti) è disponibile per la consultazione in *Russian active measures campaigns and interference in the 2016 U.S. election*, *intelligence.senate.gov*, 10 novembre 2020, e i risultati a cui è pervenuta la Digital, Culture, Media and Sport Committee della House of Commons britannica sul ruolo occupato dagli apparati di disinformazione russi nell'influenzare il referendum sulla Brexit, il rapporto è già stato citato *supra* alla nota 10.

[21] S. Woolley – N. Monaco, *Amplify the party, suppress the opposition: social media, bots, and electoral fraud*, in *Georgetown Law Technology Review*, 4, 2020, 447 ss.

[22] Per una disamina delle normative proposte od approvate all'interno dell'ordinamento degli Stati Uniti d'America per contrastare le attività dei *socialbot* si veda A. Tedeschi Toschi – G. Berni Ferretti, *Il contrasto legislativo ai socialbot e le soluzioni avanzate negli Stati Uniti d'America a livello federale e statale*, cit.

[23] Ivi.

2.1. Il *Protection from Online Falsehoods and Manipulation Act 2019* della Repubblica di Singapore

Il 02 ottobre 2019 è entrato in vigore il *Protection from Online Falsehoods and Manipulation Act 2019* (*POFMA*), approvato dal Parlamento di Singapore il 03 giugno 2019[24]. Questa estesa normativa – composta da ben 62 Sezioni – è stata adottata dalla Città dei Leoni al fine di affrontare non solo l'impiego di *bot* per potenziare la propagazione di contenuti *online* ma soprattutto il più ampio problema della diffusione delle "*fake news*", ossia, come esplicitato nel preambolo della normativa stessa: «Per impedire la comunicazione elettronica a Singapore di false dichiarazioni su di un fatto, per sopprimere il supporto a e contrastare gli effetti di tale comunicazione, per salvaguardare dall'uso di *account online* per tale comunicazione e per la manipolazione delle informazioni, per consentire l'adozione di misure per migliorare la trasparenza degli annunci politici *online* e per questioni correlate»[25].

La volontà della Repubblica di Singapore di tutelare i suoi cittadini dall'esposizione a contenuti digitali falsi e manipolatori attraverso una normativa di ampio respiro è stata oggetto di numerose critiche da parte di gruppi internazionali di difesa dei diritti umani, quali la Commissione Internazionale dei Giuristi (ICJ)[26], Reporters Sans Frontiers[27] e Human Rights Watch[28], che hanno sostenuto che la legge sopprimerebbe indebitamente la libertà di parola e potrebbe essere utilizzata in modo abusivo dal governo per ridurre al silenzio qualsiasi forma di dissenso espresso *online*. Anche in dottrina è stato messo in evidenza da molti come sia evidente il potenziale effetto di diminuire il senso di libertà nell'esprimersi (per il quale viene spesso utilizzata in inglese la locuzione «*chilling effect on the freedom of speech*») e di indurre forme di auto-censura[29], nonostante le

[24] Il testo della legge assieme ai suoi emendamenti è disponibile è liberamente consultabile sul sito istituzionale del Governo di Singapore in *Protection from Online Falsehoods and Manipulation Act 2019*, in *sso.agc.gov.sg*, 2 ottobre 2019.

[25] Preambolo del *POFMA*.

[26] International Commission of Jurists, *Singapore: ICJ calls on government not to adopt online regulation bill in current form*, in *icj.org*, 12 aprile 2019.

[27] Reporters Sans Frontiers, *RSF explains why Singapore's anti-fake news bill is terrible*, in *rsf.org*, 8 aprile 2019.

[28] Human Rights Watch, *Singapore: Reject Sweeping 'Fake News' Bill Proposed Law Would Excessively Restrict Online Freedom of Speech*, in *hrw.org*, 3 aprile 2019.

[29] S. Chen – C.W. Chia, *Singapore's latest efforts at regulating online hate speech*, in *Research Collection School Of Law*, 6, 2019, 1 ss.; K. Han, *Big Brother's regional ripple effect: Singapore's recent "fake news" law which gives ministers the right to ban content they do not like, may encourage other regimes in south-east Asia to follow suit*, in *Index on Censorship*, 48(2), 2019, 67 ss.; H. Lee – T. Lee, *From contempt of court to fake news: public legitimisation and governance in mediated Singapore*, in *Media International Australia*, 173(1), 2019, 81 ss.; S. Neubronner, *Bill to Protect from Online Falsehoods: Refinements Needed*, in *RSIS Commentaries*, 85, 2019, 1 ss.; J. Horder, *Online Free Speech and the Suppression of False Political Claims*, cit.; R.K.C. Ren, *Suppressing Fake News or Chilling Free Speech: Are the Regulatory Regimes of Malaysia and Singapore Compatible With International Law?*, in *JMCL*, 47, 2020, 25 ss.; A. Carson – L. Fallon, *Fighting fake news: a study of online misinformation regulation in the Asia Pacific*, in *opal.latrobe.edu.au*, 2021, 1 ss.; R.K. Helm – H. Nasu, *Regulatory responses to 'fake news' and freedom of expression: normative and empirical evaluation*, in *Human Rights Law Review*, 21, 2021, 302 ss.; J.Y. Tay, *No news is good news, but "fake news" is bad news: A comparative analysis of Singapore's and Australia's measures to combat misinformation on social media*, in *Singapore Academy of Law Journal*, 33(2), 2021, 600 ss.; M. Mohan, *Singapore and the Universal Periodic Review: An Ongoing Human Rights Assessment*, in E. Yong Joong Lee (a

molteplici rassicurazioni ed i chiarimenti fatti dal Ministero di Giustizia singaporiano (il *Ministry of Law*) sul fatto che l'obiettivo della legge è di prendere di mira le falsità e non le opinioni, le critiche, le satire e le parodie, che il principale provvedimento adottabile dall'Autorità Competente è volto alla correzione e non alla rimozione dei contenuti e che qualsiasi decisione del Governo su ciò che debba considerarsi come «una falsa dichiarazione su di un fatto» potrà essere annullata da un tribunale[30].
Come accennato, il *POFMA* è una normativa piuttosto ampia che contiene definizioni e chiarimenti in merito a determinati termini (Parte 1), divieti di condotte relative alla diffusione di contenuti (Parte 2), indicazioni ("*directions*") alle autorità competenti su quando e come intervenire per contrastare la diffusione di affermazioni false (Parte 3), sanzioni comminabili a coloro che non ottemperano agli ordini delle autorità competenti (Parte 3), disposizioni procedurali per fare ricorso («*appeal*») presso la *General Division* della *High Court* contro le sanzioni irrogate (Parte 3), prescrizioni per gli *Internet Services Providers* e per i «*Providers of Mass Media Services*» (Parte 4), disposizioni in merito alla attestazione delle localizzazioni *online* ("*declaration of online locations*"), indicazioni per contrastare *account online* non autentici e comportamenti coordinati non autentici (Parte 6), disposizioni per gli intermediari di pubblicità *online* e di servizi Internet (Parte 7), indicazioni in merito alle autorità competenti alternative in periodo elettorale (Parte 8), indicazioni ("*directions*") sui soggetti che dovrebbero applicare gli ordini di interruzione dei servizi di accesso a Internet (Parte 9), disposizioni in merito all'ipotesi in cui sia un'impresa a compiere atti di diffusione di affermazioni false (Parte 9).
All'interno di questo vasto ed eterogeneo insieme di disposizioni che è il *Protection from Online Falsehoods and Manipulation Act 2019* ve ne sono anche diverse – e sparse – relative all'impiego dei *bot* per la diffusione di «false dichiarazioni su di un fatto» ed alle sanzioni applicabili per queste condotte.

(A) Definizione di *bot* – Nella prima parte della legge viene affermato che il termine «*bot*» indica: «Un programma per computer creato o alterato con lo scopo di eseguire attività automatizzate» e che gli *account* controllati da uno di questi agenti *software* non rientrano nella definizione contenuta nel *POFMA* di «*account online* non autentico»[31] (in originale «*inauthentic online account*»).
Pare qui opportuno iniziare precisando che l'esclusione degli *account* controllati da un *bot* dal novero di quelli definiti come «*account online* non autentici» non deriva dall'idea che si possa attribuire una qualche forma di autenticità alle condotte tenute su di un *social medium* da questa categoria di programmi *software* automatizzati, quanto, piuttosto, dal fatto che la stessa normativa di Singapore definisce un «*account online* non autentico» (in originale un «*inauthentic online account*») come un: «*Account online* che è controllato da una persona diversa dalla persona rappresentata (sia [che ciò avvenga] tramite il profilo

cura di), *ASEAN International Law*, Singapore, 2022, 427 ss.

[30] Si vedano la trascrizione del dibattito parlamentare avvenuto in data 8 maggio 2019 in sede di seconda lettura del *POFMA*, disponibile in *Official Reports – Parliamentary Debate (Hansard)*, in *sprs.parl.gov.sg*, ed il comunicato stampa del Ministry of Law di Singapore, *New Bill to Protect Society from Online Falsehoods and Malicious Actors*, in *mlaw.gov.sg*, 01 aprile 2019.

[31] Sezione 2 (1) del *POFMA*.

utente, l'identificatore univoco o altre informazioni) come il suo titolare, e la rappresentazione è effettuata con l'obiettivo di ingannare gli utenti finali a Singapore di un qualsiasi servizio di intermediazione di Internet sull'identità del titolare»[32].

In altre parole, il legislatore singaporiano ha attribuito alla definizione di «*account online* non autentico» gli stessi caratteri che la nostra giurisprudenza nazionale ha riconosciuto come integranti il reato di sostituzione di persona all'interno di un *social network*[33], distinguendo l'ipotesi in cui una persona usi un profilo *online* dotato di questo caratteri di inautenticità da quella in cui essa usi un *bot* per gestire un profilo ed attribuendo ad entrambe le eventualità il carattere di aggravio del disvalore delle condotte di diffusione di «false affermazioni su di un fatto» a Singapore (senza, però, prendere esplicitamente in considerazione l'eventualità che queste ipotesi vengano in concreto combinate)[34]. Questa strutturazione della normativa trova la propria motivazione nel fatto che il *POFMA* non ha come primario obiettivo quello di impedire l'uso di strumenti di automazione dei profili *online* ma solo di inibire il loro impiego per la propagazione "potenziata" di determinati contenuti, permettendo, quindi, al titolare effettivo di un *account* di lasciarlo in gestione ad un *bot*, purché con esso non compia degli illeciti. Riprendendo un esempio già fatto da altri[35], si pensi ad un giornalista finanziario che, per poter immediatamente informare i suoi lettori sulle variazioni di borsa tramite il proprio profilo *social*, abbia dato ad un *social bot* le credenziali di accesso ad esso e gli abbia dato il compito di pubblicare automaticamente un *post* ad ogni fluttuazione rilevante degli indici azionari. In base alla normativa della Città dei Leoni ciò sarebbe lecito perché il titolare dell'*account* è colui che lo gestisce – *rectius* che gestisce il *software* che a sua volta lo gestisce – e perché i contenuti pubblicati non verrebbero considerati dalle autorità come delle «false dichiarazioni su di un fatto».

Inoltre, è da sottolineare come la definizione di «*bot*» data all'interno del *POFMA* sia estremamente ampia e permetta, quindi, di sanzionare non solo il suo illecito impiego per la diffusione di «false dichiarazioni su di un fatto» all'interno di una determinata piattaforma come un *social medium* o, più in generale, su Internet ma addirittura attraverso l'uso di altre infrastrutture di comunicazione digitale. Infatti, la Sezione 3 (2)(b)

---

[32] Sezione 2 (1) del *POFMA*.

[33] Si vedano, ad esempio, Cass. Pen., sez. V, 23 luglio 2020, n. 22049, in cui viene specificamente affermato che «il reato di sostituzione di persona è integrato da colui che crea ed utilizza un profilo su *social network*, utilizzando abusivamente l'immagine di una persona del tutto inconsapevole, trattandosi di condotta idonea alla rappresentazione di una identità digitale non corrispondente al soggetto che lo utilizza», richiamando anche la precedente Cass. Pen., sez. V, 08 giugno 2018, n. 33862. Prima ancora Cass. Pen., sez. V, 16 giungo 2014, n. 25774, aveva sancito che «Integra il delitto di sostituzione di persona (art. 494 c.p.) la condotta di colui che crea ed utilizza un "*profilo*" su *social network*, utilizzando abusivamente l'immagine di una persona del tutto inconsapevole, associata ad un "*nickname*" di fantasia ed a caratteristiche personali negative».

[34] Più volte, infatti, all'interno della normativa vengono considerati come ipotesi separate l'uso di un «*account online* non autentico» o l'impiego di un *bot* per comunicare una falsa affermazione su di un fatto o accelerarne la diffusione. Si vedano ad esempio le Sezioni 7 (3) e 40 (4) del *POFMA*. Tuttavia, non si esclude che l'Autorità Competente possa ritenere di comminare il massimo delle sanzioni previste dalla legge, nel caso di combinazione dell'uso di un «*account online* non autentico» e di un *bot* per la sua gestione.

[35] Si veda, *ex multis*, G. Caldarelli – R. De Nicola – F. Del Vigna – M. Petrocchi – F. Saracco, *The role of bot squads in the political propaganda on Twitter*, in *Communication Physics*, 3(1), 2020, 1 ss.

esplicitamente dichiara che il divieto di compiere atti «per comunicare a Singapore una dichiarazione sapendo o avendo motivo di credere che (a) si tratti di una falsa dichiarazione su di fatto» si estende anche all'uso di MMS e SMS.
Infine, pare opportuno rilevare come dalla lettura della normativa scaturisca il dubbio se essa possa trovare applicazione anche quando la comunicazione di «false dichiarazioni su di un fatto» avvenga all'interno di una *intranet*[36]. Infatti, sebbene da un'interpretazione formalistica della lettera del *POFMA* sembra potersi escludere questa eventualità (la stessa definizione di "comunicare" contenuta nella Sezione 3 fa riferimento solo all'uso di Internet o di MMS e SMS), l'esclusione dell'uso di una struttura di comunicazione chiusa ma accessibile ad un numero potenzialmente molto alto di utenti – ed anche di *bot* – per la commissione dell'illecito al centro della normativa stessa pare più una svista del legislatore che una decisione ponderata[37].

(B) Fattori per determinare se un profilo *online* è controllato da un *bot* – Di fronte alla diffusione *online* di contenuti falsi su di un fatto, il *POFMA* indica anche una serie di fattori da prendere in considerazione per determinare se il profilo con cui è stata compiuta questa violazione sia gestito da un essere umano ovvero da un *bot*. La Sezione 40 (4), infatti, dispone che: «Nel determinare se un *account online* è un *account online* non autentico o è controllato da un *bot*, il Ministro [competente] deve tenere conto dei seguenti fattori: (a) se le informazioni utilizzate nella creazione del profilo *online* si riferiscono a un paese o un territorio diverso dal paese o territorio da cui presumibilmente proviene il titolare del profilo; (b) se esista uno schema di attività sospette svolte utilizzando l'*account online*[38]; (c) la data in cui è stato creato il profilo *online*; (d) qualsiasi altro fattore che il Ministro [competente] consideri rilevante».
Al fine, poi, di arginare l'eccessiva discrezionalità dell'Autorità nel determinare se dalle azioni compiute dal profilo considerato risulti evidente l'utilizzo di un *bot*, la successiva sottosezione (5) impone che qualsiasi provvedimento di restrizione dell'uso dell'*account* adottato (ossia qualsiasi "*Account Restriction Direction*") «deve identificare in modo sufficientemente dettagliato l'affermazione dell'oggetto o il comportamento del soggetto, a seconda dei casi».
L'inclusione nella normativa di indicazioni circa gli aspetti da valutare per determinare se la diffusione di «false dichiarazioni su di un fatto» sia stata compiuta tramite l'impiego di un *bot*, nonostante un'evidente vaghezza, ha il pregio di fornire una prima serie

[36] Per un'analisi del funzionamento di una *intranet* e dell'opportunità per le aziende di adottarne una si vedano, ad esempio, M. Hills, *Intranet business strategies*, Hoboken, 1996; S. Baker, *Getting the most from your intranet and extranet strategies*, in *Journal of Business Strategy*, 21, 2000, 40 ss.

[37] Si pensi, ad esempio, ad una persona che utilizzi un *bot*, ossia un programma per «eseguire attività automatizzate», per comunicare tramite la rete interna di un'impresa, ossia una *intranet*, con sede a Singapore delle «false dichiarazioni su di un fatto» a tutti i dipendenti di questa. Pur non essendo questo agente *software* connesso alla rete Internet mondiale e non potendo, quindi, diffondere "*online*" questi contenuti, il suo utilizzo potrebbe essere interpretato come una violazione del *POFMA*, dato che, riprendendo le parole della Sezione 7 (1), esso verrebbe impiegato «per comunicare a Singapore una affermazione sapendo o avendo motivo di credere che (a) si tratti di una falsa affermazione su di fatto» ad un numero potenzialmente molto alto di utenti che possono accedere all'infrastruttura digitale privata sulla quale avviene la trasmissione delle false informazioni.

[38] In originale alla Sezione 40 (4)(b) viene impiegata la locuzione «*pattern of suspicious activity*».

di indici che permetta alle Autorità di avere una direzione verso cui orientare lo svolgimento delle proprie indagini, mantenendo, comunque, grazie alla disposizione di cui alla lettera (d) della Sezione 40 (4), un certo grado di discrezionalità nella valutazione e soprattutto nell'inclusione degli elementi da cui desumere questo utilizzo per il compimento di un illecito. Inoltre, pare opportuno evidenziare come gli indici esplicitati nella normativa siano – in parte – quelli che già da tempo vengono stati utilizzati da molti ricercatori per stimare la presenza di *socialbot* sui *social media*[39]. Infatti, dal momento che per l'apertura di un profilo su di una piattaforma *social* non è richiesta alcuna certificazione da parte di una autorità centrale che attesti l'identità del creatore o dell'utilizzatore di questo, la maggior parte degli strumenti di rilevazione dei *socialbot* si sono strutturati in modo da giudicare la natura di chi gestisce un profilo *social* valutando la corrispondenza delle interazioni compiute con dei modelli comportamentali standard estrapolati dai dati statistici relativi ai comportamenti di un gran numero di profili usati da utenti umani. In altre parole, gli strumenti di controllo di "attività *bot*" oggi si basano principalmente sull'analisi dei comportamenti tenuti dai profili all'interno dei *social network* e sulla corrispondenza con gli atteggiamenti abitualmente tenuti in essi dalle persone. Questa metodologia di valutazione è operata prendendo in considerazione diversi elementi, quali la ricchezza di informazioni dei profili, la struttura delle reti sociali entro le quali sono attivi, i contenuti da questi pubblicati, il tono delle opinioni espresse ed il tempismo delle loro reazioni. Tuttavia, come già ben messo in evidenza in diversi studi[40], questi agenti *software* "malevoli" sono attivi già da molto tempo all'interno delle piattaforme *social* ed hanno subito – e continuano a subire – un affinamento ininterrotto delle loro *routine* interne di mimica dei comportamenti degli utenti umani[41]. Di conseguenza, ormai l'efficacia degli strumenti di rilevazione dipende in gran parte dal grado di sofisticatezza dei *socialbot* analizzati e, quindi, quelli maggiormente capaci di imitare le azioni compiute mediamente dagli utenti umani sono in grado di passare senza problemi il vaglio di questi strumenti di controllo[42]. Tutto ciò comporta che la

[39] Si veda, ad esempio, S. Cresci, *A decade of social bot detection*, in *Communications of the ACM*, 63(10), 2020, 72 ss., in cui l'autore svolge un'approfonditissima analisi dell'evoluzione dei *social bot* e dei metodi di analisi e rilevamento di questi.

[40] Si veda, *ex multis*, quanto dichiarato in Alvisi – Clement – Epasto – Lattanzi – Panconesi, *Sok: The evolution of sybil defense via social networks*, cit.; S. Cresci – R. Di Pietro – M. Petrocchi – A. Spognardi – M. Tesconi, *The paradigm-shift of social spambots*, in *Proceedings of the 26th international conference on world wide web companion*, 2017, 963 ss.; S. Cresci – R. Di Pietro – M. Petrocchi – A. Spognardi – M. Tesconi, *Social Fingerprinting: detection of spambot groups through DNA-inspired behavioural modelling*, in *IEEE Transactions on Dependable and Secure Computing*,15(4), 2017, 561 ss.; L. Luceri – A. Deb – S. Giordano – E. Ferrara, *Evolution of bot and human behavior during elections*, cit.; R.J. Schuchard – A.T. Crooks, *Insights into elections: An ensemble bot detection coverage framework applied to the 2018 U.S. midterm elections*, in *PLoS ONE*, 16(1), 2021, e0244309.

[41] K.C. Yang – R. Harkreader – G. Gu, *Empirical evaluation and new design for fighting evolving twitter spammers*, in *IEEE Transactions on Information Forensics and Security*, 8(8), 2013, 1280 ss.; K.C. Yang – O. Varol – C. Davis – E. Ferrara – A. Flammini – F. Menczer, *Arming the public with artificial intelligence to counter social bots*, cit.; S. Cresci, *A decade of social bot detection*, cit., in cui l'autore svolge un'approfonditissima analisi dell'evoluzione dei *social bot* e dei metodi di analisi e rilevamento di questi; M. Himelein-Wachowiak – S. Giorgi – A. Devoto – M. Rahman – L. Ungar – H.A. Schwartz – D.H. Epstein – L. Leggio – B. Curtis, *Bots and Misinformation Spread on Social Media: Implications for COVID-19*, in *Journal of Medical Internet Research*, 23(5), 2021, e26933.

[42] Si vedano, ad esempio, le conclusioni raggiunte in S. Cresci – R. Di Pietro – M. Petrocchi – A.

previsione di cui alla Sezione 40 (4)(b) del *POFMA* rischia di perdere di efficacia nella pratica, dato che le attività svolte dall'*account online* considerato rischiano di non destare sospetti per quanto riguarda aspetti comportamentali e di reattività.
Inoltre, anche la previsione della lettera (c) della medesima Sezione, relativa alla data di creazione del profilo, presenta alcune criticità, dato che è già stata ipotizzata da tempo l'esistenza di un mercato nero di *socialbot* riutilizzabili per campagne di disinformazione politica, i quali si appoggerebbero a profili vecchi di anni e già in precedenza molto attivi[43].
In definitiva, perché venga svolta un'accurata valutazione che permetta effettivamente di riconoscere se un *account* è gestito da un *bot* e, di conseguenza, possa essere adottato dall'Autorità Competente un provvedimento di restrizione del suo utilizzo (in originale una «*Account Restriction Direction*»), è di estrema importanza non limitarsi alla considerazione dei primi fattori elencati dalla Sezione 40 (4) del *POFMA* e dare, invece, il massimo risalto alla Sezione 40 (4)(d), che permette l'inclusione di elementi ulteriori (si spera, riprendendo gli studi e le ricerche più avanzate compiuti in ambito informatico)[44]. Questo perché, come sopra accennato in merito allo stato dell'arte della progettazione di questi programmi *software* automatizzati, già adesso le loro evoluzioni più sofisticate sono in grado di imitare le condotte degli utenti umani in modo sufficientemente credibile da non essere riconosciuti.

(C) Divieto di creazione o di alterazione di un *bot* per la comunicazione di false affermazioni su di un fatto a Singapore – Alla Sezione 8 (1) del *POFMA* viene sancito che: «Una persona non deve, sia dentro che fuori Singapore, creare o alterare un *bot* con l'intenzione di (a) comunicare a Singapore, tramite l'uso del *bot*, una falsa dichiarazione su di un fatto; oppure (b) consentire a qualsiasi altra persona di comunicare a Singapore, tramite l'uso del *bot*, una falsa dichiarazione su di un fatto».
In merito a questa disposizione pare opportuno preliminarmente sottolineare come essa determini l'integrazione di un reato non nel caso di realizzazione di un evento dannoso ma, invece, al semplice compimento di una condotta motivata dall'intenzione di commettere, poi, un altro atto illecito. Infatti, perché l'attività di creazione o di alterazione di un programma *software* autonomo assuma il carattere dell'antigiuridicità, la norma non prevede che con essa il suo autore abbia causato alcun danno ad altri ma solo che abbia tenuto dei comportamenti che il legislatore considera come idonei a porre in pericolo l'ordine pubblico di Singapore e la sicurezza dei suoi cittadini.

Spognardi – M. Tesconi, *The paradigm-shift of social spambots*, cit.

[43] E. Ferrara, *Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election*, in *First Monday*, 22(8), 2017, dove l'autore riferisce di aver riscontrato nei suoi studi dei *pattern* dell'uso di *account* anomali, dato che essi erano risultati molto attivi durante la campagna presidenziale statunitense del 2016 (supportando Donald J. Trump) e poi erano rimasti inattivi fino alle elezioni presidenziali francesi del 2017, durante le quali avevano contribuito alla campagna di disinformazione soprannominata *MacronLeaks* (attaccando Emmanuel Macron).

[44] Si vedano, ad esempio, le (dichiarate) promettenti opere di analisi dei comportamenti collettivi menzionate in S. Cresci – R. Di Pietro – M. Petrocchi – A. Spognardi – M. Tesconi, *The paradigm-shift of social spambots*, cit. e la tecnica di rilevamento di gruppi di *spambot* attraverso modelli comportamentali ispirati alla sequenziazione del DNA descritta in S. Cresci – R. Di Pietro – M. Petrocchi – A. Spognardi – M. Tesconi, *Social Fingerprinting: detection of spambot groups through DNA-inspired behavioural modelling*, cit.

Vi è, poi, da evidenziare come la Sezione 8 (1) non punisca la mera creazione di un agente *software* o la sua modifica – anche se con quest'ultima condotta è comunque possibile violare il diritto d'autore del suo creatore originale – ma richieda, invece, che il compimento di queste condotte sia motivato dalla finalità di utilizzare gli strumenti informatici creati o innovati per la diffusione di contenuti che contengano falsità su di un fatto perché esse vengano sanzionate come illecite. In altre parole, è solo in presenza dell'intenzione di impiegarne il prodotto per il compimento di un ben determinato crimine, ossia il comunicare ai destinatari di un'interazione *online* delle informazioni non veritiere (sancito come illecito dalla Sezione 7 del *POFMA*), che la creazione o la modifica di un programma *software* autonomo, fatto di per sé lecito (tranne nella già vista ipotesi di violazione del diritto d'autore di terzi), integrano il reato previsto dalla Sezione 8 (1) della normativa.

L'applicazione pratica delle disposizioni di questa Sezione rischia di risultare meno agevole di quanto non possa apparire a prima vista. Infatti, la comunicazione *online* di contenuti ritenuti affetti da falsità può avvenire sostanzialmente secondo due modalità: (I) tramite la pubblicazione in un determinato ambiente informatico di testi, immagini e video (ad esempio, su Facebook ciò può avvenire tramite la pubblicazione di un "*post*") oppure (II) attraverso la condivisione di contenuti già pubblicati altrove (quando la struttura dell'ambiente in cui il *bot* opera lo permette). Entrambe queste attività si basano sull'interazione di un *bot* con elementi solitamente esterni al proprio codice sorgente (nulla impedisce che gli elementi da pubblicare siano, invece, contenuti nel codice sorgente ma è buona pratica strutturare un programma *software* autonomo in modo che i dati che deve diffondere siano esterni ad esso) e che, quindi, possono essere compiute con finalità diverse nel tempo oppure anche esulando dal controllo del suo creatore[45].

Di conseguenza, per quanto riguarda la condotta di cui alla Sezione 8 (1)(a), ossia l'utilizzo di un *bot* da parte del suo creatore per la comunicazione di una falsa dichiarazione su di un fatto, è possibile immaginare che quest'ultimo si difenda dichiarando di averlo inizialmente realizzato solamente per potenziare la diffusione di contenuti leciti su Internet e che solo successivamente lo avesse impiegato per la pubblicazione di uno o più contenuti ritenuti falsi – e, quindi, illeciti – dall'Autorità Competente. Di fronte ad un'ipotesi di questo tipo, è facile vedere come non sia possibile desumere la sussistenza dell'intenzione di creare un *bot* per il compimento di un reato dalla sua semplice realizzazione, data la sua natura strumentale che ne permette l'impiego sia per

[45] Si pensi, ad esempio, ad un *social bot* programmato per pubblicare su di un *social medium* i contenuti presenti all'interno di un determinato *file* di testo presente nel computer su cui anch'esso è installato. In questo caso il suo programmatore lo ha sì creato per pubblicare un ampio numero di contenuti ma questi possono essere facilmente cambiati da chiunque. In altre parole, questo particolare tipo di *bot*, che può essere un semplice programma *software* in formato *.exe*, potrebbe contenere nel proprio codice sorgente le istruzioni per cercare all'interno della cartella in cui è installato un documento di testo, come un *file* in formato *.doc* (il classico *file* di Word), e di pubblicare il contenuto di questo documento – qualunque esso sia – in un *post* sul *social medium* a cui può accedere. Una strutturazione del *social bot* in questi termini permetterebbe, quindi, a chiunque di utilizzarlo per le pubblicazioni più disparate per natura e liceità, sia a dei programmatori che a degli utenti meno esperti (i quali, sebbene privi di conoscenze approfondite in campo informatico, sarebbero ben in grado di modificare un documento di testo in formato *.doc* e di avviare un programma in formato *.exe*).

il compimento di attività lecite che illecite[46]. In altre parole, dato che questi programmi *software* autonomi non sono intrinsecamente atti ad offendere, perché possa considerarsi violata la Sezione 8 del *POFMA*, sembra necessario provare la sussistenza della volontà di utilizzarli con finalità (illecite) di disinformazione già durante il processo di scrittura del loro codice sorgente e non semplicemente farla derivare dall'utilizzo da parte del loro creatore per «comunicare a Singapore […] una falsa dichiarazione su di un fatto». Quindi, per valutare se il creatore di un *bot* abbia effettivamente violato la specifica Sezione 8 (1)(a), risulta necessario riferirsi ad elementi ulteriori rispetto alla semplice comunicazione di falsità tramite esso come, ad esempio, lo scarto temporale tra la sua creazione ed il suo impiego per questa illecita attività (un uso criminoso immediatamente successivo alla sua creazione è un valido indizio delle intenzioni del suo creatore) o la natura e la quantità di tutti contenuti diffusi con esso (la pubblicazione di numerosi contenuti leciti e di pochi – o solo uno – affetti da falsità su di un fatto ben potrebbero suggerire un intento produttivo non motivato da intenzioni prettamente disinformative).

Per quanto riguarda, invece, la condotta di cui alla Sezione 8 (1)(b), cioè la creazione o l'alterazione di un *bot* per consentire ad altri la comunicazione tramite esso di una falsa dichiarazione su di un fatto, le osservazioni compiute *supra* in merito al fatto che la comunicazione *online* di contenuti si basa sostanzialmente sull'interazione di un *bot* con elementi solitamente esterni al proprio codice sorgente acquistano una rilevanza ancora maggiore. Se infatti, la previsione di cui alla Sezione precedentemente analizzata contempla la condotta di un solo soggetto, in questo secondo caso assume rilievo anche la condotta di un soggetto diverso rispetto al creatore dello strumento di propagazione dei contenuti illeciti. Ciò deriva dal fatto che, per come è strutturata questa Sezione del *POFMA*, viene attribuito il compimento di un autonomo reato a chiunque crei un *bot* con l'intenzione di far sì che esso venga utilizzato da altri per il materiale compimento delle illecite attività di disinformazione. In altre parole, la legge di Singapore non attribuisce al creatore del *bot* la qualifica di "ausiliatore" al compimento del reato di comunicazione di false dichiarazioni su di un fatto, nonostante egli abbia volontariamente fornito un aiuto materiale determinante all'esecuzione del reato di cui alla Sezione 7[47], ma lo considera come l'autore di un reato distinto. La vertebrazione di una condotta illecita secondo questa formula ha senz'altro il vantaggio di ammantare la legge singaporiana di una maggiore forza preventiva, dato che viene così a formarsi

[46] Questa osservazione viene avanzata anche in J. Horder, *Online Free Speech and the Suppression of False Political Claims*, cit., 16, dove l'autore fa anche riferimento alla difesa del libero uso di *bot* fatta in M. Lamo – R. Calo, *Regulating Bot Speech*, in *UCLA Law Review*, 66, 2019, 988 ss.

[47] In merito alla figura del complice "ausiliatore" all'interno del nostro ordinamento si vedano, invece, G. Fiandaca – E. Musco, *Diritto penale parte generale*, Bologna, 2009, 504, nonché le considerazioni esposte in merito alla posizione del cosiddetto "palo" nel reato di rapina in Cass. pen., sez. II, 9 novembre 1971, n. 2076, in cui gli Ermellini hanno affermato che «il c.d. "palo" deve considerarsi un cooperatore immediato, in quanto egli, pur senza porre in essere l'intera attività tipica, è perfettamente consapevole dell'azione delittuosa che si va compiendo, e partecipa ad essa in maniera efficace e nel momento della perpetrazione, consentendo ai correi di realizzare gli atti materiali di esecuzione con maggiore tranquillità e di sfuggire al pericolo di sorprese di ogni genere», e le recenti precisazioni compiute in Cass. Pen., sez. V, 09 novembre 2021, n. 8973, dove è stato dichiarato che l'ausiliatore è «colui che si limita ad apportare un qualsiasi aiuto materiale nella preparazione o nella esecuzione del reato».

l'antigiuridicità di una condotta prima ancora della causazione di un danno (il quale si può comunque individuare, tramite il preambolo e la dichiarazione dello scopo della legge esplicitata alla Sezione 5, nonché le ipotesi contenute alla Sezione 8 (3), nell'ingenerazione nel destinatario della comunicazione di un'impressione erronea su eventi o qualità di altri) e dato anche che le pene previste per la creazione finalizzata all'illecito utilizzo di un *bot* sono particolarmente severe[48].

Tuttavia, impernare l'attribuzione del carattere dell'antigiuridicità ad una condotta di per sé non bollata come proibita sulla base della semplice volontà di «consentire a qualsiasi altra persona di comunicare a Singapore, tramite l'uso del *bot*, una falsa dichiarazione su di un fatto» rischia di risultare estremamente controversa o inefficace. Infatti, dato che, come *supra* evidenziato, i *bot* non sono intrinsecamente atti ad offendere – come implicitamente riconosciuto dallo stesso legislatore singaporiano – e che possono essere utilizzati per diffondere sia contenuti leciti che illeciti, diventa estremamente importante definire cosa si intenda per «intenzione di […] (b) consentire a qualsiasi altra persona di comunicare» delle affermazioni ingannevoli. Questo perché, se per «intenzione» di permettere a terzi di utilizzare il programma *software* autonomo realizzato, si volesse ricomprendere la consapevolezza che detto programma può essere utilizzato per la diffusione dei più disparati contenuti – anche illeciti – e la conseguente accettazione del rischio che il terzo ricevente il *bot* lo usi, anche solo in un momento successivo e ad anni di distanza, per pubblicare non soltanto contenuti leciti ma anche alcuni mistificatori o falsi, allora, la creazione di qualsiasi *bot* potrebbe essere compiuta in violazione della Sezione 8 del *POFMA*. Se, invece, si volesse dare una più stretta interpretazione del concetto di «intenzione» di permettere a terzi di utilizzare l'agente *software* prodotto, intendendo con esso la sola volontà di apportare un aiuto materiale alla realizzazione del conosciuto progetto delittuoso di comunicare false affermazioni su di un fatto pianificato da colui al quale ha ceduto il *bot* (assumendo, così, una posizione assimilabile a quella dell'ausiliatore di un reato prevista dalla nostra giurisprudenza)[49], allora, sarebbe necessario per l'Autorità Competente provare che il creatore del *bot* fosse a conoscenza del disegno criminoso di colui che ha poi materialmente compiuto la comunicazione che viola la Sezione 7 del *POFMA* e che fosse sua effettiva intenzione agevolarne o consentirne la realizzazione. Questa seconda interpretazione, sebbene possa essere considerata come maggiormente ragionevole, avrebbe, però, per l'Autorità Competente un alto grado di difficoltà pratica, non solo perché in generale la prova della conoscenza da parte del creatore del *bot* dei fini illeciti del comunicatore dei contenuti non è agevole ma soprattutto perché, dato che questo programma *software* autonomo può essere facilmente inviato o condiviso tramite Internet, il grado di

[48] La sezione 8 (2) prevede per il creatore del *bot* che l'abbia usato per comunicare o facilitare ad altri la comunicazione di false affermazioni su di un fatto una pena fino a 500.000 dollari di Singapore e di 3 anni di reclusione (anche in combinazione tra loro) mentre la Sezione 8 (3) dispone, nel caso di comunicazioni che potrebbero ledere degli interessi pubblici, fino ad un milione di dollari di Singapore e 6 anni di reclusione.

[49] Si veda quanto riferito alla nota 47, tenendo, però, ben presente che la struttura dei due ordinamenti differisce profondamente circa l'integrazione del reato di produzione di *bot* per fini illeciti considerato dalla Sezione qui commentata e l'attribuzione del ruolo di ausiliatore al compimento di reati attuabile sulla scorta del nostro art. 110 c.p.

anonimato raggiungibile dalle parti coinvolte nel suo scambio è tale da permettere la ragionevole esclusione della conoscibilità sia dell'identità che delle reali intenzioni del cessionario del programma. A ciò si aggiunga, poi, che sempre a causa della strutturazione di Internet è anche possibile che, nonostante l'identificazione di una delle due parti della cessione del *software*, risulti impraticabile risalire all'identità dell'altra, lasciando così impunito uno dei crimini contemplati dalla normativa singaporiana.
Inoltre, vi è da notare come nella Sezione 8 (1)(b) del *POFMA* è la creazione (o l'alterazione) del *bot* con la finalità di permettere ad altri di impiegarlo in violazione della legge di Singapore a costituire la condotta antigiuridica e non, invece, la sua cessione a qualsiasi titolo a questi. Questa previsione ha il vantaggio per l'Autorità Competente procedente di evitarle di dover provare il trasferimento del *software* prodotto, dato che, come visto, questo può essere facilmente condiviso su Internet con molti mezzi che ben potrebbero anche renderlo irriconoscibile agli occhi di un osservatore esterno[50]. Allo stesso tempo, però, in assenza della cessione la violazione di questa specifica Sezione della normativa sembra estremamente ardua da provare.
Da ultima, appare opportuna una considerazione circa l'ipotesi in cui una persona crei o modifichi un *bot* con l'intenzione di utilizzarlo per comunicare o consentire ad altri di comunicare «una falsa dichiarazione su di un fatto» ma che esso non funzioni a causa di un errore di scrittura del codice sorgente. Sebbene all'atto pratico un agente *software* così configurato sarebbe incapace di svolgere il compito prefissato e, di conseguenza, non sarebbe utile al compimento del disegno criminoso disinformativo desiderato, non si può ritenere la condotta creativa completamente priva di idoneità alla commissione del delitto di comunicazione di false dichiarazioni su di un fatto e, quindi, non punibile e che invece debba essere dato il giusto risalto all'entità dell'errore presente nel codice. Questa conclusione deriva dal fatto che la creazione di programmi *software* autonomi non è semplice ed anche il minimo errore nella scrittura del loro codice sorgente può comportare la compilazione di un *set* di istruzioni incomprensibili per un computer (basta inserire una sola volta una virgola anziché un punto e virgola perché una macchina sia incapace di far funzionare correttamente un programma il cui codice è formato da centinaia di righe). Fonte di una tale conclusione è anche il fatto che esistono diversi programmi chiamati *debugger* specificamente progettati per l'analisi e l'eliminazione degli errori di programmazione (i *bug*) con cui poter tentare di correggere gli errori di scrittura e rendere successivamente – spesso dopo variati tentativi – idonei i *bot* ad agire in violazione della normativa qui considerata.

[50] Non è difficile immaginare una situazione in cui il creatore del *bot* ne invii una copia criptata tramite Internet al destinatario e solo in un momento successivo (ad esempio, in seguito ad un pagamento compiuto tramite criptovalute) gli invii anche la chiave di decriptazione. In questo modo chiunque intercetti la comunicazione o controlli i terminali usati per l'invio della copia dell'agente *software* in assenza della chiave si troverebbe di fronte ad un cumulo di dati incomprensibile con cui non sarebbe in grado di incriminare nessuna delle parti. Un'altra ipotesi non irrealistica, data la dimensione contenuta di questo tipo di *software*, sarebbe quella in cui il creatore nasconda il codice sorgente in una o più immagini tramite le pratiche di steganografia e lo invii all'utilizzatore, rendendo anche in questo caso quasi impossibile per l'Autorità Competente individuare la transazione ed incriminare tutti i soggetti coinvolti.

(D) Aggravante specifica per l'uso di un *bot* per la comunicazione di false affermazioni su di un fatto a Singapore – Come accennato *supra* all'inizio del paragrafo, il fine principale del *POFMA* è quello di «impedire la comunicazione elettronica a Singapore di false dichiarazioni su di un fatto» e di «sopprimere il supporto a e contrastare gli effetti di tale comunicazione». In base a questo obiettivo, la normativa statuisce che: «Una persona non deve compiere alcun atto all'interno o all'esterno di Singapore per comunicare a Singapore una affermazione sapendo o avendo motivo di credere che (a) si tratti di una falsa affermazione su di fatto; e (b) la comunicazione dell'affermazione a Singapore è probabile che (i) sia di pregiudizio per la sicurezza di Singapore o di qualsiasi parte di Singapore; (ii) sia di pregiudizio per la salute pubblica, la sicurezza pubblica, la tranquillità pubblica o le finanze pubbliche; (iii) pregiudicare le relazioni amichevoli di Singapore con altri paesi; (iv) influenzare l'esito di un'elezione alla carica di Presidente, un'elezione generale dei membri del Parlamento, un'elezione suppletiva di un membro del Parlamento o un referendum; (v) incitare sentimenti di inimicizia, odio o ostilità tra diversi gruppi di persone; oppure (vi) diminuire la fiducia del pubblico nell'adempimento di qualsiasi dovere o funzione o nell'esercizio di qualsiasi potere da parte del Governo, di un Organo di Stato, di un consiglio statutario o di una parte del Governo, di un Organo di Stato o di un consiglio statutario»[51].

Alla determinazione dell'antigiuridicità delle condotte appena elencate la Sezione 7 (3) aggiunge il riconoscimento come aggravamento del loro disvalore l'utilizzo di un «*bot*» per «(a) comunicare a Singapore la dichiarazione menzionata alla sottosezione (1); e (b) allo scopo di accelerare tale comunicazione».

Questa previsione di un'aggravante specifica per l'uso dei *bot* riconosce implicitamente la loro natura strumentale nel compimento di atti illeciti e, soprattutto, riconosce come essi siano estremamente utili per potenziare la diffusione di contenuti ritenuti dall'Autorità Competente come falsi e potenzialmente dannosi per l'ordine pubblico di Singapore o la sicurezza dei suoi cittadini[52]. Infatti, sebbene la sintassi impiegata alla Sezione 7 (3) non sia delle più felici, è possibile ricavare la loro identificazione come mezzi «per accelerare» la propagazione di comunicazioni viste come pregiudizievoli per i beni giuridici propri della collettività elencati dalla normativa stessa (Sezione 7 (1)(b) da (i) a (vi)). Inoltre, data la previsione di massimi edittali più alti rispetto alla semplice comunicazione di «una falsa affermazioni su di un fatto», pare evidente che il legislatore dia per scontato che il loro impiego permetta una lesione più grave. Ciò anche in ragione del fatto che, come già *supra* rilevato, questi agenti *software* possono facilmente essere – e spesso sono – impiegati in squadre o, comunque, può essere loro affidata la gestione di molteplici profili *online* al fine di dare ai meno esperti l'illusione che sia un vasto pubblico di utenti a condividere e a seguire le opinioni comunicate, in realtà, da uno o pochi soggetti che tirano i fili di questa compagnia di marionette digitali[53].

[51] Sezione 7 (1) del *POFMA*.

[52] Si tenga ben presente che all'interno della normativa qui considerata, per quanto riguarda il verbo "comunicare" (in originale «*communicate*»), la Sezione 3 (1) del *POFMA* specifica che «una dichiarazione o [un] contenuto viene comunicato a Singapore se è reso disponibile a uno o più utenti finali a Singapore su o tramite Internet».

[53] Si veda al proposito quanto riferito dagli autori citati *supra* alle note 11, 12, 14 e 19.

La particolare gravità con cui viene sanzionato l'impiego di *bot* per la comunicazione di false dichiarazioni su di un fatto che potrebbero compromettere l'armonia sociale di Singapore (la Sezione 7 (3) prevede l'irrogazione di pene con un massimo edittale di 100.000 dollari di Singapore e di 10 anni di carcere ovvero «in ogni altro caso» fino ad un milione di dollari di Singapore) trova la base della propria giustificazione nella considerazione che oggi anche le cerchie virtuali di connessioni giocano un ruolo importante nella formazione delle convinzioni personali e delle opinioni politiche, che già da tempo vien fatto un massiccio impiego dissimulato di questi programmi *software* autonomi per la diffusione di contenuti *online* che vengano percepiti dagli utenti umani come espressione di un genuino e condivisibile sentimento popolare[54] e che proprio questa suggestione di apprezzamento diffuso può avere l'effetto di sviare artificiosamente lo sviluppo delle convinzioni personali, come già messo in luce da alcuni celebri studi[55].

In ultima analisi, la specifica previsione di una circostanza aggravante del reato di cui alla Sezione 7 (1) integrata dall'uso dei *bot*, mostra – almeno agli occhi di scrive – che il legislatore di Singapore abbia compreso la loro natura di moltiplicatori, anzi, di elevatori alla potenza[56] dell'estensione della diffusione *online* di contenuti (in particolare sui *social media*) e, quindi, della potenziale portata offensiva delle condotte disinformative considerate all'interno della normativa qui analizzata.

(E) Provvedimenti di restrizione dell'uso di un *account* gestito da un *bot* – La previsione della Sezione 40 di attribuire all'Autorità Competente il potere di adottare i provvedimenti di restrizione dell'uso dell'*account* (chiamati "*Account Restriction Directions*") che essa abbia riconosciuto come gestito da un *bot* trasmette – almeno a chi scrive – l'impressione che il legislatore di Singapore abbia sottovalutato una delle caratteristiche fondamentali di questo genere di programmi *software* automatizzati: il fatto che essi vengono progettati per funzionare su di una determinata piattaforma e non per gestire un determinato profilo. Infatti, per compiere un accesso ad una qualsiasi infrastruttura informatica, un *bot* si limita ad utilizzare delle credenziali di accesso, ossia una combinazione di termini quali *username* (oppure indirizzo *e-mail*) e *password*, e ad in-

[54] J. Ratkiewicz – M. Conover – M. Meiss – B. Gonçalves – A. Flammini – F. Menczer, *Detecting and tracking political abuse in social media*, in *Fifth international AAAI conference on weblogs and social media*, 5(1), 2011, 297 ss.; J. Ratkiewicz – M. Conover – M. Meiss – B. Gonçalves – S. Patil – A. Flammini – F. Menczer, *Truthy: Mapping the spread of astroturf in microblog streams*, in *WWW '11: Proceedings of the 20th International Conference Companion on World Wide Web*, 2011, 249 ss.; N. Abokhodair – D. Yoo – D.W. Mcdonald, *Dissecting a Social Botnet: Growth, Content and Influence in Twitter*, in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15)*, 2015, 839 ss.; S.C. Woolley, *Automating power: Social bot interference in global politics*, cit.

[55] Si vedano le note 15, 16 e 17.

[56] L'avanzamento della definizione dei *bot* come "elevatori a potenza delle diffusione di contenuti *online*" deriva dal fatto che Internet ed in particolare i *social media* sono già stati definiti come dei «moltiplicatori di discorsi d'odio (*hate speech*) e di notizie false (*fake news*)» in M.R. Allegri, *Alcune considerazioni sulla responsabilità degli intermediari digitali, e particolarmente dei social network provider, per i contenuti prodotti dagli utenti*, in *Informatica e Diritto*, 26(1), 2017, 104-105, dove l'autrice fa anche riferimento a C.R. Sunstein, *Republic. com. Cittadini informati o consumatori di informazioni?*, Bologna, 2003, 82 ss.; C.R. Sunstein, *Voci, gossip e false dicerie*, Milano, 2010; G. Pitruzzella – O. Pollicino – S. Quintarelli, *Parole e potere. Libertà di espressione, hate speech e fake news*, Milano, 2017; Aa.Vv., in questa *Rivista*, 1, 2017, spec. 11-115.

terfacciarsi con un ambiente standardizzato e per lui ben riconoscibile. Di conseguenza, in caso di applicazione di restrizioni all'*account* gestito da un *bot*, nulla impedisce al suo "padrone" di fornirgli le credenziali di accesso ad un altro profilo[57], rendendo nei fatti inefficace il provvedimento che vorrebbe impedire la prosecuzione dell'opera di diffusione *online* potenziata di contenuti mendaci.

Una soluzione (di poco) più efficace e fin troppo lapidaria sarebbe stata, quindi, quella di imporre delle restrizioni non tanto all'uso dell'*account* utilizzato per la diffusione automatizzata di contenuti illeciti quanto alla possibilità di accedere ad Internet all'indirizzo IP collegato all'*account* incriminato o, per quanto possibile, al soggetto beneficiario dei servizi di intermediazione di Internet che sia stato individuato come titolare del profilo incriminato[58]. Tuttavia, questa ipotesi è stata esclusa dal *POFMA*, come si può desumere dalla lettura combinata delle Sezioni 2 e 40 (1). Infatti, dalla quarantesima Sezione è possibile ricavare che, in caso di condotte criminose compiute con l'ausilio di un «*account online* non autentico» («*inauthentic online account*») o di un *bot* – ipotesi espressamente considerate alla Sezione 40 (2)(c) – a detto profilo il fornitore dei servizi di intermediazione di Internet (in originale «*Internet intermediary*») debba, su provvedimento motivato (ossia una «*direction*») dell'Autorità Competente, impedire che esso possa usufruire dei suoi servizi per «comunicare qualsiasi affermazione a Singapore» (Sezione 40 (1)(a)) e che debba impedire a chiunque di poter utilizzare l'*account* per «interagire con qualsiasi utente finale» dei suoi servizi (Sezione 40 (1)(b)). Dalla lettura della Sezione 2, poi, si ricava che per «fornitore dei servizi di intermediazione di Internet» si intende colui che permette ai propri utenti di «accedere a contenuti provenienti da terzi su o tramite Internet», di trasmettere questi contenuti su o tramite Internet e di fare ricerche *online* e di consultare i contenuti trovati[59] mentre da questa categoria ne viene esplicitamente escluso il fornitore di accesso ad Internet e di servizi di «incremento della capacità di elaborazione o la capacità di archiviazione di un computer», ossia l'*Internet Service Provider* che consente la connessione al *web* o, ad esempio, il fornitore di servizi di *cloud computing*[60]. In altre parole, le restrizioni che l'Autorità Competente può richiedere

[57] Questa operazione può risultare particolarmente facile e veloce. Chi scrive, infatti, è stato capace di creare un *social bot* – invero molto rudimentale – che per compiere l'accesso ad un *social medium* era programmato per cercare delle credenziali di accesso in un file esterno in formato *.txt*, permettendo così al suo gestore di cambiare i dati per l'accesso senza dover intervenire sul codice sorgente (operazione comunque non eccessivamente complicata) ma, semplicemente, modificando un file di testo (consultato poi in automatico dal programma).

[58] In merito alla maggiore rilevanza dell'indirizzo IP rispetto al semplice *nickname* di un profilo *online* si vedano le considerazioni della nostra giurisprudenza espresse in Cass. Pen., sez. V, 22 novembre 2017, n. 5352, e in Cass. Pen., sez. V, 05 febbraio 2018, n. 5352.

[59] Il *POFMA* stesso fornisce alla Sezione 2 un esempio di quali siano i «servizi di intermediazione di Internet» che identificano i soggetti che devono, su richiesta dell'Autorità Competente, restringere l'uso di un *account*. Esso contempla: servizi di *social networking*, servizi di ricerca *online*, servizi di aggregazione di contenuti, servizi di messaggistica basati su Internet e servizi di condivisione di video. Ne deriva, quindi, che le società che gestiscono piattaforme come, rispettivamente, Facebook, Google, Flipboard, WhatsApp e YouTube possono essere i destinatari di provvedimenti di restrizione dell'uso dei profili dei loro utenti.

[60] Dall'interpretazione delle definizioni contenute alla Sezione 2 – in particolare, della definizione di *Internet intermediary service* – è, quindi, possibile escludere dal novero degli *Internet intermediary* società quali, ad esempio, la AT&T e la Amazon Web Services.

in base alla Sezione 40 (1) del *POFMA* all'*Internet intermediary* si limitano a colpire l'accessibilità di un *account* ad alcune funzionalità di Internet e l'accessibilità a detto profilo per interagire con altri, lasciando così spazio alla creazione di nuovi profili *online* con cui continuare l'opera di disinformazione.

Rimane, comunque, da notare come la chiusura – *rectius* la limitazione delle attività in rete – di un *account* che fosse effettivamente gestito da un *bot* avrebbe il vantaggio di rallentare l'attività di diffusione di contenuti da questo tipo di programma *software*, dato che gli potrebbe poi essere assegnato solamente un profilo privo di quella rete di contatti sociali (il *social network*, appunto) che rendeva efficace la diffusione automatizzata di contenuti *online* e che sarebbe, quindi, necessario parecchio tempo per ricostituirla o per crearne un'altra delle medesime dimensioni.

Infine, pare qui opportuno sottolineare come dalla lettura delle condizioni elencate alla Sezione 40 (2) necessarie perché l'Autorità Competente possa adottare un provvedimento di restrizione dell'uso di un *account* emerga che il legislatore di Singapore non abbia considerato illecito il semplice controllo di un profilo *online* da parte di un *bot* ma, invece, che perché l'Autorità abbia il potere di intervenire sia necessario il soddisfacimento congiunto di molteplici condizioni (tra cui l'effettivo compimento di un illecito tramite esso).

Come visto, oltre alle numerose critiche di facilità d'impiego della normativa della Repubblica di Singapore qui brevemente analizzata come strumento del governo per ridurre al silenzio il dissenso e le critiche[61], sono riscontrabili anche diverse problematiche relative allo specifico ambito della regolamentazione dell'uso di programmi *software* autonomi per la diffusione automatizzata e potenziata di contenuti *online*. Infatti, sebbene dalla lettura del *POFMA* traspaia la comprensione della natura dei *bot* come neutra, strumentale e di elevatori alla potenza della diffusività di contenuti sul *web*, le soluzioni accolte lasciano, comunque, aperte delle "porte sul retro" (per riprendere il termine "*backdoor*", utilizzato in ambito informatico per indicare dei metodi e degli accorgimenti utili ad aggirare le misure di sicurezza di un sistema o di un'infrastruttura) che rischiano di inficiare l'efficacia della sua applicazione. In ultima analisi, anche se la normativa della Città dei Leoni contiene diverse criticità nel suo tentativo di arginare l'utilizzo dei *bot* come strumento di propagazione potenziata di contenuti mistificatori e dannosi ed evidenzi l'orientamento «autoritario e paternalistico» del legislatore singaporiano[62], appaiono, comunque, calzanti le parole di Jones, per la quale «il diritto alla libertà di espressione non implica che le tecniche di manipolazione dell'attenzione, come l'uso di *bot* e *troll*, debbano essere prive di restrizioni»[63].

[61] Si vedano le critiche *supra* menzionate alle note 26, 27, 28 e 29.

[62] A. Carson – L. Fallon, *Fighting fake news: a study of online misinformation regulation in the Asia Pacific*, cit., 15.

[63] K. Jones, *Online Disinformation and Political Discourse: Applying a Human Rights Framework*, in *chathamhouse.org*, novembre 2019, 45 e 56.

2.2. La *Online Advertising and Social Media (Transparency) Bill* 2017 della Repubblica d'Irlanda

Nell'ambito normativo europeo stiamo assistendo da alcuni anni – soprattutto dopo le interferenze nel dibattito *online* sull'evento referendario britannico del 2016[64] – ad una crescente attenzione ai fenomeni dei comportamenti coordinati ed inautentici sul *web* e, soprattutto, sui *social media*. L'interesse dei legislatori del Vecchio Continente si è, così, tradotto in diverse iniziative di riforma delle normative nazionali e comunitarie[65]. Tra le prime pare qui interessante prendere in considerazione quella avanzata al Dáil Éireann (la camera bassa del Parlamento) della Repubblica d'Irlanda, ossia la *Online Advertising and Social Media (Transparency) Bill 2017*[66].
Anche la proposta legislativa attualmente dibattuta alla camera bassa irlandese ha il fine di affrontare il più ampio problema dell'opacità nelle pratiche di pubblicità politica *online* e, come la normativa della Repubblica di Singapore appena analizzata, contiene solo alcune disposizioni contro l'impiego malevolo dei *bot*. A differenza, però, della normativa dell'Isola dei Leoni, la *OASM Bill* ritiene illecito l'uso di questi agenti *software* solo quando sia caratterizzato da finalità politiche.

(A) Definizione di *bot* – Alla Sezione 2 (1) della *OASM Bill* viene data la definizione di «*bot*» come di un: «Qualsiasi elemento di un *software* che è programmato per eseguire compiti automatizzati su una piattaforma *online*».
Viene poi specificato che nella definizione di «piattaforma *online*» rilevante per la legge viene ricompreso: «Qualsiasi sito *web*, applicazione *web* o applicazione digitale (che include un *social network* o un motore di ricerca) che ha 10.000 o più visitatori unici visitatori o utenti unici mensili nello Stato in almeno sei dei dodici mesi precedenti; ovvero, quando la piattaforma *online* è rivolta a un pubblico locale o regionale, che ha 1.000 o più visitatori o utenti unici mensili nello Stato in almeno sei dei precedenti dodici mesi»[67].
Preliminarmente, si può notare come una delineazione in questi termini dei «*bot*» riecheggi le nozioni di "*bot*" e di "*internet bot*" (detti anche "*web bot*") avanzate da Tsvetkova, Garcia-Gavilanes, Floridi e Yasseri[68], riprendendo, per la prima, le analisi compiute

[64] Si veda quanto detto *supra* al paragrafo 1 e, in particolare, alle note 5, 7 e 8.

[65] In merito alla normativa dell'Unione si veda la recente proposta di regolamento *relativo a un mercato unico dei servizi digitali* (COM(2020) 825), nella quale, ai Paragrafi 57 e 68, vengono espressamente presi in considerazione i *bot* come strumenti «che possono condurre alla rapida e ampia diffusione di informazioni che costituiscono contenuti illegali» (Paragrafo 57). Si veda anche lo *Strengthened Code of Practice on Disinformation 2022*, un codice di autoregolamentazione per i gestori delle piattaforme online promosso dalla Commissione europea.

[66] Il testo della proposta di legge presentata il 06 dicembre 2017 al Dáil Éireann è liberamente consultabile sul sito istituzionale dell'Oireachtas (il parlamento irlandese) in *Online Advertising and Social Media (Transparency) Bill 2017*, in *oireachtas.ie*, 6 dicembre 2017.

[67] Sezione 2 (1) della *OASM Bill*.

[68] M. Tsvetkova – R. García-Gavilanes – L. Floridi – T. Yasseri, *Even good bots fight: The case of Wikipedia*, in *PLoS ONE*, 12(2), 2017, spec. 1-2.

da Franklin e Graesser[69] e, per la seconda, anche quelle di Berners-Lee e Cailliau[70], Koster[71] e Cheong[72]. Infatti, parafrasando le parole di Tsvetkova, Garcia-Gavilanes, Floridi e Yasseri, è possibile descrivere un *internet bot* come un programma *software* che viene eseguito in continuazione e che è in grado – senza alcun intervento umano – di attivarsi al verificarsi di determinate condizioni e di individuare le azioni da compiere per portare a termini i compiti affidatigli, avendo consapevolezza dell'ambiente informatico *online* in cui opera ed adattandosi autonomamente ai cambiamenti di questo.
Per quanto riguarda la definizione di «piattaforma *online*» contenuta sempre nella Sezione 2 (1) si può notare come il legislatore irlandese abbia ripreso ampiamente la definizione dei medesimi termini contenuti nel Paragrafo 17940 del *California Business and Professions Code* (introdotto nel settembre del 2018 con la promulgazione del *Bolstering Online Transparency Act of 2018* (S.B. 1001))[73]. Infatti, la normativa d'oltreoceano identifica come «piattaforma *online*» un: «Qualsiasi sito *web*, applicazione *web* o applicazione digitale rivolta al pubblico, inclusi un *social network* o una pubblicazione, che abbia 10.000.000 o più di visitatori o utenti mensili unici negli Stati Uniti per la maggior parte dei mesi durante i 12 mesi precedenti»[74].
Inoltre, è possibile notare come la proposta normativa irlandese si differenzi da quella singaporiana per quanto riguarda l'identificazione delle strutture entro cui sono in grado di operare i *bot*, pur finendo con l'ottenere un risultato estremamente simile. Infatti, mentre la normativa dell'Isola dei Leoni vieta espressamente l'uso di SMS e MMS per l'illecita diffusione di «una falsa dichiarazione su di un fatto»,[75] quella dell'Isola di Smeraldo accoglie una definizione di «piattaforma *online*» che, grazie anche all'inclusione di «qualsiasi […] applicazione digitale», risulta sufficientemente generica ed aperta da annoverare non solo le applicazioni basate sull'uso delle reti GSM e UMTS (le prime a permettere l'invio di SMS e MMS) ma anche altre tecnologie digitali tra quelle illecitamente utilizzabili per far sì che un profilo gestito da un «*bot*» appaia come quello di un individuo e diffonda messaggi elettorali o politici.

(B) Reato di utilizzo di un *bot* per realizzare presenze multiple *online* con il fine politico di presentarsi come un profilo individuale – È la Sezione 6 della *OASM Bill* a determinare le condizioni in base alle quali l'utilizzo di un *bot* integri un illecito (una «*offence*»). In essa, intitolata «reato di utilizzo di un *bot* per realizzare presenze multiple *online* con il fine politico di presentarsi come un *account* o un profilo individuale su di una piattaforma *online*», viene stabilito che: «Chiunque utilizzi consapevolmente

[69] S. Franklin – A. Graesser, *Is It an Agent, or Just a Program? A Taxonomy for Autonomous Agents*, in J.P. Müller – M.J. Wooldridge – N.R. Jennings (a cura di), *Intelligent Agents III Agent Theories, Architectures, and Languages*, Heidelberg, 1996, 21 ss.

[70] T. Berners-Lee – R. Cailliau, *The world wide web project*, in *World Wide Web*, 1991.

[71] M. Koster, *Guidelines for robot writers*, in *info.webcrawler.com*, 1993.

[72] F.C. Cheong, *Internet agents: spiders, wanderers, brokers, and bots*, Thousand Oaks (USA), 1993.

[73] Per un'approfondita disamina della normativa statale di contrasto delle attività dei *bot* per finalità politiche della California si veda A. Tedeschi Toschi – G. Berni Ferretti, *Il contrasto legislativo ai socialbot e le soluzioni avanzate negli Stati Uniti d'America a livello federale e statale*, cit., spec. paragrafo 4.4.

[74] Paragrafo 17940 (c) del *California Business and Professions Code.*

[75] Sezione 3 (2)(b) del *POFMA.*

un *bot*, o lo faccia utilizzare, in modo tale da far sì che più presenze *online* con un fine politico si presentino a un utente di una piattaforma *online* come un *account* o un profilo individuale su qualsiasi piattaforma *online* è colpevole di un reato»[76].

Preliminarmente, è necessario rivolgere l'attenzione al significato che viene dato ai termini «fine politico» (in originale «*towards a political end*») all'interno della normativa in oggetto. Questo perché esso riveste un'importanza cruciale nel determinare quando l'uso di un *internet bot* non sia considerato illecito e quando, invece, lo sia, dato che anche nel caso di questo legislatore pare – almeno a chi scrive – essere stata fatta propria la considerazione che i *bot* non sono intrinsecamente atti ad offendere (come implicitamente riconosciuto pure da quello di Singapore)[77] e che possono, quindi, essere utilizzati per diffondere sia contenuti leciti che illeciti. Infatti, viene poi precisato che una «questione» (in originale «*matter*») è considerata come «avente un fine politico» (in originale «*directed towards a political end*») solo: «Se comunica un messaggio che promuove uno o più candidati a cariche pubbliche in un'elezione all'interno dello Stato o un partito politico registrato nel registro dei partiti politici, o se promuove un messaggio su una questione di interesse o importanza politica o una questione che, al momento in cui la pubblicità *online* è posta o promossa, è in discussione o che si intende presentare a una delle Camere dell'Oireachtas o dell'Assemblea dell'Irlanda del Nord o del Parlamento europeo o di un'autorità locale all'interno dello Stato o che sia oggetto di un referendum o che ha una qualsiasi relazione con una controversia industriale in corso nello Stato»[78].

Dalle parole della Sezione 6 si può, quindi, ricavare che la *OASM Bill*, al pari del *BOT Act* californiano e del *POFMA* singaporiano, non istituirebbe un divieto *tout-court* dell'uso di *bot* ma si limiterebbe, invece, a vietare determinate modalità di impiego di essi. Rispetto alla normativa della piccola repubblica del sud-est asiatico, poi, la proposta di legge presentata al Dáil Éireann prevede un ambito di illiceità dell'utilizzo di questi agenti *software* ancora più ristretto, dato che quest'ultima stabilisce la rilevanza penale del loro impiego solo quando sia dissimulato, avvicinandola di più all'ordinamento della Stato d'Oro (che espressamente dichiara illegale fuorviare un'altra persona sulla propria identità artificiale)[79].

In aggiunta, questa proposta di legge risulta avere un ambito di applicazione ancora più ristretto di quello della sua (ormai approvata) controparte di Singapore, in quanto riconosce come reato non il semplice utilizzo di un *internet bot* per la gestione di un profilo ma, invece, ritiene penalmente rilevante il suo utilizzo solo per realizzare «più presenze *online*» (in originale «*multiple online presences*»), le quali vengono indicate nella Sezione 2 (1) in un numero minimo pari a 25 *account* o profili[80]. In altre parole, l'uti-

[76] Il testo in lingua originale della Sezione 6 (1) della *OASM Bill* recita «*Any person who knowingly uses a bot, or causes a bot to be used, in such a way as to cause multiple online presences that are directed towards a political end to present to a user of an online platform as an individual account or profile on any online platform shall be guilty of an offence*».

[77] Si veda in merito quanto detto *supra* al paragrafo 2.1.(C) e, in particolare, quanto riportato alla nota 46.

[78] Sezione 2 (2) della *OASM Bill*.

[79] Paragrafo 17941 (a) del *California Business and Professions Code*.

[80] Come rimarcato anche dal promotore della *OASM Bill*, il deputato James Lawless, nel corso del

lizzo dissimulato di un programma *software* autonomo verrebbe qui reso un illecito (e, quindi, rappresentante una minaccia per la società irlandese) solamente quando esso renda l'impressione che un intero gruppo di persone condivida un messaggio politico «per disinformare o ingannare il pubblico in modo malevolo»[81]. La costituzione della normativa in questi termini mostra come il legislatore irlandese abbia ben compreso come sia facile fornire ad un *bot* le credenziali di accesso ad uno o più profili *online*[82] e farglieli gestire in autonomia e come essi possano rappresentare una seria minaccia non singolarmente ma quando, invece, operano in modo coordinato e mascherato nella gestione di ampi gruppi di *account*[83].

Sempre nel paragone con la legge dell'Isola dei Leoni, poi, vi è da notare come in merito ai contenuti la cui comunicazione costituisce un delitto la *OASM Bill* sia caratterizzata da una maggior ampiezza. Mentre, infatti, la prima ritiene antigiuridica la diffusione di «false affermazioni su di un fatto» che si sappiano o si suppongano poter essere di pregiudizio per l'ordine pubblico di Singapore e per i suoi cittadini[84], per la seconda è sufficiente che essa promuova «uno o più candidati a una carica pubblica in un'elezione […] o un partito politico registrato»[85] oppure «un messaggio su una questione di interesse o importanza politica»[86]. In altre parole, perché si possa considerare violata la Sezione 6 della proposta di legge irlandese è sufficiente usare un *internet bot* per costituire una "presenza *online* con un fine politico", ossia impiegarlo per fargli gestire in forma dissimulata venticinque o più profili *online* con cui diffondere contenuti propagandistici in favore di determinati soggetti o posizioni politiche (dando, quindi, la falsa impressione che questi siano più popolari di quanto non siano in realtà)[87]. La

dibattito del 13 dicembre 2017, disponibile in *Dáil Éireann debate*, in *oireacthtais.ie*, 13 dicembre 2017.

81 *Ibid.*

82 Si veda a questo riguardo quanto descritto *supra* alla nota 57.

83 Questa considerazione viene anche espressa nella Sezione 2 del *Bot Disclosure and Accountability Act of 2018* (S. 3127), presentato al Senato degli Stati Uniti d'America e in cui viene affermato che i *bot* vengono impiegati «per creare un effetto carrozzone, per costruire false tendenze sui *social media* diffondendo automaticamente gli *hashtag*, e anche per sopprimere le opinioni dell'opposizione». Per un'analisi del testo di questa proposta di legge federale americana si veda A. Tedeschi Toschi – G. Berni Ferretti, *Il contrasto legislativo ai socialbot e le soluzioni avanzate negli Stati Uniti d'America a livello federale e statale*, cit.

84 Sezione 7 (1)(b), da (i) a (vi), del *Protection from Online Falsehoods and Manipulation Act 2019*, la quale ha comunque suscitato critiche in merito al fatto che la tutela dell'ordine pubblico di Singapore potrebbe facilmente essere usata come scusa dal governo per ridurre al silenzio il dissenso e le critiche alle autorità (si vedano le critiche *supra* menzionate alle note 26, 27, 28 e 29).

85 Sezione 2 (2) della *OASM Bill.*

86 *Ibid.*

87 In merito alle analisi condotte sull'impiego dei *bot* per distorcere le discussioni *online* su determinati temi, stimolare i seguaci di ideologie o personaggi pubblici e per generare false impressioni di popolarità si vedano E. Mustafaraj – P.T. Metaxas, *From obscurity to prominence in minutes: Political speech and real-time search*, in *Proceedings of the WebSci10*, 2010; J. Ratkiewicz – M. Conover – M. Meiss – B. Gonçalves – A. Flammini – F. Menczer, *Detecting and tracking political abuse in social media*, cit.; Z. Chu – S. Gianvecchio – H. Wang – S. Jajodia, *Detecting automation of Twitter accounts: Are you a human, bot, or cyborg?*, in *IEEE Transactions on Dependable and Secure Computing*, 9(6), 2012, 811 ss.; C. Wagner – S. Mitter – C. Körner – M. Strohmaier, *When social bots attack: Modeling susceptibility of users in online social networks*, in *Proceedings of the WWW '12 Workshop on 'Making sense of microposts'*, 2012, 41 ss.; A. Bessi – E. Ferrara, *Social bots distort the 2016 US Presidential election online discussion*, in *First Monday*, 21(11), 2016; P.N. Howard – B. Kollanyi, *Bots, #Strongerin, and #Brexit: Computational Propaganda During the UK-EU Referendum*, cit.; S.C. Woolley,

strutturazione della normativa dell'Isola di Smeraldo secondo questi termini, invero abbastanza simile a quella dello Stato della California[88], pone, però, tre problemi di puntualizzazione: quando si possa parlare (i.) di comunicazione di un messaggio, (ii.) di contenuti che effettivamente promuovono un candidato od un partito e (iii.) di questione di interesse o di importanza politica.

(i.) Modalità di comunicazione di un messaggio – Per quanto riguarda il primo dei problemi di puntualizzazione congeniti nella *OASM Bill*, bisogna partire dalla considerazione che su Internet il concetto di "comunicazione" da applicare alla definizione di cui alla Sezione 2 (2) può includere una varietà più o meno ampia di azioni, a seconda delle conoscenze e dell'opinione di chi si potrebbe trovare a dover interpretare questa disposizione. Infatti, se da un lato è evidente che azioni compiute da un *bot* come l'invio di messaggi su di un'applicazione di messaggistica *online* ad un determinato destinatario[89], l'invio di una *e-mail* o la pubblicazione di un commento ai contenuti condivisi da altri utenti su di un *social medium* costituiscano delle comunicazioni – in particolare la prima – o comunque delle interazioni con una persona rilevanti per la Sezione 6 della proposta di legge irlandese, altre tipologie di azioni, come la pubblicazione di contenuti sulle piattaforme *social* o la ri-condivisione di contenuti di altri possono far sorgere dei problemi interpretativi[90]. Sembra, però, possibile attribuire anche a queste ultime condotte il concetto di "comunicazione", dato che i contenuti pubblicati all'interno dello "spazio personale" *online* di un profilo *social* (come, ad esempio, il "*diario personale*" di Facebook) vengono solitamente mostrati in automatico dal sistema della piattaforma ai profili con i quali sono stati stretti dei collegamenti o che più semplicemente lo "seguono", permettendo, quindi, una forma di comunicazione con un numero indeterminato di destinatari[91].

Automating power: Social bot interference in global politics, cit.; M.T. Bastos – D. Mercea, *The Brexit botnet and user-generated hyper-partisan news*, in *Social Science Computer Review*, 37(1), 2019, 38 ss.; J.C.M. Serrano – M. Shahrezaye – O. Papakyriakopoulos – S. Hegelich, *The Rise of Germany's AfD: A Social Media Analysis*, in *Proceedings of the 10th International Conference on Social Media and Society*, 2019, 214 ss.; F. Giglietto – N. Righetti – G. Marino, *Understanding coordinated and inauthentic link sharing behavior on Facebook in the run-up to 2018 general election and 2019 European election in Italy*, cit. La considerazione della pericolosità dell'impiego di questi agenti *software* per incrementare artificiosamente la popolarità di contenuti *online* è stata esposta anche dal deputato James Lawless nel corso di un dibattito contestuale alla presentazione della *OASM Bill*, avvenuto il 6 dicembre 2017. La trascrizione del dibattito è disponibile in *Dáil Éireann debate*, cit.

88 Si veda al riguardo quanto esposto in A. Tedeschi Toschi – G. Berni Ferretti, *Il contrasto legislativo ai socialbot e le soluzioni avanzate negli Stati Uniti d'America a livello federale e statale*, cit., spec. 472-478.

89 Si veda in merito a questo tipo di interazioni compiute da un *bot* il recente caso esposto in T. Rasmussen, *There was a tinder election bot fanning the fire of the youth vote*, in *i-d.vice.com*, 15 giugno 2017, in cui è stato riportato che un *bot* venne usato per spingere gli utenti dell'applicazione di incontri Tinder a registrarsi per poter votare alle elezioni per il rinnovo della Camera dei Comuni del Regno Unito del 2017. Stime approssimative riportarono che il Tinder Election Bot abbia inviato tra i 30.000 ed i 40.000 messaggi a persone di età compresa tra i 18 ed i 25 anni. Durante questa votazione si assistette alla più alta percentuale di voti espressi dai giovani durante le elezioni in Inghilterra dal 1992: il 66,4% degli elettori della fascia d'età considerata (non vi fu, però, modo di individuare alcun tipo di correlazione tra l'uso di questo *bot* per scambiare messaggi con gli utenti dell'applicazione e il numero di elettori giovani presentatisi ai seggi).

90 In merito alle critiche circa la vaghezza della terminologia impiegata nella normativa californiana si vedano R. Diresta, *A New Law Makes Bots Identify Themselves–That's the Problem*, in *wired.com*, 24 luglio 2019; J. Horder, *Online Free Speech and the Suppression of False Political Claims*, cit., 15-16.

91 A favore di questo orientamento interpretativo di inclusione della maggior parte delle condotte

L'interpretazione della norma rischia, invece, di risultare più complessa per quanto riguarda l'inquadramento dell'apposizione delle cosiddette "reazioni" ai contenuti pubblicati da altri (ad esempio i «Mi piace» di Facebook, gli «*Upvote*» di Reddit, o i «Consiglia» di LinkedIn). Riguardo a queste forme di azione nei confronti dei contenuti pubblicati da altri profili, è opinione di chi scrive che esse debbano rientrare nel novero delle comunicazioni rilevanti per la normativa in oggetto, dato che con esse si è in grado di comunicare (in forma più o meno ampia, a seconda della strutturazione della piattaforma su cui esse vengono impiegate) un'opinione riguardo a quanto detto e a farla sapere non solo al suo creatore ma anche alla platea di persone che abbia modo di visionarla, soprattutto perché – come già detto riguardo ai contenuti pubblicati all'interno dello "spazio personale" *online* di un profilo *social* – i sistemi dei *social media* solitamente mostrano ai profili di terzi che sono ad essi collegati o che li seguono i contenuti pubblicati od oggetto di "reazioni"[92].

(ii.) Contenuti che promuovono un candidato o un partito – Ulteriore nodo venutosi a creare con la strutturazione della proposta di legge irlandese nei suoi termini attuali riguarda la definizione di quali contenuti possano essere ritenuti di promozione per un candidato, un partito o un'opinione su di una questione di interesse o importanza politica tramite la loro diffusione in rete potenziata dai *web bot*.

Innanzitutto, è importante evidenziare come la normativa sia strutturata in modo da sanzionare come illecito la mera comunicazione di contenuti promuoventi soggetti, organizzazioni politiche registrate od opinioni, senza che abbia rilevanza l'effettiva realizzazione di una qualche forma di ascendenza sui destinatari. Di conseguenza, nemmeno le forme più puerili di supporto ad un certo candidato o ad un certo partito politico possono dirsi estranee all'ambito di applicazione della *OASM Bill*, in quanto, a prescindere dalla loro reale efficacia, se messe in atto da un profilo gestito da un *bot*, esse integrano una violazione delle sue disposizioni, dato che suggeriscono comunque l'espressione di una determinata preferenza. Siamo, quindi, anche in questo caso[93], di fronte ad un'antigiuridicità integrata tramite una mera condotta e non a seguito della realizzazione di un evento dannoso.

La decisione di considerare alla Sezione 6 della proposta di legge irlandese un reato il semplice mantenimento di un comportamento anziché la realizzazione di un evento dannoso può avere una duplice motivazione. La prima ragione che pare trasparire dalla lettera della normativa è la scarsa chiarezza circa il bene giuridico da tutelare imponendo delle limitazioni all'uso di *internet bot* per la diffusione di contenuti *online*. Infatti,

attuabili su Internet nel concetto di "comunicare" vi è anche B. Stricke, *People v. Robots: A Roadmap for Enforcing California's New Online Bot Disclosure Act*, in *Vanderbilt Journal of Entertainment & Technology Law*, 22, 2020, 838 ss., in cui l'autore opera un'approfondita disamina del testo della riforma legislativa approvata nello Stato della California (che ha diversi punti di contatto con quella qui analizzata) e, riferendosi ai precedenti giurisprudenziali *Mirkin v. Wasserman*, 858 P.2d 568, 578 (Cal. 1993) e *Comm. on Children's Television, Inc. v. Gen. Foods Corp.*, 673 P.2d 660, 674 (Cal. 1983), ha evidenziato come questo genere di pubblicazione di contenuti ben possa qualificarsi come una "comunicazione indiretta" e, quindi, violare le disposizioni del Paragrafo 17941 (a) del *California Business and Professions Code*.

[92] Questa posizione è sostenuta anche in B. Stricke, *People v. Robots: A Roadmap for Enforcing California's New Online Bot Disclosure Act*, cit., 853.

[93] Si veda quanto riferito *supra* al paragrafo 2.1.(C) di questo articolo in merito alle condizioni per la violazione della Sezione 8 (1) del *POFMA* di Singapore.

mentre dal *POFMA* trapela chiaramente la preoccupazione del legislatore singaporiano di proteggere beni giuridici di primaria importanza per lo Stato, quali l'ordine pubblico, la sicurezza e la salute dei suoi cittadini e il corretto svolgimento delle elezioni[94], le indicazioni della *OASM Bill* risultano alquanto laconiche nel definire l'obiettivo della norma (il fine indicato nel preambolo è, infatti, semplicemente di «garantire la trasparenza nella divulgazione delle informazioni nella pubblicità politica online; e per provvedere a questioni correlate»). Sembra, comunque, possibile immaginare che il proposito del legislatore irlandese sia quello di tutelare la libera formazione delle opinioni politiche dei suoi cittadini, evitando che le loro cerchie virtuali di connessioni vengano infiltrate in maniera dissimulata da agenti *software* e sottoposte ad un'intensa opera di diffusione di contenuti secondo modalità per le quali vengano percepiti dagli utenti umani come espressione di un genuino e condivisibile sentimento popolare[95].
La seconda delle ragioni intuibili dal senso della proposta di legge – conseguente alla prima – è la difficoltà quasi insormontabile di provare l'effettiva realizzazione di un evento dannoso, quale il compimento di un'indebita influenza sui convincimenti dei destinatari delle comunicazioni di «un messaggio che promuove uno o più candidati […] o un partito politico registrato nel registro dei partiti politici, o se promuove un messaggio su una questione di interesse o importanza politica»[96], tramite strumenti di falsificazione della reale rinomanza di un contenuto (quali sono gli *internet bot*). Soprattutto, è quasi insuperabile la problematicità di dimostrare che sia stata sufficiente questa forma di manipolazione della celebrità di un'opinione a convincerli della validità di quei candidati, partiti od opinioni[97].
Nonostante, come appena visto, non sia rilevante ai fini dell'attribuzione del carattere delittuoso delle condotte la realizzazione di un evento dannoso, permane il problema di definire quando i contenuti del messaggio comunicato possano dirsi di promozione di candidati, partiti od opinioni. Infatti, se, come detto, anche le forme più puerili di invito all'espressione di una determinata preferenza elettorale sono considerate come forme di promozione che il combinato disposto delle Sezioni 2 e 6 sanziona come illecite, riportare acriticamente solo alcuni dei caratteri, delle affermazioni o degli episodi della vita di un candidato o di un partito o solo alcuni punti del loro programma elettorale risulta già una condotta non immediatamente inquadrabile come esaltatoria o meno. Questo perché un'indicazione parziale di caratteri, azioni o parole di un personaggio politico (o dei membri di un partito), anche quando veritiera e non celebrativa, ben può essere in concreto idonea a fornire al destinatario di una comunicazione *online*

[94] Si veda la Sezione 7 (1)(b), da (i) a (vi), del *POFMA*, analizzata *supra* al paragrafo 2.1.(D) di questo articolo.

[95] Si vedano al riguardo i contributi riportati *supra* alle note 17 e 54.

[96] Sezione 2 (2) della *OASM Bill*.

[97] Nonostante siano stati condotti numerosi studi in merito al fatto che le persone tendono a prestare attenzione a ciò che sembra popolare e a fidarsi delle informazioni che circolano all'interno del loro contesto sociale e l'importante ruolo giocato dalle cerchie virtuali di connessioni nella formazione delle convinzioni personali e delle opinioni politiche, sembra difficile che citare dette ricerche sarebbe sufficiente a provare in sede giurisdizionale la sussistenza di un nesso di causalità tra l'accrescimento artefatto della diffusione di determinati contenuti e l'espressione da parte dei destinatari di dette opere propagandistiche dell'opinione da essi veicolata. Per gli studi condotti in quest'ambito, si veda quanto riportato *supra* alle note 16, 17, 18, 54 e 87.

una rappresentazione distorta del loro valore in un senso per questi favorevole e finire, così, col suscitare o rafforzare in colui che riceve il messaggio il convincimento ad esprimere una preferenza in ambito elettorale che altrimenti non avrebbe compiuto. In altre parole, un resoconto veritiero ed obiettivo ma parziale delle qualità di un candidato o di un partito ben potrebbe essere considerato come una forma di supporto che, ai sensi della *OASM Bill*, non può essere compiuta attraverso l'utilizzo di un *bot*.

Sebbene un'interpretazione della normativa in oggetto in termini così restrittivi possa apparire eccessiva, è necessario prendere in considerazione che questi agenti *software* vengono anche impiegati in gruppi coordinati e composti da un alto numero di unità per la diffusione su ampia scala di contenuti che seppelliscano opinioni ed interpretazioni diverse da quelle dei loro "padroni". Questa attività, definita *astroturfing*[98], può facilmente essere compiuta anche in ambito elettorale per nascondere i contenuti negativi verso un candidato o un partito dietro una quantità esorbitante di altri che riportano – anche in modo veritiero e spassionato – solo aspetti di questi visti come positivi dalla collettività a cui appartengono, impedendo, così, ai loro elettori di compiere delle ricerche complete su di loro e riuscendo, di fatto, a supportarli.

Inoltre, il nodo relativo alla determinazione di quali messaggi abbiano una connotazione promozionale di candidati, partiti od opinioni interessa anche l'apposizione di "reazioni" ai contenuti di terzi tramite un *bot*. Infatti, data l'interpretazione estensiva sopra esposta al sottoparagrafo 2.2.(B)(I) di questo articolo di quali azioni *online* – e in particolare sui *social media* – possano essere considerate modalità di comunicazione di un messaggio, far cliccare ad un *socialbot*, ad esempio, il tasto «Mi piace» sotto ad un *post* su Facebook o quello «Consiglia» su LinkedIn risulta pacificamente integrante una violazione del combinato disposto delle Sezioni 2 (2) e 6 (1) della *OASM Bill*. Questo perché azioni di questo tipo sono in grado di trasmettere al creatore di un *post* e a coloro che possono visionarlo un giudizio di merito sul suo contenuto e, quindi, eventualmente anche di supportare le persone o le opinioni politiche che sono menzionati in esso[99]. L'importanza di questa considerazione deriva anche dal fatto che un alto numero di "reazioni" ad un determinato contenuto e, quindi, ai soggetti o alle opinioni in esso descritti, potrebbe rendere una falsa impressione di popolarità di esso e dei suoi soggetti e indurre delle persone a prestargli attenzione o a ritenerlo attendibile come non avrebbero fatto in assenza della sua celebrità artificiale[100].

---

[98] J. Ratkiewicz – M. Conover – M. Meiss – B. Gonçalves – A. Flammini – F. Menczer, *Detecting and tracking political abuse in social media*, cit.; Ratkiewicz – M. Conover – M. Meiss – B. Gonçalves – S. Patil – A. Flammini – F. Menczer, *Truthy: Mapping the spread of astroturf in microblog streams*, cit.; J. Zhang – D. Carpenter – M. Ko, *Online astroturfing: A theoretical perspective*, in *Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, August 15-17, 2013*, 2013, 1 ss.; N. Abokhodair – D. Yoo – D.W. Mcdonald, *Dissecting a Social Botnet: Growth, Content and Influence in Twitter*, cit.; S.C. Woolley, *Automating power: Social bot interference in global politics*, cit.; M. Kovic – A. Rauchfleisch – M. Sele – C. Caspar, *Digital astroturfing in politics: Definition, typology, and countermeasures*, in *Studies in Communication Sciences*, 18(1), 2018, 69 ss.; E. Dubois – F. McKelvey, *Political Bots: Disrupting Canada's Democracy*, in *Canadian Journal of Communication*, 44(2), 2019, 27 ss.; F.B. Keller – D. Schoch – S. Stier – J. Yang, *Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign*, in *Political Communication*, 37(2), 2020, 256 ss.

[99] Questa interpretazione è avanzata anche in B. Stricke, *People v. Robots: A Roadmap for Enforcing California's New Online Bot Disclosure Act*, cit., 853, dove l'autore definisce le reazioni ai contenuti di terzi come "funzioni di sostegno" (in originale "*Endorsement features*").

[100] In merito alla tendenza delle persone a prestare attenzione a ciò che sembra popolare e a fidarsi delle

Rimane da ultimo da notare come la Sezione 2 (2), nel definire le finalità politiche che vengono vietate dalla Sezione 6 nell'impiego dei *bot*, parli solo di promozione di soggetti, organizzazioni ed opinioni politici, tralasciando l'ipotesi che detti agenti *software* vengano, invece, utilizzati per avversarli. Sebbene sia facile immaginare che un tale sfruttamento di questi strumenti digitali autonomi possa rientrare nell'ambito delle condotte vietate dalle norme di tutela della reputazione di persone od organizzazioni, di fatto colmando quella che a prima vista appare come una notevole lacuna, la *OASM Bill* rischia, comunque, di sembrare priva della necessaria considerazione per la diffusione potenziata *online* di due particolari tipologie di contenuti: quelli che riportano solo fatti veri ma considerati riprovevoli dalla collettività o dalla legge e quelli che non promuovono un messaggio su una questione di interesse o importanza politica ma che si limitano, invece, a criticare quelli espressi da altri.

In merito alla prima tipologia di contenuti pare possibile riportare le medesime considerazioni esposte *supra* in merito alla presentazione di solo alcune caratteristiche o qualità di un candidato o di un partito politici, ossia che, pur essendo veritiera, una descrizione parziale è comunque capace di riportare una rappresentazione distorta del suo oggetto. Sebbene tale tipologia di condotta non possa ovviamente essere definita come illecita, data la continenza formale dei messaggi comunicati, essa può avere, comunque, degli effetti nefasti sull'andamento del dibattito pubblico. Infatti, come visto, gli *internet bot* possono essere impiegati anche in attività di *astroturfing* che, in questo caso, sarebbero finalizzate a seppellire i contenuti riguardanti aspetti positivi sotto una soverchiante quantità di altri che riportano solo i caratteri socialmente riprovevoli di candidati o partiti politici esecrati dai "padroni" di questi agenti *software*, finendo, così, con lo sviare artificiosamente le convinzioni personali e le opinioni politiche degli elettori dal loro naturale percorso di formazione.

Per quanto riguarda, invece, la propagazione tramite *web bot* di contenuti contrari ai messaggi espressi da altri in merito a una «questione di interesse o importanza politica», pare qui possibile argomentare che qualsiasi critica – che non scada nell'ingiuria o nella diffamazione – alle opinioni espresse da altri in merito ad una questione sia comunque una forma implicita di promozione della tesi opposta e ricada, quindi, nell'ambito del divieto sancito dalla Sezione 6 della proposta di legge introdotta al Dáil Éireann. Tuttavia, permane una certa ambiguità riguardo alla possibilità di includere queste particolari condotte.

(iii.) Questioni di interesse o di importanza politica – Oltre ai dubbi interpretativi visti in merito al concetto di comunicazione di un contenuto e della determinazione del suo carattere promozionale o meno, la scarna definizione del reato di utilizzo di un *bot* con finalità politiche lascia anche un fosco alone di incertezza in merito a cosa rientri nel concetto di «questione di interesse o importanza politica». Questo anche perché oggi addirittura argomenti come l'uso di materiale medico-sanitario[101] o di cannucce

informazioni che circolano all'interno delle loro cerchie virtuali di connessioni si veda quanto riportato *supra* alle note 16, 17, 18, 54 e 87.

[101] Si vedano, ad esempio, L.H. Kahane, *Politicizing the Mask: Political, Economic and Demographic Factors Affecting Mask Wearing Behavior in the USA*, in *Eastern Economic Journal*, 47(2), 2021, 163 ss.; L. Aratani, *How did face masks become a political issue in America?,* in *theguardian-com*, 29 giugno 2020.

di plastica[102] possono assumere connotazioni violentemente politiche. Soprattutto di fronte alle successive previsioni contenute nella Sezione 2 (2) di quali altri argomenti non possano essere oggetto di promozione tramite l'uso di un *bot* camuffato da essere umano, ossia quelli oggetto di un dibattito parlamentare, di una proposta di legge o di un referendum (quindi, in qualche modo identificabili facendo riferimento a precisi indicatori esterni, come il calendario dei lavori parlamentari), appare ancora più arduo identificare i confini dell'ambito di applicazione di questa indicazione di stampo sostanzialmente residuale, rendendo, così, facilmente plausibile che ai sensi della Sezione 6 (1) nessun argomento possa essere oggetto di contenuti diffusi in forma potenziata dall'impiego di programmi *software* automatizzati[103].

Deve, poi, essere evidenziato come la Sezione 6 (1) della *OASM Bill* vieti di usare i *bot* con l'obiettivo «di presentarsi come un *account* o un profilo individuale», ossia che essa definisca come illecito l'impiego di agenti *software* per gestire «più *account* falsi mascherati da entità individuali»[104]. In altre parole, è la direzione compiuta da dietro le quinte e tramite l'utilizzo di un *bot* di almeno 25 profili, creati in modo da sembrare appartenere ad altrettante persone vere, perché questi supportino un candidato, un politico o un'opinione su di un tema politico (facendoli apparire più popolari di quanto non siano in realtà tra la gente) ad essere decretata come un crimine. Di conseguenza, pare ammissibile – o quantomeno non immediatamente riconoscibile come vietato – un utilizzo "in chiaro" di questi programmi *software* autonomi, ossia il loro impiego non dissimulato per la realizzazione di «più presenze *online*». Questa ipotesi, invero qui non apertamente contemplata, è invece espressamente prevista al Paragrafo 17941 (a) del *Bolstering Online Transparency Act of 2018* della California (con cui la *OASM Bill* ha diversi punti di contatto) e avrebbe i suoi meriti per quanto riguarda le necessità di buon funzionamento del Potere giurisdizionale. Allo stesso tempo, però, lascerebbe aperta – forse anche ingigantendola – la problematica relativa all'apposizione di "reazioni" ai contenuti di terzi. Infatti, mentre un messaggio pubblicato su Internet da un profilo chiaramente marcato come gestito da un *bot* renderebbe consci i suoi lettori della natura artificiale del suo comunicatore e gli permetterebbe di soppesare con maggior precisione e consapevolezza il suo valore, nell'apposizione di reazioni ai contenuti di terzi, l'identità robotica di coloro che hanno compiuto quest'azione si perde nella moltitudine degli identificativi sommariamente riportati tramite un semplice numero, finendo di fatto col perpetrare quell'indebita influenza sulla formazione delle convinzioni personali di coloro ai quali detti contenuti vengono mostrati[105].

---

[102] Si vedano, ad esempio, E. Bradner, *Plastic straws are the subject of the latest 2020 culture war*, in *edition.cnn.com*, 5 settembre 2019; L. O'Neil, *How plastic straws became the latest battleground in the US culture wars*, in *theguardian.com*, 3 agosto 2018.

[103] La vaghezza di questa disposizione è stata messa in evidenza anche nel corso dei dibattiti parlamentari che hanno riguardato la sua approvazione. Si veda, ad esempio, l'intervento compiuto dal parlamentare Brian Stanley nel corso del dibattito del 13 dicembre 2017, disponibile in *Dáil Éireann debate*, cit., durante il quale egli ha espressamente chiesto ai suoi colleghi con fare retorico «cosa costituisce una "questione di interesse politico"?».

[104] Intervento del deputato Lawless durante la presentazione della *OASM Bill* del 06 dicembre 2017.

[105] In merito alla tendenza delle persone a prestare attenzione a ciò che sembra popolare si veda quanto riportato *supra* alle note 15 e 16.

Infine, per quanto la proposta di legge avanzata dal deputato Lawless davanti al Dáil Éireann abbia il merito di aver riconosciuto la necessità ormai impellente di un intervento di regolamentazione di un aspetto nuovo della realtà sociale o politica per poter meglio tutelare i cittadini da indebite influenze – perpetrate attraverso delle vere e proprie frodi in merito ad aspetti ritenuti, anche inconsciamente, come degni di attenzione – sul processo di formazione delle loro opinioni ed orientamenti politici, essa non è esente da difetti, sia in merito alle definizioni proposte che riguardo all'identificazione delle condotte da bollare come criminose. Per di più, l'assenza di qualsiasi potere di adottare dei provvedimenti di restrizione dell'uso degli *account* gestiti da un *internet bot* che abbia violato le disposizioni della legge stessa (come, invece, previsto dalla normativa della Repubblica di Singapore)[106] sembra mettere in luce una scarsa comprensione da parte del legislatore irlandese della capacità di questi agenti *software* di portare avanti la propria opera di propaganda e disinformazione rimanendo al di fuori della giurisdizione delle Autorità deputate a far rispettare la legge dello Stato[107].

3. Conclusioni

l'avvento di Internet e dei *social media* ha permesso uno scambio di contenuti con dei volumi ed una velocità in precedenza impensabili, portando ad un progresso della conoscenza e ad un allargamento dei dibattiti che non sarebbero stati altrimenti possibili negli stessi termini. Tuttavia, le architetture alla base di questo sistema di libero scambio di idee hanno tralasciato alcuni aspetti di sicurezza ed affidabilità che oggi costituiscono delle vere e proprie falle di sistema che permettono a chiunque (umano e non) di mostrarsi con le caratteristiche che più gli aggradano e permettendo, così, di non far trasparire su Internet la propria effettiva natura e di distorcere la realtà dei fatti tramite strumenti relativamente semplici da usare, quali i *socialbot*.

Lo sfruttamento delle fragilità delle piattaforme *social* per la malevola diffusione di contenuti propagandistici e disinformativi è ormai giunto ad un livello tale da essere identificato come uno dei «rischi sistemici» per la tenuta delle istituzioni democratiche di un paese[108]. Di fronte a questi pericoli, alcune nazioni hanno deciso di adottare delle normative che – agli occhi dei loro legislatori – dovrebbero formare un solido bastione di difesa della stabilità dei loro ordinamenti e della fiducia dei loro cittadini.

La Repubblica di Singapore ha voluto rispondere con fermezza a questi nuovi fenomeni approvando una legge che è stata fortemente criticata per la durezza delle soluzioni adottate e per la facilità con cui essa potrebbe essere trasformata da strumento di tutela

[106] Si veda quanto scritto *supra* al paragrafo 2.1.(E) di questo articolo in merito alla Sezione 40 del *POFMA*.

[107] Come già perspicacemente rilevato anche dal deputato Seán Kyne nel corso del dibattito del 13 dicembre 2017, il quale ha dichiarato che «l'idea che possiamo rintracciare i *bot* e perseguire le persone o le organizzazioni dietro di loro ignora la realtà che se la persona che gestisce i falsi *account* ha sede fuori dallo Stato, come la maggior parte di loro, allora sarà al di là della portata del disegno di legge».

[108] Si veda quanto riportato al considerando 57 della COM(2020) 825 final, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali)*, detto anche *Digital Service Act*.

dell'opinione pubblica a mezzo di repressione del dissenso (in particolare per via del fatto che ha tra i propri capisaldi una valutazione del contenuto delle opinioni espresse dalle persone)[109]. Inoltre, la normativa dell'isola-stato del sud-est asiatico presenta numerose criticità nella definizione del proprio oggetto di regolamentazione e delle condotte sanzionabili. Tuttavia, tutti questi fattori non possono mettere in secondo piano come il *POFMA* contenga anche delle previsioni interessanti per quanto riguarda il contrasto ai *socialbot*.

La Repubblica d'Irlanda sta cercando a sua volta di arginare un fenomeno a cui ha potuto assistere da vicino e che viene visto dai suoi legislatori come una minaccia per il suo ordinamento. Nel tentativo di edificare una propria difesa legislativa, l'Isola di Smeraldo ha tratto evidente ispirazione dalla normativa statale della California statunitense, cercando, però, anche di superare le problematiche in essa contenute[110]. Al momento, come visto, la proposta di legge in discussione al Dáil Éireann non è priva di criticità – sia per quanto riguarda le definizioni date che in merito alle condotte da vietare – ed ha già subito una battuta d'arresto[111]. Ad ogni modo, essa attualmente non è stata abbandonata e non è nemmeno arrivata alla camera alta del Parlamento irlandese. Rimane, quindi, ancora possibile che venga modificata in futuro in termini più appropriati al suo scopo e poi approvata.

L'analisi qui compiuta delle normative delle due repubbliche (che condividono un modello di ordinamento giuridico di *common law* di origine britannica) ha permesso – almeno agli occhi di chi scrive – di porre in evidenza alcune problematiche relative alla regolamentazione delle nuove tecnologie digitali e dei fenomeni ad esse collegate.

Innanzitutto, il fatto che una produzione legislativa relativa a innovazioni recenti e con profondi riflessi sulla società civile debba per forza appoggiarsi alle esperienze e alle competenze di soggetti che abbiano una piena e profondissima comprensione delle questioni considerate. In caso contrario, il rischio di adottare riforme inefficaci o addirittura controproducenti è estremamente alto.

In secondo luogo – e in diretta conseguenza della considerazione appena esposta – la comparazione qui svolta ha fatto emergere come delle leggi nazionali possano facilmente risultare inadatte ad impedire o anche solo arginare delle condotte nefaste che possono essere compiute al di fuori dei loro ambiti territoriali di applicazione[112]. L'insegnamento che pare potersi trarre da questa comparazione è, quindi, che sia necessario pensare ad una soluzione di regolazione sovranazionale che permetta di superare i limiti degli interventi dei singoli Stati (in questa direzione la Commissione europea ha già mosso i primi passi tramite la promozione dello *Strengthened Code of Practice on*

[109] Si veda al riguardo quanto riportato *supra* al paragrafo 2.1. di questo articolo e, in particolare, alle note 26, 27, 28 e 29.

[110] Per un'analisi delle problematiche della normativa di contrasto ai *socialbot* della California statunitense, si veda A. Tedeschi Toschi – G. Berni Ferretti, *Il contrasto legislativo ai socialbot e le soluzioni avanzate negli Stati Uniti d'America a livello federale e statale*, cit.

[111] Si veda in merito M. O'Halloran, *Government defeated on online advertising and social media Bill*, in *irishtimes.com*, 14 dicembre 2017. Successivamente al voto contrario della Camera bassa, la proposta di legge è tornata alla commissione parlamentare dove dal 31 marzo 2021 è ancora in fase di modifica.

[112] Si vedano a questo proposito le perplessità esposte dal deputato irlandese Seán Kyne e riportate *supra* alla nota 103.

Disinformation 2022, un codice di autoregolamentazione per i *Social Network Providers*)[113]. In ultima analisi, le normative qui considerate sono tutto fuorché adeguate, sia a causa delle loro criticità strutturali sia perché cercano di regolare in forma locale un fenomeno transnazionale che esula dagli ambiti di esercizio della sovranità dei singoli Stati, ma costituiscono comunque un primo tentativo da parte dei legislatori nazionali di garantire una maggior tutela alla libera formazione delle opinioni dei loro cittadini.

[113] La stessa Commissione europea, però, aveva riconosciuto come la prima versione di questo codice di autoregolamentazione avesse delle criticità significative, tra le quali un'applicazione incoerente e incompleta della sua disciplina tra le diverse piattaforme e gli Stati membri, delle limitazioni intrinseche alla sua natura di strumento di autoregolamentazione e diverse lacune (SWD(2020) 180 final, *Assessment of the Code of Practice on Disinformation–Achievements and areas for further improvement*).

Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale*

Agostino Sola

Abstract

Le economie data driven hanno mostrato un ruolo assolutamente nuovo dei dati, tanto nella creazione delle relazioni economiche quanto nel determinare la forza economica di un'impresa. Questa nuova consapevolezza sta portando all'applicazione di regole specifiche, anche nuove, incentrate sul rapporto tra innovazione e diritto. Nel diritto amministrativo, le economie *data driven* stanno sollevando alcuni interrogativi su quale norma debba essere applicata e da quale autorità: è nota, ad esempio, la correlazione emergente e inaspettata tra diversi ambiti del diritto (privacy, antitrust, cybersicurezza, proprietà intellettuale, per citarne alcune). Le economie *data driven* stanno determinando un'inedita combinazione di poteri e competenze amministrative, individuandone anche di nuove, come è la cybersicurezza. In questo senso, si descrive l'evoluzione del contesto normativo che ha portato alla creazione di un organismo amministrativo assolutamente nuovo al fine di tutelare questo nuovo emergente interesse pubblico per la cybersicurezza: l'Agenzia per la Cybersicurezza Nazionale (ACN).

It is a fact that data driven economies have shown a new role of data in the creation of economic relationships and in determining the economic strength of a company. This new awareness of economic value is leading to the application of specific rules, even new ones, focusing on the relationship between innovation and law. From an administrative perspective, data driven economies are raising some questions about which rule should be applied and by which authority: it is known, for example, the emerging and unexpected correlation between different fields of law: privacy and antitrust but also data retention and cybersicurezza. This phenomenon is representing not only a national but already an European concern. In Italy, following this path, could be observed the growing interest in cybersicurezza that has led to the creation of a new administrative body to protect this newly emerged public interest in cybersicurezza: the Agency for National Cybersicurezza.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Sommario

1. Introduzione. L'attuale indiscussa centralità dei dati e le economie dei dati. - 2. - Il nuovo ruolo della cybersicurezza nelle società digitali. - 3. La cybersicurezza: evoluzione normativa europea. - 4. - (segue): panorama normativo nazionale. - 5. - Profili amministrativi di cybersicurezza. La creazione di nuove autorità *ad hoc* e la nuova architettura istituzionale di riferimento. - 6. - Conclusioni. Il prisma di Newton nella regolazione dei dati, l'esempio della cybersicurezza.

Keywords

economia dei dati – cybersicurezza – competenze amministrative - Agenzia per la Cybersicurezza Nazionale

1. Introduzione. L'attuale indiscussa centralità dei dati e le economie dei dati

L'attuale contesto socioeconomico è ormai caratterizzato dall'intervenuta creazione e dal crescente sviluppo di sistemi decisionali, pubblici e privati, basati sull'analisi dei dati, che hanno portato alla definizione della nostra epoca quale oggetto della cd. quarta rivoluzione industriale[1]. Tale rivoluzione si riferisce, in particolar modo, alla circostanza in base alla quale tutti gli ambiti della vita sociale ed economica sono influenzati, direttamente o indirettamente, dalle nuove tecnologie digitali che, con l'avvento e la diffusione di Internet, hanno determinato nuove modalità di comunicazione ed elaborazione dei dati ed una costante interconnessione della popolazione.

Dall'attuale disponibilità di dati[2] e dalle capacità tecnologiche[3] acquisite negli ultimi anni si sono sviluppate le economie dei dati le quali si caratterizzano, in via di prima approssimazione, per l'utilizzo, *recte* lo sfruttamento, di dati, personali e non, all'interno di processi decisionali, tanto pubblici quanto privati, con la finalità di contribuire all'efficienza e alla qualità dei processi produttivi tradizionali ovvero di qualificare in termini di innovazione (anche intesa come personalizzazione) l'offerta di beni e ser-

[1] Secondo K. Schwab – P. Pyka, *Die Vierte Industrielle Revolution*, München, 2016, richiamato da A. Lalli, Il sapere e la professionalità dell'amministrazione pubblica nell'era dei big data e dell'intelligenza artificiale, in *aipda.it*, relazione al Convegno AIPDA 2019.

[2] Il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025 (Report IDC 2018, richiamato nella Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni, *Una strategia europea per i dati*, COM(2020) 66 final, 12 febbraio 2020, 2). Occorre osservare anche che i dati e le informazioni crescono ad una velocità vertiginosa tale da creare un ambiente saturo di dati, in tal senso D.U. Galetta, *La pubblica amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?,* in *Ciberspazio e diritto,* 3, 2018, 327, riporta alcuni dati in tema di aumento del volume delle informazioni disponibili.

[3] Senza adeguata tecnologia, infatti, l'acquisizione di grandi quantità di dati – inintelligibili alla conoscenza umana - rimarrebbe fine a se stessa e priva di qualsiasi utilità pratica e, quindi, di rilevanza economica. La rilevanza dei *big data* è comunque tale da aver portato alla creazione di modelli di business concentrati unicamente nella raccolta e nell'analisi degli stessi.

vizi, digitali e non.[4]

I dati, dunque, al pari delle tecniche algoritmiche di analisi[5], rappresentano ormai un fattore di produzione[6] ed una risorsa economica di fondamentale importanza nell'organizzazione delle attività di produzione e di scambio[7].

L'accennato fenomeno, che ha preso il nome di data driven innovation, non ha interessato soltanto i tradizionali modelli economici[8] ma ha altresì portato alla nascita di particolari sistemi economici che ruotano attorno all'ecosistema dei big data[9].

2. Il nuovo ruolo della cybersicurezza nelle società digitali

La centralità dei dati, unitamente all'utilizzo di risorse tecnologiche, ha sollevato inedite questioni ordinamentali in risposta alle quali si iniziano ad osservare, anche a livello europeo, primi esempi di politiche di regolamentazione *ex ante* sulla loro circolazione ed utilizzo i cui prodotti normativi assumono ormai una forma definitiva[10].

---

[4] In tema si veda il Rapporto OECD, *Data-Driven Innovation. Big Data for Growth and Well-Being*, in *oecd-ilibrary.org*, 6 ottobre 2015.

[5] Ed infatti, se sono gli algoritmi di calcolo che rendono possibile l'inedito sfruttamento di dati deve osservarsi che la disponibilità di nuovi e aggiornati dati consente, a loro volta, il miglioramento degli algoritmi. Dati e algoritmi, dunque, si manifestano sinergicamente connessi non solo quantitativamente ma anche qualitativamente. Il valore dei dati, infatti, dipende non già dalla loro quantità, bensì dalla loro qualità, intesa quale possibilità di estrarre informazioni utili e rilevanti. La disponibilità di dati, in chiave antitrust, non è affatto idonea a determinare *ex se* una posizione dominante nel mercato di riferimento. Ed è proprio su tale deduzione, unitamente ad altre argomentazioni, che si radica lo scetticismo, se non la contrarietà, della dottrina avverso l'obbligo di garantire l'accesso a terzi concorrenti dei dati detenuti dalle imprese. In tema si veda A. Preta – L. Zoboli, *Profili regolatori e concorrenziali in tema di accesso e condivisione dei dati,* in *Analisi Giuridica dell'Economia,* 1, 2019, 213 ss.

[6] Tale locuzione non è casuale ma intende sottolineare l'impiego dei big data nei processi di produzione di altri beni (informazioni rilevanti da questi estratti) successivamente utilizzati per l'offerta di beni e servizi.

[7] In particolare, pare rilevante l'individuazione di due grandi categorie di imprese *data driven*, tanto nei settori ICT quanto in quelli tradizionali: chi fornisce beni e servizi basandosi sui dati raccolti, sia autonomamente sia mediante *data brokers* (*i*); chi fornisce beni e servizi al fine di generare altri dati al fine di migliorare l'esperienza di consumo e per fornire servizi aggiuntivi (*ii*). In tal senso, P. Hartmann – M. Zaki – N. Feldman – A. Neely, *Big data for big business? A taxonomy of data-driven business models used by start-up firms*, in *cambridgeservicealliance.eng.cam.ac.uk*, marzo 2014.

[8] Si tratta, se si vuole, dell'utilizzo analogico dei dati digitali che si ha laddove il prodotto finale non presenta elementi digitali ma, tramite il perfezionamento delle tradizionali catene di produzione, la produzione viene migliorata in termini qualitativi e quantitativi. In termini analoghi, ad esempio, si discute dell'utilizzo di big data per risolvere l'annoso problema delle perdite della rete idrica nazionale (pari al 42% del volume di acqua immesso nella rete, secondo ISTAT, *Censimento delle acque per uso civile* per l'anno 2018, in *istat.it*, 10 dicembre 2020).

[9] Nonostante non vi sia una definizione univoca di *big data,* si preferisce richiamare la definizione a carattere meramente descrittivo in OECD, *Executive Summary of the Competition Committee Roundtable on Big Data,* in *one.oecd.org*, 26 aprile 2017, secondo cui «*Big Data is commonly understood as the use of large scale computing power and technologically advanced software in order to collect, process and analyse data characterised by a large volume, velocity, variety and value*».

[10] Il riferimento è alle iniziative intraprese dalla Commissione europea ha iniziato il proprio percorso verso un approccio globale all'economia dei dati, riconosciuti quale elemento centrale di tutti i sistemi economici e delle società innovativi e moderni, e quale vera e propria «linfa vitale dello sviluppo

Le economie dei dati e le nuove possibilità offerte dall'evoluzione tecnologica, inoltre, stanno influenzando la quotidianità dei rapporti giuridici[11] e, per quanto d'interesse, anche le modalità con cui operano gli Stati in risposta alla necessità di regolazione di fenomeni inediti. In particolare, la rinnovata esigenza di un intervento pubblico si sta innestando su norme e competenze tradizionali alle quali se ne iniziano ad aggiungere di nuove.

Un aspetto di indubbia novità relativo alla risposta degli Stati a tale necessità è offerto dalla crescente attenzione per i profili inerenti alla cybersicurezza, la cui vulnerabilità è stata resa evidente con la diffusione della digitalizzazione.

La cybersicurezza, infatti, viene invocata al fine di garantire l'affidabilità e la sicurezza di quelle attività[12], pubbliche e private, aventi carattere economico ovvero sociale, che vengono svolte mediante utilizzo di tecnologie digitali e, in generale, nello "spazio cibernetico"[13]. L'erogazione di beni e servizi, infatti, è sempre più mediata da piat-

economico» (così come nella Comunicazione COM(2020) 66, cit.). Va ricordato che sin dal 2014, la Commissione ha intrapreso una serie di iniziative per facilitare lo sviluppo di un'economia agile basata sui dati, quali il regolamento sulla libera circolazione dei dati non personali (regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, GU L 303/59); il regolamento sulla cibersicurezza (regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), GU L 151/15); la direttiva sui dati aperti (direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione), GU L 172/56); il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), GU L 119/1). Nel 2018, ancora, viene presentata per la prima volta una strategia per l'intelligenza artificiale, concordando un piano coordinato con gli Stati membri. La creazione di un contesto normativo di disciplina della risorsa economica dei dati faciliterà altresì l'adozione di primi strumenti di regolazione dell'intelligenza artificiale, basata principalmente sulla capacità di analisi dei dati raccolti e sul punto, allora, pare di interesse ricordare che, nelle sue comunicazioni del 25 aprile 2018 e del 7 dicembre 2018, la Commissione europea ha definito la sua visione a sostegno di un'intelligenza artificiale che sia «etica, sicura e all'avanguardia realizzata in Europa». Ed ancora, in European Group on Ethics in Science and New Technologies, *Statement on Artificia, Robotics and 'Autonomous' Systems*, in *op.europa.eu*, 9 marzo 2018, presentato alla Commissione, sono individuati nove «principi etici e requisiti pre-democratici» che dovrebbero fornire una guida futura per legislatori, regolatori e giudici: dignità umana; autonomia; responsabilità; giustizia, equità e solidarietà; democrazia; *rule of law and accountability*; sicurezza, integrità fisica e mentale; protezione dei dati e privacy; sostenibilità.

[11] Le rivoluzioni scientifiche e tecnologiche contribuiscono a modificare i paradigmi sociali e, quindi, giuridici: portano a trasformazioni anche radicali della società umana e, conseguentemente, del contesto normativo di riferimento. Si pensi, ad esempio, alle questioni di bioetica che il progresso scientifico ha sollevato.

[12] Come osservato da A. Tina, *Cybersicurezza: integrità dei processi e dei dati*, in M. Cian – C. Sandei (a cura di), *Diritto del Fintech*, Padova, 2020, 103, i rischi per le imprese, legati ad un *cyber attack,* possono essere così enucleati: *privacy liability* (1); *network security liability* (violazione rete aziendale) (2); *media liability* (violazione copyright) (3); interruzione di attività – malfunzionamenti (4); data asset loss (5); *cyber extortion* (6); *cyber crime* (7).

[13] In via di prima approssimazione potremmo definire l'oggetto della disciplina relativa alla cybersicurezza come quello "spazio cibernetico" formato dalle infrastrutture informatiche, *hardware* e *software,* interconnesse tra loro e attraverso le quali circolano dati e nelle quali si relazionano utenti. In particolare, nello spazio cibernetico si ricomprende internet, le reti di comunicazioni, i sistemi di

taforme e servizi digitali. Reti e sistemi informativi non coinvolgono solamente le economie digitali ma sono essenziali per il funzionamento anche di molte imprese tradizionali che fondano le proprie strategie di mercato proprio sull'utilizzo di tali servizi digitali.

Da tale interdipendenza deriva la necessità di garantire – tramite idonee misure di cybersicurezza - la sicurezza, la continuità e l'affidabilità delle reti e dei sistemi informativi mediante i quali vengono offerti servizi digitali su cui fanno sempre più affidamento molte imprese.

In termini più generali, come già osservato a livello globale[14], si sta assistendo alla comparsa di nuove minacce alla sicurezza che, in quanto tali, richiedono risposte inedite in grado di salvaguardare la spinta innovativa delle economie data driven.

Tra i profili di rischio legati alla cybersicurezza si devono tenere in considerazione anche i sistemi aggregati di conservazione di dati, necessari per le attuali tecnologie algoritmiche, ed in relazione ai quali continua a trovare applicazione la disciplina europea di protezione dei dati personali.[15]

La necessità di una adeguata risposta alle nuove minacce derivanti dalla diffusione delle tecnologie digitali ha determinato una rinnovata sensibilità per gli aspetti propri della cybersicurezza tanto in relazione al corretto funzionamento dei sistemi informativi quanto in relazione al possibile coinvolgimento di dati personali.

L'erogazione di beni e servizi mediante l'utilizzo di infrastrutture digitali ha manifestato il bisogno che queste siano rese affidabili e sicure a vantaggio tanto degli utenti dei servizi digitali quanto degli operatori coinvolti. L'aumento delle infrastrutture digitali e la crescente accessibilità a strumenti informatici e digitali hanno condotto, nell'ultimo decennio, a sempre più frequenti attacchi cibernetici, dovuti anche alla scarsità (in termini qualitativi e quantitativi) dei mezzi di difesa.[16]

La creazione e il mantenimento di uno spazio digitale capace di offrire adeguate garanzie di sicurezza, infatti, rappresenta una condizione necessaria per fruire pienamente delle possibilità, in parte ancora inesplorate, offerte dal progresso tecnologico. Viceversa, le garanzie di sicurezza consentono altresì di evitare l'esposizione a rischi sistemici rovinosi per lo Stato, ad oggi ancora il principale obiettivo degli attacchi ci-

elaborazione dati e i *dispositivi* attraverso cui si accede alla rete. Ad oggi, la *cybersicurezza* viene definita dalla legislazione europea (regolamento (UE) 2019/881, cit., art. 2, n. 1) quale «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche».

[14] OECD, *Data-Driven Innovation,* cit., 40.

[15] Con particolare riferimento alla Sezione II del regolamento (UE) 2016/679, cit. (GDPR) in tema di misure di sicurezza da adottare qualora siano coinvolti dati personali. E ciò indipendentemente dalla conservazione dei dati per finalità pubblicistiche (*public data retention*), anche a carattere securitario.

[16] In particolare, per una visione d'insieme si deve osservare Presidenza del Consiglio dei Ministri – Sistema di Informazione per la Sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2021*, in *sicurezzanazionale.gov.it*, febbraio 2022. In particolare, viene osservata una tendenza in crescita delle attività ostili per la sicurezza cibernetica: nel corso del 2021, ad esempio, maggiormente colpite sono le infrastrutture informatiche della Pubblica Amministrazione (69%, in diminuzione di 14 punti percentuali rispetto al 2020), perlopiù Amministrazioni Centrali dello Stato (56%, valore in aumento rispetto all'anno precedente) e infrastrutture IT riferibili a enti locali e strutture sanitarie (pari a circa il 30%). In ambito privato, sono stati interessati prevalentemente i settori energetico (24%), dei trasporti (18%) e delle telecomunicazioni (12%).

bernetici.

In termini più generali, dunque, in ragione del crescente utilizzo delle tecnologie informatiche, la cybersicurezza non è più solo limitata a settori strategici per la sicurezza nazionale (difesa militare, infrastrutture essenziali, telecomunicazioni) ma coinvolge l'intero mercato e trova un'applicazione generalizzata a tutte quelle attività economiche e sociali che si svolgono mediante l'utilizzo della rete e dei sistemi informativi. Tratto distintivo della cybersicurezza è che, tutelando il proprio interesse primario, finisce per rappresentare anche distinti ed ulteriori interessi di carattere pubblicistico. Occorre però notare che la cybersicurezza non garantisce solamente il corretto funzionamento delle attività economiche e sociali che si svolgono mediante l'utilizzo della rete e dei sistemi informativi ma rappresenta uno strumento di tutela eterogenea. È chiara, dunque, l'interdisciplinarietà della cybersicurezza che, nel tutelare il proprio interesse primario, finisce per rappresentare anche distinti ed ulteriori interessi di carattere pubblicistico. In particolare, modo, ad esempio, la cybersicurezza, nel garantire l'inviolabilità delle reti, tutela altresì i dati digitali che in queste sono conservati. Dati digitali che, spesso, hanno carattere personale e per i quali si rende necessaria una particolare tutela che tenga altresì in considerazione la specifica normativa sui dati personali. La disciplina di sicurezza delle reti non esclude l'applicazione delle regole poste a protezione dei dati personali che prevedono l'adozione di «misure tecniche e organizzative adeguate» [17] tali da evitarne trattamenti non autorizzati, e, quindi, illeciti. La portata degli obblighi previsti dalla disciplina della protezione dei dati personali, è stato già osservato[18], è in larga parta sovrapponibile alla disciplina sulla cybersicurezza: senza pretesa di esaustività, si consideri che entrambi le discipline prevedono misure di sicurezza "adeguate" alla gestione del rischio e tra queste rientra, ormai, anche la gestione del rischio *cyber*.

Ad oggi, la rinnovata consapevolezza della pericolosità del fenomeno ha oggi portato il legislatore nazionale ed europeo ad ideare una strategia normativa al fine di assicura-

[17] Così prevede l'art. 5, regolamento (UE) 2016/679, cit. in tema di principi applicabili al trattamento dei dati personali, da leggere unitamente all'art. 24 sulla responsabilità del titolare del trattamento dei dati personali.

[18] In particolare, M. Giordano – I. Oldani – M. Simbula, *Principi di sicurezza applicabili ai cloud computing services: GDPR, Direttiva NIS e PSD2 a confronto*, in *Ciberspazio e diritto*, 1, 2020, 123; A. Tina, *Cybersicurezza,* cit., 99 e, sulla complementarità delle due discipline, M. Viggiano, *Cybersicurezza and Data Protection in European Union Policies and Rules: The NIS Directive anche the GDPR Synergy*, in G. De Minico – O. Pollicino (a cura di), *Virtual freedoms terrorism and the law,* Torino, 2020, 63 ss. Ancora, sul rapporto tra *privacy* e cybersicurezza è interessante richiamare una guida dell'autorità inglese per la protezione dei dati personali: ICO, *NIS and the UK GDPR*, in *ico.org.uk*. Lo stesso considerando 63 della direttiva NIS (direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, GU L 194/1) osserva la possibile compromissione di dati personali a seguito di evento con un impatto sulla sicurezza della rete e dei sistemi informativi ragion per cui, poi, nel corpo della Direttiva si delinea, una rete di collaborazione e scambio di informazioni tra autorità e si prevedono «ove opportuno e conformemente al diritto nazionale» (art. 8) consultazioni e collaborazioni tra le autorità competenti e le autorità per la protezione dei dati nazionali. Ad oggi, tale direttiva è stata sostituita per effetto dell'entrata in vigore della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2), GU L 333/80.

re *ex ante* la tenuta cibernetica dei sistemi digitali così da limitare le possibilità di attacco, diversamente dalle prime disposizioni in materia che, complice l'assoluta novità del fenomeno, si concentravano su una «difesa, per ora, di tipo prevalentemente - anche se non esclusivamente - reattivo»[19].

3. La cybersicurezza: evoluzione normativa europea

La centralità dei dati, unitamente all'utilizzo di risorse tecnologiche, ha sollevato inedite questioni ordinamentali in risposta alle quali si osserva, anche a livello europeo, un esempio di regolazione trasversale della materia. In particolare, si osserverà l'evoluzione della disciplina della cybersicurezza.

Il legislatore europeo, nonostante l'attenzione per la sicurezza delle infrastrutture dell'informazione fosse già stata evidenziata sin dai primi anni 2000[20], ha iniziato a tratteggiare una prima architettura regolamentare con la "*Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*" (JOIN(2013) 1 final, 7 febbraio 2013)[21] e la contestuale proposta di direttiva sulla sicurezza delle reti e dell'informazione che vedrà la luce con la nota direttiva 2016/1148/UE (cd. direttiva NIS).

La direttiva NIS definiva un livello comune di intervento europeo a protezione delle infrastrutture critiche anche mediante inediti schemi e modalità di cooperazione internazionale. L'elemento caratterizzante era l'indicazione di una prima base normativa unitaria in un panorama piuttosto eterogeneo e diversificato[22].

---

[19] Presidenza del Consiglio dei ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, in *agid.gov.it*, dicembre 2013, 11.

[20] In particolare, si fa qui riferimento alla Comunicazione della Commissione europea al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica,* COM/2000/0890 def., 26 gennaio 2001. Come ricorda C. Cencetti, *Cybersicurezza: Unione europea e Italia. Prospettive a confronto,* Roma, 2014, nella fase iniziale le politiche europee si sono concentrate sulla sicurezza delle infrastrutture critiche, sulla protezione dei dati personali e sulla repressione dei crimini *cyber*. Si deve menzionare altresì l'istituzione dell'ENISA, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, con regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, GU L 77/1, al fine di «assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione» nonché di «assiste[re] la Commissione e gli Stati membri, e di conseguenza collabora con la comunità degli operatori economici». Il regolamento è stato poi abrogato e sostituito dal regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004, GU L 165/41. Ad oggi, per effetto del regolamento (UE) 2019/881, cit., il ruolo dell'ENISA è ancora più centrale per la promozione di un elevato livello di cybersicurezza e cyber-resilienza.

[21] Per un interessante ed esaustivo commento si rinvia a M. Bassini, *Cybersicurezza*, in M. Paracampo (a cura di), *Fintech*, Vol. I, Torino, 2021, 321 ss.

[22] E ciò con evidente compromissione del livello globale di sicurezza delle reti e dei sistemi informativi in Europa, sino ad allora solo in parte mitigato dalle linee guida ENISA. In questo senso, la direttiva NIS, nell'istituire le misure necessarie alla creazione di «un livello comune elevato di sicurezza delle reti e dei sistemi informativi» compiva un rilevante sforzo definitorio nell'individuare le nozioni comuni di "rete e sistema informativo" e la relativa "sicurezza della rete e dei sistemi informativi", fornendone un primo approccio unitario e ripreso poi dalla direttiva NIS 2, direttiva (UE) 2022/2555, cit.

Ad oggi, tale direttiva è stata sostituita per effetto dell'entrata in vigore della Dir. 2022/2555/UE "relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)".[23] L'obbligo di recepimento della Direttiva NIS 2 (direttiva 2022/2555/UE) viene indicato al 17 ottobre 2024: dal giorno successivo sarà abrogata la direttiva 1016/1148/UE.
In ragione dell'espansione del panorama delle minacce informatiche, si è esteso l'ambito di applicazione della Direttiva NIS 2 che oggi risulta più ampio ed omogeno: da una parte, infatti, si rivolge anche a soggetti pubblici[24]; dall'altra, supera la differenziazione tra gli operatori di servizi essenziali e i fornitori di servizi digitali, propria della precedente direttiva e ritenuta ormai «obsoleta»[25]. Le disposizioni in materia di cybersicurezza trovano applicazione nei confronti di quelle imprese che operano in settori ritenuti critici[26] e i soggetti privati cui la direttiva si riferisce sono suddivisi in

[23] La modifica della disciplina in materia è parte delle azioni indicate nella più ampia strategia digitale europea. In tema, sulla strategia digitale europea, con particolare riferimento alle economie dei dati, sia consentito il rinvio ad A. Sola, *Primi cenni di regolazione europea nell'economia dei dati*, in questa *Rivista,* 3, 2021, 188 ss. La modifica della direttiva NIS è mossa dal dichiarato fine di «rafforzare l'autonomia strategica dell'Unione per migliorarne la resilienza e la risposta collettiva e creare una rete Internet globale e aperta» sulla scorta dell'impatto subìto in termini di adeguatezza ed aderenza all'attuale digitalizzazione ed interconnessione dei servizi chiave all'economia e alla società.

[24] In particolare, agli enti della pubblica amministrazione centrale e regionale (ma, questi ultimi, solo qualora risulti che forniscono «servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche»). Così, l'art. 2, c. 2, lett. f, della direttiva NIS 2, direttiva (UE) 2022/2555, cit. È rimessa alla discrezionalità del legislatore nazionale la scelta di estendere l'ambito di applicazione delle norme in materia anche alle amministrazioni locali ed agli istituti di istruzione. Sono escluse le amministrazioni pubbliche nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati.

[25] In questi termini, al considerando 6 della Direttiva NIS 2, direttiva (UE) 2022/2555, cit. Il precedente impianto normativo offerto dalla direttiva NIS distingueva, ai fini dell'applicazione delle regole ivi contenute, tra "operatori di servizi essenziali" e i "fornitori di servizi digitali", sottoposti a distinti obblighi preventivi in materia di sicurezza e di controlli successivi tramite l'obbligo di notifica degli incidenti. In particolare, ai sensi dell'art. 5, direttiva (UE) 2016/1148, cit., si consideravano "operatori di servizi essenziali" quanti forniscano un servizio «essenziale per il mantenimento di attività sociali e/o economiche fondamentali» (a); la cui fornitura dipende dalla rete e dai sistemi informativi (b); e in caso di incidente si avrebbero «effetti negativi rilevanti sulla fornitura di tale servizio» (c). Erano invece "fornitori di servizi digitali", secondo quanto previsto dall'Allegato III, le imprese che operano nei mercati online (*marketplace*), che forniscono servizi di motori di ricerca online e che offrono servizi di *cloud computing*.

[26] In particolare, secondo l'Allegato II alla Direttiva NIS 2, direttiva (UE) 2022/2555, cit., si riconoscono "settori ad alta criticità", con un'elencazione che amplia quella degli "operatori di servizi essenziali" di cui alla precedente direttiva. In particolare, rientrano in questa categoria le imprese che operano nei settori dell'energia (elettricità, teleriscaldamento e teleraffrescamento, petrolio, gas, idrogeno), del trasporto (aereo, ferroviario, portuale, stradale), bancario, delle infrastrutture dei mercati finanziari, sanitario, della distribuzione dell'acqua potabile, della gestione delle acque reflue, delle infrastrutture digitali, di gestione dei servizi di telecomunicazione (*business-to-business)*, amministrazioni pubbliche e, da ultimo, di fornitura di servizi spaziali. Secondo l'Allegato III alla Direttiva NIS 2, direttiva (UE) 2022/2555, cit., si riconoscono come "altri settori critici" quelle imprese che operano nei settori dei servizi postali e di corriere, della gestione dei rifiuti, industria chimica (fabbricazione, produzione e distribuzione di sostanze chimiche), industria alimentare (produzione, trasformazione e distribuzione di alimenti), fabbricazione di dispositivi medici, fabbricazione di computer e prodotti di elettronica e ottica, fabbricazione di apparecchiature elettriche, fabbricazione di macchinari e apparecchiature n.c.a., fabbricazione di mezzi di trasporto, fornitori di servizi digitali e organizzazione di ricerca.

"essenziali" ed "importanti"[27].

Riprendendo quanto già previsto dalla precedente direttiva, la Direttiva NIS 2 prevede l'obbligo per gli Stati di adottare una "Strategia nazionale per la cibersicurezza", mediante l'adozione di uno o più strumenti legislativi o non legislativi. Tale atto programmatico, al netto dello specifico contenuto delle «misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza» [28], si viene ad arricchire di nuovi contenuti e diventa strumento centrale per garantire l'efficace coordinamento tra le autorità coinvolte, non soltanto a livello internazionale[29] ma anche, e, soprattutto, a livello nazionale.[30]

Gli attori istituzionali coinvolti a livello nazionale si ispirano a quelli già indicati dalla precedente direttiva (e già operativi nei singoli Stati): un'autorità competente responsabile della cibersicurezza e dei compiti di vigilanza che svolge anche le funzioni di

[27] La prima categoria viene puntualmente definita dall'art. 3, c. 1, della Direttiva NIS 2, direttiva (UE) 2022/2555, cit. La seconda, invece, viene definita in negativo come «soggetti di una tipologia elencata negli allegati I o II che non sono considerati soggetti essenziali» (art. 3, c. 3). Così come il precedente quadro normativo, i soggetti privati cui la direttiva si riferisce sono individuati in un elenco tenuto ed aggiornato ad opera dei singoli Stati. Si prevede, tuttavia, l'inedita possibilità per gli stati di indicare le modalità di registrazione autonoma dei soggetti.

[28] L'ambito di riferimento di tali "misure strategiche" viene puntualmente declinato dalla Direttiva NIS 2, direttiva (UE) 2022/2555, cit., laddove, invece, la precedente direttiva NIS, direttiva (UE) 2016/1148, non forniva indicazioni in tal senso e, di fatto, determinava una forte disomogeneità sul territorio europeo in grado di pregiudicare la tenuta del sistema di sicurezza. Tra le varie misure strategiche indicate si segnalano misure di prevenzione ed educazione alla cybersicurezza ed alla cyber-resilienza (*cyber hygiene*). Le strategie nazionali devono essere poi valutate ed aggiornate periodicamente.

[29] Il coordinamento "strategico" a livello internazionale è garantito dall'istituzione di un gruppo di cooperazione (art. 14, direttiva (UE) 2022/2555, cit.), già previsto dalla precedente disciplina, e composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA. Allo scopo di garantire un coordinamento "operativo" rapido ed efficace tra Stati membri viene, invece, istituita una "rete dei CSIRT nazionali" (art. 15, direttiva (UE) 2022/2555, cit.), già prevista dalla precedente disciplina. Al fine di una gestione coordinata degli incidenti sul territorio europeo, viene creata una rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) (art. 16, direttiva (UE) 2022/2555, cit.) formata da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri e, nei casi più gravi, anche dalla Commissione. Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una rete dei CSIRT nazionali.

[30] L'architettura generale del coordinamento in materia risulta analoga alla precedente e si mantiene un sistema capillare di autorità nazionali competenti, punti di contatto unici a livello nazionale e CSIRT, in coordinamento tra loro. Si prevede l'indicazione delle misure di coordinamento specifiche conseguenti alla relazione tra le disposizioni in materia di cybersicurezza e le normative di settore. In particolare, infatti, si prevede che queste ultime trovino applicazione prioritaria solo qualora siano "almeno equivalenti", pur dovendo garantire «la coerenza e l'efficacia del trattamento delle notifiche degli incidenti» tra autorità. Oggetto di richiamo puntuale, tra le normative di settore dell'Unione, è quella relativa ai soggetti finanziari contemplati dal regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (c.d. regolamento DORA) nei cui confronti non trovano applicazione le disposizioni in materia di cybersicurezza. Al contrario, invece, ai soggetti identificati come soggetti critici a norma della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, GU L 333/164, si applicano le disposizioni in materia di cybersicurezza e sono considerati soggetti essenziali (esclusi gli operatori del settore delle infrastrutture digitali).

punto di contatto unico[31]; quadri nazionali di gestione delle crisi informatiche;[32] gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)[33].

Le misure indicate dalla Direttiva NIS 2 al fine di garantire la sicurezza dei sistemi informatici e di rete sono principalmente due: l'attuazione di strumenti per la gestione del rischio di cibersicurezza ed il rispetto degli obblighi di segnalazione.[34] Come già osservato, i soggetti tenuti all'applicazione della disciplina in materia sono quelli considerati "essenziali" ed "importanti".

La gestione dei rischi di cybersicurezza, indicata dall'art. 21, direttiva 2022/2555/UE, trova attuazione mediante l'adozione di misure tecniche, operative e organizzative che siano "adeguate e proporzionate" alle specificità del soggetto.[35] Si incoraggia, in questi termini, l'adozione di ogni tecnologia innovativa, compresa l'intelligenza artificiale, il cui utilizzo potrebbe migliorare l'individuazione e la prevenzione degli attacchi informatici.

In particolare, le misure di gestione dei rischi devono risultare adeguate ai rischi esistenti e proporzionate alla tipologia di attività svolta. L'approccio da adottare è definito "multirischio".

L'obbligo di notifica di incidenti, invece, indicato dall'art. 23, direttiva 2022/2555/UE, impone la comunicazione "senza indebito ritardo", rapida ma approfondita, al

---

[31] In particolare, l'autorità competente (o il punto di contatto unico in caso di più autorità competenti) svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA, nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro. In Italia, l'autorità competente è l'Agenzia per la cybersicurezza nazionale (ACN), di recente istituzione. In tema, per ulteriori approfondimenti circa i profili organizzativi e funzionali dell'Agenzia si rimanda a L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale di Diritto Amministrativo,* 6, 2021, 709 ss.

[32] Si tratta di una o più una autorità responsabili «della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala» (art. 9, direttiva (UE) 2022/2555, cit.) definite anche "autorità di gestione delle crisi informatiche*"*. Non si riscontra una figura analoga nella precedente direttiva che non faceva alcun riferimento alle "crisi informatiche*"*.

[33] Il "Team di risposta agli incidenti di sicurezza informatica", anche definito "*Computer Security Incident Response Team*" da cui l'acronimo inglese "CSIRT*",* svolge funzioni di prevenzione delle minacce informatiche (monitoraggio, assistenza, emissione di preallarmi, analisi preventive sui rischi, "scansione proattiva dei sistemi informatici"), funzioni di risposta e assistenza in caso di incidenti nonché di coordinamento e cooperazione in risposta a incidenti di sicurezza informatica. Il CSIRT si viene ad arricchire anche di nuove funzioni correlate al contrasto alle vulnerabilità dei sistemi informatici e di rete la cui la rapida individuazione e correzione è un fattore importante per la riduzione dei rischi *cyber*. In questo senso, vengono introdotte misure di "divulgazione coordinata delle vulnerabilità" (art. 12, direttiva (UE) 2022/2555, cit.) per segnalarle ai produttori e fornitori così da consentire loro di diagnosticarle ed eliminarle. In questo contesto, il CSIRT svolte funzioni di coordinamento CSIRT come "intermediario di fiducia" tra segnalanti e i fabbricanti o fornitori di prodotti o servizi interessati dalle vulnerabilità. Con l'art. 12, direttiva (UE) 2022/2555, cit., si viene a disporre la creazione di una "banca dati europea delle vulnerabilità", curata e gestita dall'ENISA, al fine di divulgare le vulnerabilità e fornire informazioni su di esse così da consentire agli utenti di adottare adeguate misure di attenuazione. Il CSIRT Italia è istituito presso l'Agenzia per la cybersicurezza nazionale (ACN).

[34] Si riprende e si amplia, anche rendendola unitaria, la previsione di "obblighi in materia di sicurezza e notifica degli incidenti", propri della precedente direttiva.

[35] Al fine di dimostrare l'adeguatezza delle misure di gestione del rischio è possibile fare applicazione di prodotti, servizi e processi certificati nell'ambito dei sistemi europei di certificazione della cibersicurezza previsti dal regolamento (UE) 2019/881, cit., (art. 49). Al medesimo scopo, gli Stati membri possono individuare standard tecnici relativi alla sicurezza dei sistemi informatici e di rete.

proprio CSIRT di eventuali incidenti "significativi" [36] tali da impattare negativamente sulla fornitura dei loro servizi. Analoga comunicazione può essere notificata – ove opportuno – ai destinatari dei servizi interessati. Alla disciplina delle ipotesi di notifica obbligatoria si accompagnano ipotesi di notifica volontaria di incidenti esclusi dall'ambito di applicazione dell'art. 23 ovvero da parte di soggetti esclusi dall'applicazione della Direttiva NIS 2.

Le misure di esecuzione e le funzioni di vigilanza circa l'attuazione delle disposizioni in materia sono riservate alle autorità competenti, in stretto coordinamento con le altre autorità coinvolte[37], anche al fine di evitare duplici sanzioni a fronte delle medesime condotte.[38]

Il regolamento (UE) 2019/881 ("*Cybersecurity Act*") prevede altresì l'introduzione di sistemi europei di certificazione della cybersicurezza, coordinati poi a livello nazionale e volti ad uniformare ulteriormente la risposta preventiva alle minacce *cyber* nel territorio europeo.

4. (segue): panorama normativo nazionale

L'attuale quadro di riferimento normativo è offerto principalmente dal d.lgs. 65/2018 (decreto attuativo della direttiva NIS), dal d.l. 105/2019 istitutivo del perimetro di sicurezza nazionale cibernetica e, più di recente, dal d.l. 82/2021 istitutivo, come si vedrà, dell'Agenzia per la Cybersicurezza Nazionale (ACN).

L'architettura istituzionale di riferimento è influenzata dalla peculiarità degli interessi coinvolti: organi di raccordo verticale a livello internazionale, sistemi orizzontali ed un forte accentramento di poteri. In particolare, poi, il coinvolgimento di interessi di sicurezza nazionale ha imposto una serie di interazioni con il "Sistema di informazione per la sicurezza della Repubblica" ed ha determinato l'accentramento delle funzioni in materia in capo al Presidente del Consiglio dei ministri[39].

La disciplina nazionale in materia di cybersicurezza, al netto della più o meno raggiunta definitività, ha preso le mosse, pur in ritardo, con il D.P.C.M. 24 gennaio 2013

[36] Ai sensi del richiamato art. 23, direttiva (UE) 2022/2555, cit., sono significativi quegli incidenti che causino «una grave perturbazione operativa» dei servizi o perdite finanziarie per il soggetto interessato ovvero ripercussioni su soggetti terzi causando loro «perdite materiali o immateriali considerevoli».

[37] Tra queste, le autorità poste a tutela dei dati personali: in tal senso, infatti, l'art. 31, direttiva (UE) 2022/2555, cit., prevede «nei casi di incidenti che comportano violazioni di dati personali». Specifico riferimento è anche alle autorità competenti sulla vigilanza e sull'esecuzione nei confronti dei soggetti finanziari ai sensi del regolamento (UE) 2022/2554, cit.

[38] In particolare, si fa espresso riferimento alle "violazioni che comportano una violazione dei dati personali": in tal senso, infatti, l'art. 35, direttiva (UE) 2022/2555, cit., prevede specifici obblighi informativi nel caso in cui la violazione degli obblighi imposti in materia di cybersicurezza da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali. In tali ipotesi le autorità compenti sono tenute ad informare "senza indebito ritardo" le autorità di controllo poste a tutela dei dati personali. Nel caso in cui queste impongano una sanzione amministrativa pecuniaria, le autorità competenti in materia di cybersicurezza si astengono dall'imporre una sanzione amministrativa pecuniaria relativa al medesimo comportamento, già sanzionato.

[39] Al quale l'ACN, come si dirà, sembra avvicinarsi: in tal senso, Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit., 719.

"Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". A tale decreto sono poi seguiti, nello stesso anno, il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", e il "Piano nazionale per la protezione cibernetica e la sicurezza informatica", successivamente aggiornato nel 2017. Emerge sin da subito la centralità del ruolo del Presidente del Consiglio dei ministri e degli organi della sicurezza nazionale, veri protagonisti in materia di cybersicurezza chiamati ad intervenire tramite il coordinamento degli enti coinvolti a fini di prevenzione, risposta e resilienza dei sistemi di rete nazionali.

L'attuale sistema istituzionale di cybersicurezza trova il proprio fondamento nel D.P.C.M. del 17 febbraio 2017 (c.d. Decreto Gentiloni) "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*"* con cui si è aggiornata l'architettura istituzionale del ricordato D.P.C.M. 24 gennaio 2013 individuando gli attori principali nel Presidente del Consiglio dei Ministri[40], nel Comitato interministeriale per la sicurezza della Repubblica (CISR)[41] – e relativo organo di supporto tecnico[42] - e nel Dipartimento delle informazioni per la sicurezza (DIS)[43]. Si rese, dunque, ancora più evidente lo stretto legame tra il quadro nazionale della governance in materia di cybersicurezza e le strutture coinvolte nelle questioni di sicurezza nazionale.

Sin qui la disciplina viene resa in assenza di fonti primarie e basata, come visto, su provvedimenti di indirizzo e coordinamento degli enti coinvolti.[44] È solo successiva-

[40] Indicato «quale responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della Repubblica» ed avente le seguenti competenze: convoca il CISR nelle situazioni di crisi che coinvolgono aspetti di sicurezza nazionale; adotta, su proposta del CISR, il quadro strategico nazionale per la sicurezza dello spazio cibernetico; adotta, su delibera del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali ed emana le relative direttive di indirizzo ed attuazione; impartisce, sentito il CISR, le direttive necessarie per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali.

[41] In particolare, al CISR erano originariamente riconosciute funzioni di: proposta (con riferimento al quadro strategico nazionale per la sicurezza dello spazio cibernetico); delibera, controllo e attuazione (con riferimento al Piano nazionale per la sicurezza dello spazio cibernetico); indirizzo, collaborazione tra i soggetti istituzionali e gli operatori privati interessati; cooperazione internazionale; proposta di intervento normativo. Con il D.P.C.M. del 17 febbraio 2017 (c.d. Decreto Gentiloni) gli vengono riconosciute anche funzioni di consulenza e di proposta in caso di crisi cibernetica a supporto del Presidente del Consiglio dei ministri. Ad oggi, le competenze del CISR in materia di cybersicurezza sono state trasferite al CIC – Comitato interministeriale per la cybersicurezza (ad esclusione di quelle previste dall'art. 5, d.l. 5/2019).

[42] Istituito con il D.P.C.M. del 17 febbraio 2017, cit., il CISR Tecnico ha funzioni di supporto (preparatorie ed istruttorie) alle ricordate attribuzioni del CISR.

[43] Ai sensi della l. 124/2007 ha principalmente, ma non solo, funzioni di coordinamento per le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali. All'interno del Dipartimento delle informazioni per la sicurezza (DIS) operano (*recte,* operavano) il punto di contatto unico ai fini dell'applicazione della direttiva NIS, il Nucleo sicurezza cibernetica (NSC), il Computer Security Incident Response Team (CSIRT). Con D.P.C.M. del 17 febbraio 2017, cit., al Dipartimento delle informazioni per la sicurezza (DIS) viene attributo il compito di adottare le linee di azione di interesse generale con l'obiettivo di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti. Ad oggi, le competenze del DIS in materia di cybersicurezza sono state trasferite in capo all'ACN.

[44] Per una ricognizione dell'evoluzione normativa in materia si richiama A. Renzi, *La sicurezza cibernetica: lo stato dell'arte,* in *Giornale di Diritto Amministrativo,* 4, 2021, 538 ss. e B. Carotti, *Sicurezza cibernetica e Stato-nazione*, in *Giornale di Diritto Amministrativo,* 5, 2020, 629 ss.

mente che, nel recepire la direttiva NIS, 2016/1148/UE, si interviene nella materia con una fonte legislativa primaria, il d.lgs. n. 65/2018 e successivi decreti attuativi. Tra questi, di particolare rilevanza risulta essere il D.P.C.M. 8 agosto 2019, con cui è stato costituito il "Computer Security Incident Response Team" (CSIRT) presso il Dipartimento delle informazioni per la sicurezza della Repubblica, altresì indicato quale punto di contatto unico ai sensi delle ricordate direttive europee. Quanto all'individuazione delle Autorità NIS, invece, si sono indicate nelle strutture ministeriali, con attribuzione di competenze al Ministero dello Sviluppo economico (per i settori energia, infrastrutture digitali e per gli FSD), al Ministero delle Infrastrutture e dei trasporti (per il settore trasporti), al Ministero dell'Economia e delle finanze, in coordinamento con Banca d'Italia e Consob (per i settori bancario e infrastrutture dei mercati finanziari), al Ministero della Salute, alle Regioni e Province autonome di Trento e Bolzano (per il settore sanitario) e, infine, quest'ultime, insieme al Ministero dell'Ambiente e della tutela del territorio e del mare (per il settore della fornitura e distribuzione di acqua potabile).

Da qui, però, la disciplina di riferimento viene ancora una volta a mutare per effetto dell'entrata in vigore del d.l. 105/2019 (convertito, con modificazioni, dalla l. 133/2019). Tale elaborato normativo ha istituito il "perimetro di sicurezza nazionale cibernetica" ed ha riorganizzato l'architettura istituzionale di riferimento in materia. Il perimetro di sicurezza nazionale cibernetica, salutato come inedito strumento ideato dal legislatore nazionale[45], prevede ed assicura un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici all'interno dello stesso perimetro, nel quale si trovano amministrazioni pubbliche, enti ed operatori nazionali, pubblici e privati, dai quali dipende l'esercizio di funzioni essenziali dello Stato[46] e la prestazione di servizi essenziali per gli interessi dello Stato.

All'interno del perimetro possono essere esercitati poteri tipicamente pubblicistici di controllo, ispettivi e sanzionatori da parte delle amministrazioni preposte[47] e sono sottoposti altresì ad una serie di previsioni gravanti direttamente sui soggetti all'interno del perimetro e relative ad attività di prevenzione, di notifica e risposta agli incidenti nonché agli obblighi informativi gravanti sugli stessi[48].

---

[45] Osserva A. Renzi, *La sicurezza cibernetica*, cit., 539 che si tratta di un sistema di protezione cibernetica avanzato di cui non si rinvengono simili neanche nel panorama internazionale: la misura è entrata in funzione per un periodo di prova di sei mesi a partire dal 23 giugno 2021, proprio con la finalità di testarne le debolezze e le peculiarità.

[46] In tema, circa gli interrogativi sollevati dalla nozione di "funzione essenziale dello Stato" si veda B. Carotti, *Sicurezza cibernetica e Stato-nazione*, cit., 632.

[47] Deve essere evidenziato altresì che all'interno del perimetro di sicurezza nazionale cibernetica *ex* d.l. 105/2019, a difesa dell'interesse della cybersicurezza nazionale, al Presidente del Consiglio è riconosciuta la possibilità di utilizzare strumenti ibridi riferibili solo in parte alla tutela dell'economia (*golden powers*) su atti e operazioni suscettibili di coinvolgere la sicurezza o l'integrità delle reti e, in generale, nei settori ad alta intensità tecnologica. In tema si richiama L. Fiorentino, *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. Della Cananea – L. Fiorentino (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Napoli, 2020, 39 ss.

[48] I soggetti inclusi, infatti, devono effettuare un'analisi del rischio sui loro *asset* ICT, anche in relazione agli effetti di un'interruzione e/o compromissione della propria attività, nonché valutazioni sulla mitigazione di questi eventi. In particolare, poi si prevede un obbligo di comunicazione al CVCN per qualsiasi fornitura di prodotti e servizi, secondo il procedimento di notifica regolato dal d.P.R. 54/2021.

La definizione delle modalità di attuazione del perimetro di sicurezza è stata demandata a successivi decreti attuativi.[49]
I profili organizzativi individuati dal d.l. 105/2019 prevedono l'istituzione, presso il Ministero dello sviluppo economico, prima, presso l'ACN, ora, del Centro di Valutazione e di Certificazione Nazionale (CVCN), con il compito di valutare e certificare le infrastrutture tecnologiche che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato.

5. Profili amministrativi di cybersicurezza. La creazione di nuove autorità *ad hoc* e la nuova architettura istituzionale di riferimento

Con il d.l. 82/2021, al fine di assicurare un più efficace coordinamento istituzionale, razionalizzare le competenze amministrative già delineate dal D.P.C.M. del 17 febbraio 2017 (c.d. Decreto Gentiloni) e introdurre strumenti che consentano di affrontare con efficacia e tempestività le situazioni di emergenza che coinvolgano profili di sicurezza cibernetica, è stata istituita l'Agenzia per la Cybersicurezza Nazionale-ACN[50].
Come già osservato, la cybersicurezza coinvolge una molteplicità di interessi, già oggetto di discipline puntuali ed autonome, che rendono il quadro normativo di riferimento piuttosto eterogeneo (anche in ragione delle competenze europee), stante anche l'evidente complessità tecnica della materia.[51]
Il decreto istitutivo dell'Agenzia per la Cybersicurezza Nazionale-ACN evidenza sin da subito il ruolo fondamentale[52] riconosciuto al Presidente del Consiglio dei ministri

Le misure di sicurezza, che i soggetti inclusi nel Perimetro sono tenuti ad adottare, e le modalità di notifica degli incidenti sono state definite con il D.P.C.M. 81/2021.

[49] Si fa riferimento D.P.C.M. 131/2020 per l'individuazione dei criteri sulla cui base vanno individuati i soggetti inclusi nel perimetro. In particolare, si prevede che siano le Amministrazioni competenti nei rispettivi settori strategici– interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro – ad indicare - sulla base di specifici criteri – i soggetti pubblici e privati che offrono tali servizi o funzioni essenziali. Con D.P.C.M. 81/2021, invece, si sono disciplinate le modalità e le tempistiche di notifica degli incidenti nonché ulteriori misure volte a garantire elevati livelli di sicurezza. Con D.P.C.M. del 15 giugno 2021, invece, si è proceduto all'individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, dai soggetti ivi inclusi. Da ultimo, si segnala il D.P.C.M. 92/2022 con cui, regolamentando l'accreditamento dei Centri di Valutazione (CV) e dei Laboratori Accreditati di Prova (LAP), sono completati i decreti attuativi necessari per supportare l'operatività dell'ACN e delle strutture che ad essa afferiscono, assicurando il presidio del perimetro di sicurezza nazionale cibernetica, sancendo l'operatività del Centro di Valutazione e Certificazione Nazionale (CVCN).

[50] Per ulteriori approfondimenti circa i profili organizzativi e funzionali dell'Agenzia si rimanda a L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit., 709-719.

[51] A tal riguardo, il Consiglio di Stato (Cons. Stato, sez. atti norm., 26 maggio 2020, n. 983) ha già manifestato la propria preoccupazione per i rischi di incoerenze e frammentarietà di un quadro normativo che, come visto, risulta piuttosto eterogeneo.

[52] Tendenza già nota in materia di sicurezza nazionale, specialmente a seguito della riforma del Sistema di informazione per la sicurezza della Repubblica *ex* l. 124/2007. In tema si veda, M. Savino, *Solo per i tuoi occhi? La riforma del sistema italiano di intelligence*, in *Giornale di Diritto Amministrativo,* 2, 2008, 121 ss.

in termini di alta direzione e responsabilità generale delle politiche di cybersicurezza e ciò tanto nei confronti dell'Agenzia (poteri di nomina, controllo e regolamentari) e, più in generale, nell'architettura istituzionale, con la previsione di ampie competenze in materia di cybersicurezza.[53]

Il decreto istitutivo, poi, affida una pluralità di funzioni all'Agenzia, sia istituendone di nuove in risposta alle necessità emerse in materia, sia redistribuendo e riaffidando alcune di quelle già previste, andando a semplificare il quadro normativo già esistente[54].

I compiti affidati all'Agenzia possono essere suddivisi in cinque macrocategorie.

La prima si riferisce alla funzione consultiva nei confronti del Presidente del Consiglio dei ministri nell'esercizio delle proprie competenze in materia di cybersicurezza ed in relazione alle iniziative legislative o regolamentari concernenti - anche solo parzialmente - la cybersicurezza, al fine di promuovere la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente

La seconda si riferisce alle funzioni di coordinamento interistituzionale e cooperazione internazionale (in raccordo con il Ministero degli esteri). In particolare, l'ACN garantisce l'unità dell'azione amministrativa mediante la predisposizione della strategia nazionale di cybersicurezza adottata poi dal Presidente del Consiglio dei ministri. Tra le ipotesi di collaborazione – indicate in termini generali[55] - pare interessante osservare l'espressa indicazione della possibilità di dotarsi di strumenti di coordinamento *ad hoc* con l'Autorità Garante per la protezione dei dati personali[56].

La terza si riferisce a funzioni di certificazione e qualificazione e relativi poteri ispettivi e sanzionatori. In particolare, l'Agenzia viene indicata quale autorità nazionale di certificazione della cybersicurezza ai sensi dell'art. 58 del regolamento (UE) 2019/881 con i relativi compiti di vigilanza, ispezione e sanzione.[57]

---

[53] In particolare, il Presidente del Consiglio gode rilevanti poteri nei confronti dell'Agenzia e preside il Comitato interministeriale per la cybersicurezza ed è il «vertice del Sistema di informazione per la sicurezza della Repubblica, ai fini della tutela della sicurezza nazionale anche nello spazio cibernetico» (art. 3, D.P.C.M. del 17 febbraio 2017, cit.). Ed ancora il Presidente del Consiglio ha il potere di disporre la «disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi», in caso di rischio grave e imminente per la sicurezza nazionale, ma solo «ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità» e previa deliberazione del Comitato interministeriale per la cybersicurezza (art. 5, d.l. 105/2019). Si devono altresì richiamare gli ulteriori poteri di controllo, collaborazione e interazione che il quadro normativo di riferimento attribuisce al Presidente del Consiglio e che sono stati qui richiamati diffusamente nel testo e nelle precedenti note. In senso critico a tale accentramento atteso il rischio di frammentarietà della disciplina è L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit., 718.

[54] Ad esempio, l'ACN assorbe le funzioni in materia cybersicurezza già proprie del Dipartimento delle informazioni per la sicurezza (DIS), del MISE e dell'AgID. Si veda la Tabella A nella quale si è cercato di riportare, senza pretesa di esaustività, l'evoluzione delle competenze in materia nel tempo.

[55] Non soltanto al fine di ottenere, nel rispetto delle diverse competenze, l'assistenza di altri organi o amministrazioni dello Stato, incluse le forze di polizia, ma altresì al fine di dare concreta attuazione ai trasferimenti delle competenze già esistenti n favore dell'Agenzia.

[56] Protocollo d'intesa stipulato in data 26 gennaio 2022.

[57] Facendo proprie le funzioni del Centro di Valutazione e di Certificazione Nazionale (CVCN), in tema di valutazione e certificazione delle infrastrutture tecnologiche che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato. Dal Ministero dello Sviluppo economico il CVCN è trasferito presso l'Agenzia e la sua operatività è assicurata dal 30 giugno 2022.

L'Agenzia, ancora, garantisce la qualificazione dei servizi cloud per la pubblica amministrazione e accredita, quali organismi abilitati a certificare la conformità dei sistemi di rispettiva competenza, le strutture specializzate del Ministero della difesa e del Ministero dell'interno, delegate a rilasciare il certificato europeo di sicurezza cibernetica.
La quarta si riferisce, invece, all'esercizio di poteri di vigilanza (e corrispettivi poteri sanzionatori) che vengono svolti tanto nell'ambito del perimetro di sicurezza nazionale cibernetica[58] quanto nell'ambito del proprio ruolo di Autorità nazionale competente e punto di contatto unico ai sensi della direttiva NIS in materia di sicurezza delle reti e dei sistemi informativi.
La quinta si riferisce a poteri di *moral suasion* mediante l'adozione di potere di linee guida contenenti regole tecniche di cybersicurezza nonché mediante la diffusione della consapevolezza dell'importanza della *cybersicurezza* mediante attività formative rivolte ad enti universitari, di ricerca e imprese, con i quali può concludere accordi e altre forme di partenariato pubblico-privato.
In senso trasversale all'Agenzia sono riconosciute poteri e funzioni della cd. *cyber-resilienza* quale individuazione ed attuazione delle misure necessarie a rafforzare le capacità nazionali di difesa cibernetica, attraverso il coordinamento istituzionale con gli altri soggetti pubblici coinvolti nonché mediante la promozione di iniziative dirette a sviluppare la digitalizzazione, riducendone il grado di vulnerabilità.
L'osservazione dei compiti attribuiti, anche con riferimento alla *cyber-resilienza,* rende evidente l'evoluzione rispetto alla precedente architettura istituzionale, nella quale era si riscontrava, invece, uno stretto legame tra il quadro nazionale della governance in materia di cybersicurezza e le strutture coinvolte nelle questioni di sicurezza nazionale. In realtà, nonostante le materie siano comunque affini e, spesso, orientate nella medesima direzione, il decreto istitutivo dell'Agenzia per la Cybersicurezza Nazionale separa le competenze direttamente riferibili alla sicurezza nazionale (cd. *cyberintelligence* da quelle proprie della cybersicurezza e della *cyber-resilienza* In tal senso, infatti, deve essere letto, l'accentramento di competenze in capo all'Agenzia e la conseguenziale spoliazione di competenze in capo agli organismi di informazione e sicurezza (*in primis,* CISR e DIS), pur attribuendo poteri di controllo in capo al Comitato parlamentare per la sicurezza della Repubblica (COPASIR)[59].
Come visto, allora, l'Agenzia per la Cybersicurezza Nazionale si inserisce in più ampio contesto istituzionale, adeguatamente razionalizzato mediante una generale redistribuzione delle competenze amministrative in materia – anche creandone di nuove – quanto individuando apposite sedi di coordinamento istituzionale[60]. In tal senso, dunque,

[58] Già attribuiti *ex* d.l. 105/2019 alla Presidenza del Consiglio dei ministri e al Dipartimento delle informazioni per la sicurezza.

[59] Il Presidente del Consiglio dei Ministri, infatti, è tenuto a trasmettere al Comitato parlamentare per la sicurezza della Repubblica (COPASIR) (ad ulteriore evidenza – ove vi fosse ancora qualche dubbio - della correlazione tra la *cybersicurezza* e la sicurezza nazionale), con cadenza annuale (entro il 30 giugno), una relazione sulle attività svolte nell'anno precedente dall'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del COPASIR. Analoga relazione viene trasmessa al Parlamento sull'attività svolta dall'Agenzia nell'anno precedente.

[60] Ad esempio, il Nucleo di sicurezza cibernetica (NSC), già incardinato presso il Dipartimento delle informazioni per la sicurezza, con funzioni di raccordo tra le diverse componenti dell'architettura istituzionale in materia, viene ora trasferito presso l'Agenzia.

si deve ricordare che il quadro istituzionale è arricchito dalla costituzione del "Nucleo per la cybersicurezza" e del "Comitato interministeriale per la cybersicurezza" con il compito di affiancare le autorità e gli organi già esistenti e già provvisti di competenze in materia di sicurezza cibernetica al fine di assicurare un più efficace coordinamento interistituzionale[61].

Il Nucleo per la cybersicurezza, in particolare, supporta il Presidente del Consiglio nella predisposizione e attivazione delle procedure di allertamento in caso di crisi cibernetiche, nonché nella prevenzione di queste ultime. Sulla base di tali attività, l'Agenzia darà attuazione ai provvedimenti assunti dal Presidente del Consiglio, controllandone anche la corretta esecuzione. Il Nucleo per la cybersicurezza ha un importante ruolo operativo in relazione alle situazioni di crisi cibernetica (tanto mediante attività di programmazione e pianificazione delle risposte da adottare, quanto mediante l'elaborazione delle procedure di coordinamento interministeriale). In occasione di minacce per la cybersicurezza valuta se tali eventi assumano intensità o natura tali da non poter essere fronteggiati adeguatamente dalle singole amministrazioni e può imporre l'adozione di decisioni coordinate in sede interministeriale, dandone tempestiva informazione al Presidente del Consiglio dei ministri.

Istituito presso la Presidenza del Consiglio dei ministri, al Comitato interministeriale per la cybersicurezza, invece, sono attribuite funzioni consultive di consulenza, bilancio, indirizzo e proposta[62] e vigilanza[63] in materia di politiche di cybersicurezza[64].

6. Conclusioni. Il prisma di Newton nella regolazione dei dati, l'esempio della *cybersicurezza*

Il presente contributo si è aperto con la descrizione del nuovo ruolo dei dati, si sono poi accennate le connesse tematiche della cybersicurezza – prendendole ad esempio - ed ora, concludendo, si vuole tracciare una linea lungo cui estendere l'ambito di indagine per ricomprendervi l'intera regolazione amministrativa dei dati, equiparandola al prisma di Newton.

L'immagine è nota ai più e riproduce il fenomeno della rifrazione: la luce bianca entra

[61] Che, come osserva L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit., si tratta, in particolare, del Presidente del Consiglio dei ministri, del Comitato interministeriale per la sicurezza della Repubblica (CISR), del Dipartimento delle informazioni per la sicurezza (DIS), dell'Agenzia informazioni e sicurezza esterna (AISE), dell'Agenzia informazioni e sicurezza interna (AISI) e del Comitato parlamentare per la sicurezza della Repubblica (COPASIR). Si tratta, come già osservato, di enti posti a garanzia della sicurezza nazionale, tutti istituiti o riformati dalla l. 124/2007.

[62] In particolare, presso il Comitato interministeriale per la cybersicurezza (CIC) propone al Presidente del Consiglio gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza e promuove l'adozione di iniziative volte a favorire la collaborazione, anche a livello internazionale, tra soggetti istituzionali e operatori privati ai fini dell'adozione delle migliori pratiche.

[63] Quanto poi alle funzioni di vigilanza, il Comitato esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza.

[64] Al Comitato interministeriale per la *cybersicurezza*, come visto, sono affidate tutte le funzioni di consulenza e proposta già attribuite al CISR (fatta eccezione per quelle previste dall'art. 5, d.l. 105/2019, in materia di determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica).

nel prisma, si separa nello spettro dei colori costituenti, e, nell'uscire, li manifesta e li accentua per effetto della rifrazione.
Visivamente, il prisma di Newton esplicita la tesi che si propone: l'unicità del fenomeno dell'utilizzo dei dati a fini decisionali nelle economie data driven (la luce bianca), passando attraverso la necessità, *recte* doverosità, di una regolazione pubblica (il prisma), ne esce in un fascio di competenze e attribuzioni distinte (lo spettro dei colori costituenti), che sollevano questioni interpretative che si vanno ponendo.
Le istanze di certezza del diritto in materia di regolazione dei dati sono accentuate dalla considerazione per la quale questi vengono a costituire la base per comprendere e disciplinare lo sviluppo dell'intelligenza artificiale – verso il quale ci si dirige ad ampi passi.
Il fenomeno dell'affermazione del valore economico dei dati, elaborati mediante algoritmi e sistemi di intelligenza artificiale, si deve osservare nel tradizionale rapporto tra diritto e tecnologia, che si viene ad intrecciare in un profondo legame che li rende assolutamente permeabili alle novità, l'uno dell'altro. Da una parte, infatti, il diritto è chiamato a disciplinare le nuove possibilità offerte dall'evoluzione tecnologica, dall'altra quest'ultima influenza la quotidianità dei rapporti giuridici[65] e, per quanto d'interesse, anche le modalità con cui opera la pubblica amministrazione. Infatti, se da un lato il sorgere di nuovi interessi e nuove dinamiche sociali impone una tutela e regolamentazione delle situazioni quanto attraverso la creazione di nuove forme di tutela[66]; dall'altro, allo stesso tempo, è anche il diritto ad utilizzare l'evoluzione tecnologica per il perseguimento dei propri fini[67].
La *cybersicurezza*, infatti, al pari di ogni disciplina che coinvolge l'utilizzo nei processi decisionali dei dati (anche con finalità commerciali), si scontra con più o meno inedite questioni ordinamentali che qui possono essere così indicate nell'ibridazione delle competenze (*i*) e nell'internazionalizzazione dei fenomeni da regolare (*ii*); nella necessità di acquisire maggiori competenze tecniche (*iii*) e di rapidi tempi di reazione (*iv*).
È stato già osservato come le peculiarità dell'utilizzo dei dati (anche personali) nei processi decisionali, tanto pubblici quanto privati, conducono ad un coinvolgimento di distinti interessi pubblici, la cui tutela è affidata ad altrettante autorità amministrative e disciplinata secondo distinti plessi normativi. In tal senso, ad esempio, si sta animando il dibattito circa la possibilità di individuare illeciti antitrust attuati mediante la violazione di norme poste a tutela della privacy[68] e, in termini più generali, circa la

[65] Le rivoluzioni scientifiche e tecnologiche contribuiscono a modificare i paradigmi sociali e, quindi, giuridici: portano a trasformazioni anche radicali della società umana e, conseguentemente, del contesto normativo di riferimento. Si pensi, ad esempio, alle questioni di bioetica che il progresso scientifico ha sollevato. Per un'analisi delle connessioni tra tecnologia e sviluppo economico, invece, si veda M. Clarich, *Istituzioni, nuove tecnologie, sviluppo economico*, in *Diritto pubblico,* 1, 2017, 75 ss.

[66] Il diritto è, infatti, una scienza sociale e, come tale, risente delle grandi direttrici di cambiamento della società. Il diritto mantiene una funzione ordinatrice anche riguardo ai mutamenti tecnologici e scientifici della società. Si pensi alla crescente sensibilità maturata in ambito ecologico che ha portato ad un ripensamento del diritto ambientale, ad esempio, ovvero all'impatto avuto dall'espansione dell'industria ferroviaria.

[67] È evidente, allora, che il diritto – e non solo quello amministrativo – risenta della trasformazione in essere della società contemporanea derivante dallo sviluppo dell'informatica e dell'intelligenza artificiale.

[68] È stato osservato, infatti, che il potere raggiunto venga esercitato nei confronti dei consumatori,

crescente interdisciplinarietà portata dai descritti fenomeni.[69] Ad oggi, a legislazione invariata, le amministrazioni, nel perseguimento degli interessi pubblici che sono loro affidati, sono chiamate a rispondere alle nuove sfide poste dalle economie dei dati, non soltanto nella rappresentata maggiore interdipendenza tra competenze e i rispettivi plessi amministrativi di riferimento ma altresì nella maggiore cooperazione ed interazione a livello internazionale determinata dalla rilevanza sovranazionale dei dati e della loro circolazione.

Tali questioni conducono ad una necessaria analisi della perdurante efficacia dei tradizionali istituti amministrativi e, in particolar modo, delle modalità con cui queste trovano applicazione procedimentale: ciò che si vuole sostenere è che la struttura del diritto amministrativo, ancorata saldamente su principi cardine di carattere generale,[70] non deve necessariamente essere oggetto di specifici adattamenti a fronte di mutamenti rivoluzionari che interessano la società di riferimento: ciò non significa però che il quadro normativo di riferimento sia sempre sufficiente alla regolazione dei nuovi fenomeni economici e sociali che il progresso scientifico consente.

sottoponendoli anche a processi e trattamenti in contrasto con i loro diritti fondamentali (tra tutti, la privacy, la libertà di autodeterminazione) piuttosto che in violazione delle regole proconcorrenziali. La letteratura sul tema si va ampliando e, senza pretesa di esaustività, si richiama, G. Pitruzzella, *Big data, competition and privacy: a look from the antitrust perspective,* in *Concorrenza e mercato,* 23, 2016; G. Colangelo – M. Maggiolino, *Big data, data protection and antitrust in the wake of the "bundeskartellamt" case against Facebook*, in *Rivista Italiana Antitrust*, 1, 2017, 104 ss.; M. Midiri, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *Federalismi.it*, 14, 2020, 209 ss. Recente è anche M. E. Stucke, *The Relationship Between Privacy and Antitrust*, in *Notre Dame Law Review*, in corso di pubblicazione, in *ssrn.com*, 5 marzo 2022; F. Costa – C.O. Lynskey, *Family ties: the intersection between data protection and competition in EU law*, in *Common Market Law Review*, 54(1), 2017, 11 ss.

[69] In termini più generali, si veda, ad esempio, L. Tarasco – M. Giaccaglia, *Facebook è gratis? "Mercato" dei dati personali e giudice amministrativo*, in *Il diritto dell'economia,* 102, 2020, 265 ss.; S. Gobbato, *Big Data e "tutele convergenti" tra concorrenza, GDPR, e Codice del Consumo,* in questa *Rivista,* 3, 2019, 148 ss. Sul rapporto tra antitrust e tutela della proprietà intellettuale, si rimanda a M. Maggiolino – L. Zoboli, *The Intersection Between Intellectual Property and Antitrust Law*, in I. Calboli – M. L. Montagnani (a cura di), *Handbook on Intellectual Property Research*, Oxford, 2021.

[70] Cons. Stato, Ad. Plen., sent. 3/1981.

Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo

Flavia Bavetta

Abstract

Grazie ad una rapida trasformazione del digitale e all'interconnessione della società, i sistemi e servizi informatici, così come le infrastrutture di rete, occupano una posizione centrale nello svolgimento di tutte le attività che compiamo ogni giorno. Da tale considerazione ne discende inevitabilmente un'espansione del panorama delle minacce informatiche, le quali, ponendo nuove sfide al legislatore sia europeo che nazionale, richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. A tal riguardo, il legislatore europeo aveva emanato già nel 2016 la direttiva (UE) 2016/1148 (c.d. Direttiva NIS 1) con l'intento di innalzare i livelli di cybersecurity di un ristretto alveo di operatori ritenuti essenziali per la continuità operativa delle funzioni e dei servizi più importanti degli Stati membri. Tuttavia, tale obiettivo è stato solo parzialmente raggiunto, rendendosi così necessario un intervento in materia a distanza di pochissimi anni. Infatti, il 27 dicembre 2022 è stata emanata la direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, (cd. Direttiva NIS 2), con il preciso obiettivo di rendere il livello di *cybersecurity* di operatori considerati "essenziali" e "importanti" uniforme su tutto il territorio europeo.
Alla luce di ciò, il presente contributo analizza i principali adempimenti previsti dalla Direttiva NIS 2.

Thanks to a rapid digital transformation, ICT systems and services, as well as network infrastructures, occupy a central position in the maintenance of all the activities we carry out every day. Therefore, inevitably an expansion of the cyber threat landscape can be observed, posing new challenges to both European and national legislators, requiring appropriate, coordinated and innovative responses across all member states. In this regard, the European legislature had already enacted Directive (EU) 2016/1148 (NIS 1 Directive) in 2016 with the intention of raising the cybersecurity levels of a narrow range of operators deemed essential for the continuity of the most important functions and services of the member states. However, this goal has only been partially achieved, thus requiring more actions on the matter. Indeed, on December 27, 2022, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the

Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) was enacted, with the specific aim of making the level of cybersecurity of operators considered "essential" and "important" uniform throughout Europe.
In light of this, this paper analyzes the main obligations and novelties under the NIS 2 Directive.

Sommario

1. L'aumento delle minacce cibernetiche e la risposta del legislatore; 2. Ambito di applicazione della Direttiva NIS 2; 3. Soggetti essenziali e importanti; 4. Gli adempimenti della Direttiva NIS 2; 4.1. Misure in materia di gestione dei rischi di cybersicurezza; 4.1.1. Misure in materia di gestione dei rischi; 4.1.2. Ruolo dei membri degli organi gestori; 4.1.3. Obblighi di formazione; 4.2 Obblighi di segnalazione; 4.3 Condivisione delle informazioni sulla cybersicurezza; 4.3.1 Accordi di condivisione delle informazioni sulla cybersicurezza; 4.3.2. Notifica volontaria di informazioni pertinenti; 4.4. Misure di vigilanza e di esecuzione; 5. Misure sanzionatorie; 6. Conclusione.

Keywords

cybersecurity - DirettivaNIS2 - misuredisicurezza - resilienza - UnioneEuropea.

1. L'aumento delle minacce cibernetiche e la risposta del legislatore

Grazie ad una rapida trasformazione del digitale e all'interconnessione della società, i sistemi e servizi informatici, così come le infrastrutture di rete, occupano una posizione centrale nello svolgimento di tutte le attività che compiamo ogni giorno.
Da tale considerazione ne discende inevitabilmente un'espansione del panorama delle minacce informatiche, le quali, ponendo nuove sfide al legislatore sia europeo che nazionale, richiedono risposte adeguate, coordinate e innovative in tutti gli Stati membri. Infatti, i dati degli ultimi anni dimostrano come il numero, la portata, il livello di sofisticazione, la frequenza e l'impatto degli incidenti sia sempre più in aumento, rappresentando una grave minaccia per il funzionamento dei sistemi informatici e di rete che, nella maggior parte dei casi, hanno un impatto sulle infrastrutture necessarie per l'erogazione delle funzioni e dei servizi essenziali dello Stato. Tali incidenti hanno il potenziale di impedire l'esercizio delle attività economiche nel mercato interno, provocare perdite finanziarie, minare la fiducia dei cittadini e causare gravi danni all'economia e alla società dell'Unione[1]. Pertanto, l'efficacia delle misure di cybersicurezza sono oggi

[1] A tal proposito, si veda l'ENISA Threat Landscape 2022. Tale documento riporta indicazioni sullo stato delle minacce di *cybersecurity* a livello globale. In particolare, il *report* ha l'obiettivo di identificare le principali minacce, le tendenze osservate rispetto a queste ultime, l'evoluzione di *threat actors* e di tecniche di attacco, nonché l'analisi del loro impatto. Nel merito, da quanto osservato dall'Autorità, con oltre 10 *terabyte* di dati rubati mensilmente, il *ransomware* è ancora una delle principali minacce, mentre

più che mai essenziali per il corretto funzionamento del mercato interno, soprattutto considerato che esse sono un fattore abilitante fondamentale per molti settori critici. A tal riguardo, il legislatore europeo aveva emanato già nel 2016 la direttiva (UE) 2016/1148 (c.d. Direttiva NIS 1) con l'intento di innalzare i livelli di *cybersecurity* di un ristretto alveo di operatori ritenuti essenziali per la continuità operativa delle funzioni e dei servizi più importanti degli Stati membri. Tuttavia, tale obiettivo è stato solo parzialmente raggiunto, rendendosi così necessario un intervento in materia a distanza di pochissimi anni. Infatti, il 27 dicembre 2022 è stata emanata la direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, (cd. Direttiva NIS 2), con il preciso obiettivo di rendere il livello di *cybersecurity* di operatori considerati "essenziali" e "importanti" uniforme su tutto il territorio europeo. Come espressamente sancito nelle disposizioni finali, gli Stati membri dovranno emanare le normative di recepimento a livello nazionale entro e non oltre il 17 ottobre 2024 al fine di permettere agli operatori ricompresi di raggiungere i precisi obiettivi previsti dalla Direttiva NIS 2.

2. Ambito di applicazione della Direttiva NIS 2

Con riguardo all'ambito applicativo della direttiva, a differenza della precedente Direttiva NIS 1, il legislatore ha ampliato il novero di soggetti ivi compresi. A tal proposito, l'art. 2 della direttiva chiarisce innanzitutto che essa si applica a soggetti pubblici o privati che, congiuntamente:

- operino in settori strategici, quali quelli dell'energia, dei trasporti, delle banche, delle infrastrutture dei mercati finanziari, dell'acqua potabile, della sanità e delle infrastrutture digitali, dell'*e-commerce*, dei motori di ricerca e del *cloud computing*;
- siano considerati medie imprese ai sensi all'art. 2, par. 1, dell'allegato alla raccomandazione 2003/361/CE, o che superano i massimali per le medie imprese di cui al par. 1 di tale articolo. A tal proposito, si precisa che la raccomandazione 2003/361 individua come soglie per la definizione di media impresa l'occupazione di più di 250 persone, un fatturato annuo superiore agli euro 50 milioni o un totale di bilancio annuo superiore agli euro 43 milioni; e
- prestino i loro servizi o svolgono le loro attività all'interno dell'Unione.

Inoltre, la Direttiva NIS 2 si applica, indipendentemente dalle dimensioni degli operatori, qualora:

il *phishing* è identificato come il vettore iniziale più comune per tali attacchi. In aggiunta, l'importanza del tema è ancor più chiara a seguito della situazione geopolitica e, in particolare, dell'invasione russa dell'Ucraina, che può essere considerata come punto di svolta per l'identificazione della rilevanza del dominio dello spazio cibernetico. A tal proposito, l'ENISA osserva un continuo aumento del numero di minacce, l'emergere di una gamma più ampia di vettori come *exploit zero-day*, disinformazione e *deepfake*. Tra l'altro, secondo quanto indicato nel rapporto, gli attacchi cibernetici sono aumenti nella seconda metà del 2021 e durante il 2022, non solo in termini di vettori e numeri, ma anche in termini di impatto. Tutti i settori sono coinvolti. Gli attacchi sono diretti sia verso i settori della pubblica amministrazione (24%), che nei confronti dei *digital service providers* (13%) e del pubblico in generale (12%), nonché, più diffusamente, verso i soggetti operanti in ogni settore dell'economia.

- i servizi siano forniti da:
  - fornitori di reti di comunicazione elettroniche pubbliche o di servizi di comunicazione elettronica accessibili al pubblico;
  - prestatori di servizi di fiducia;
  - registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;
- il soggetto sia l'unico fornitore in uno Stato membro di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
- una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
- una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;
- il soggetto sia critico in ragione della sua particolare importanza a livello nazionale regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nello Stato membro;
- il soggetto sia un ente della pubblica amministrazione;
- il soggetto sia identificato come critico ai sensi della direttiva (UE) 2022/2557.

3. Soggetti essenziali e importanti

Un'ulteriore novità della Direttiva NIS 2 è la distinzione dei soggetti ivi ricompresi tra "soggetti essenziali" e "soggetti importanti". Nella prima categoria vi rientrano, a differenza della precedente normativa, anche le pubbliche amministrazioni, che si affiancano ad operatori del settore energetico, sanitario, spaziale, bancario, dei trasporti, delle infrastrutture digitali, delle acque. Tra i "soggetti importanti", invece, si annoverano, *inter alia*, operatori di servizi postali e di corriere, di gestione dei rifiuti, del settore chimico, del settore agroalimentare.

4. Gli adempimenti della Direttiva NIS 2

Nonostante le normative di recepimento nazionale dettaglieranno la portata di molti degli adempimenti previsti dalla Direttiva NIS 2, è possibile già in questa fase analizzarne alcuni e, in particolare:

a) l'adozione di misure in materia di gestione dei rischi di cybersicurezza (artt. 20 – 21 – 24);
b) l'adempimento di obblighi di segnalazione (art. 23);
c) l'adozione di canali per la condivisione delle informazioni sulla cybersicurezza (artt. 29 – 30);
d) la sottoposizione a misure di vigilanza e di esecuzione (artt. 32 – 33).

4.1. Misure in materia di gestione dei rischi di cybersicurezza

Tra gli obblighi previsti dalla normativa che avranno un impatto diretto sui soggetti "essenziali" e "importanti" rientrano (i) quelli relativi alle misure in materia di gestione dei rischi di cybersicurezza; (ii) l'individuazione del ruolo dei membri degli organi gestori; e (iii) gli obblighi di formazione.

4.1.1. Misure in materia di gestione dei rischi

In particolare, ai sensi dell'art. 21 della direttiva, al fine di assicurare un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti, «gli Stati membri provvedono affinché i soggetti essenziali e i soggetti importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.
Le [predette] misure […] sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:

a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
b) gestione degli incidenti;
c) continuità operativa, come la gestione del *backup* e il ripristino in caso di disastro, e gestione delle crisi;
d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;
g) pratiche di igiene informatica di base e formazione in materia di cybersicurezza;
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;
j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso».

Pertanto, la lista ivi descritta risulta di particolare importanza in quanto permette di comprendere, almeno in linea generale, quali siano le misure di sicurezza che gli operatori soggetti alla Direttiva NIS 2 saranno tenuti ad implementare.
In aggiunta a quanto sopra e per mera completezza, si segnala che, ai sensi dell'art. 24 della direttiva, «al fine di dimostrare il rispetto di determinate prescrizioni di cui

all'art. 21, i soggetti essenziali potranno utilizzare determinati prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza adottati a norma dell'art. 49 del regolamento (UE) 2019/881». Dunque, nell'implementazione delle misure di sicurezza precedentemente illustrate, anche al fine di facilitarne l'attuazione, gli operatori potranno servirsi di prodotti sviluppati da soggetti che abbiamo acquisito la certificazione di cybersicurezza ai sensi del Regolamento sulla cybersicurezza.

4.1.2. Ruolo dei membri degli organi gestori

Inoltre, l'art. 20 prevede che i membri degli organi di gestione approvino le misure di gestione dei rischi di cybersicurezza, adottate ai sensi dell'art. 21. A tal proposito, si precisa che essi dovranno sovraintendere alla loro attuazione e potranno essere ritenuti responsabili di ogni violazione della Direttiva NIS 2. Dunque, la direttiva identifica il ruolo centrale degli organi di gestione degli operatori che, per legge, dovranno essere coinvolti nell'attuazione degli obblighi da questa derivanti. Ciò anche considerato che, come verrà meglio chiarito dalle legislazioni nazionali, essi potranno essere ritenuti responsabili della mancata adozione delle misure atte a rendere gli operatori conformi alle prescrizioni della normativa.

4.1.3. Obblighi di formazione

In ultimo, si segnala che ai sensi dell'art. 20, c. 3, della direttiva i membri dell'organo di gestione saranno tenuti a seguire una specifica formazione, al fine di acquisire conoscenze e competenze sufficienti per individuare i rischi e valutare le modalità di gestione dei rischi di cybersicurezza, nonché il loro impatto sui servizi offerti. Tra l'altro, il medesimo articolo consiglia di estendere la stessa iniziativa anche nei confronti dei dipendenti. Dunque, al fine di adempiere ai suddetti obblighi, gli operatoti dovranno tenere sessioni di formazione per i membri dell'organo di gestione volte all'acquisizione delle conoscenze e competenze in materia di cybersicurezza.

4.2 Obblighi di segnalazione

Secondo quanto stabilito dall'art. 23 della Direttiva NIS 2 «i soggetti essenziali e i soggetti importanti notificano senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, conformemente al par. 4, eventuali incidenti che hanno un impatto significativo sulla fornitura dei loro servizi quali indicati al par. 3 (incidente significativo). Se opportuno, i soggetti interessati notificano senza indebito ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi».

A tal proposito, l'art. 23, c. 3, della direttiva precisa che per incidenti significativi devono intendersi quegli eventi in grado di causare (i) una grave perturbazione dei servizi o perdite finanziarie o (ii) di avere ripercussioni su altre persone fisiche o giuridiche.
Inoltre, viene indicato che i soggetti importanti ed essenziali dovranno comunicare qualunque informazione che consenta al CSIRT o, se opportuno, all'autorità competente di determinare l'eventuale impatto transfrontaliero dell'incidente.
Pertanto, qualora gli operatori subiscano un incidente qualificabile come "significativo" dovranno comunicarlo all'autorità competente e ai destinatari dei loro servizi, fornendo:

a) senza indebito ritardo, e comunque entro 24 ore da quando sarà venuta a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo sia sospettato di essere il risultato di atti illegittimi o malevoli o possa avere un impatto transfrontaliero;
b) senza indebito ritardo, e comunque entro 72 ore da quando sarà venuta a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, aggiorni le informazioni di cui alla lettera *a)* e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
c) su richiesta di un CSIRT o, se opportuno, di un'autorità competente, una relazione intermedia sui pertinenti aggiornamenti della situazione;
d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera *b)*, che comprenda:
    - una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;
    - il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;
    - le misure di attenuazione adottate e in corso;
    - se opportuno, l'impatto transfrontaliero dell'incidente;
e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera *d)*, una relazione sui progressi in quel momento e una relazione finale entro un mese dalla gestione dell'incidente.

Dunque, alla luce dell'*iter* descritto, gli operatori dovranno adeguare i propri processi interni alle richieste del legislatore, nonché prevedere un'apposita procedura che individui gli obblighi da adempiere in caso di incidente.

4.3 Condivisione delle informazioni sulla cybersicurezza

4.3.1 Accordi di condivisione delle informazioni sulla cybersicurezza

Secondo quanto previsto dall'art. 29 della direttiva gli Stati membri dovranno prevedere dei canali che diano la possibilità ai soggetti essenziali e importanti di scambiare, su base volontaria, pertinenti informazioni sulla cybersicurezza, comprese informazioni

relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di cybersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cybersicurezza per individuare le minacce informatiche. Inoltre, ai sensi del comma 2, tale scambio potrà avvenire anche nei confronti dei fornitori. Pertanto, al netto delle specifiche indicazioni che verranno fornite dagli Stati membri, è necessario segnalare che gli operatori, su base volontaria, potranno valutare se condividere le informazioni sopra indicate. Chiaramente, una simile scelta implica anche la valutazione di diversi aspetti legali – come quelli contrattuali nei confronti dei fornitori – a cui i soggetti "essenziali" e "importanti" dovranno necessariamente porre attenzione.

4.3.2. Notifica volontaria di informazioni pertinenti

In aggiunta a quanto sopra, ai sensi dell'art. 30 della direttiva, si precisa che, unitamente alle notifiche trasmesse in ossequio all'art. 23, potranno essere notificati al CSIRT su base volontaria:

- gli incidenti, ovvero un evento che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi;
- le minacce informatiche, ovvero qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone;
- i quasi incidenti, ovvero qualsiasi evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato.

Dunque, anche in questo caso, gli operatori dovranno valutare diversi aspetti legali al fine di decidere se procedere con la notifica di incidenti su base volontaria.

4.4. Misure di vigilanza e di esecuzione

In ultimo, si segnala che alla luce dell'art. 32 della Direttiva NIS 2, dedicato agli aspetti generali delle misure di vigilanza e di esecuzione, gli operatori potranno essere soggetti alle seguenti attività di vigilanza:

a) ispezioni in loco e vigilanza a distanza, compresi controlli casuali, effettuati da professionisti formati;
b) *audit* sulla sicurezza periodici e mirati effettuati da un organismo indipendente o da un'autorità competente;
c) *audit ad hoc*, ivi incluso in casi giustificati da un incidente significativo o da una violazione della direttiva da parte del soggetto essenziale;
d) scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non di-

scriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

e) richieste di informazioni necessarie a valutare le misure di gestione dei rischi di cybersicurezza adottate dal soggetto interessato, comprese le politiche di cybersicurezza documentate, nonché il rispetto dell'obbligo di trasmettere informazioni alle autorità competenti;
f) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei compiti di vigilanza;
g) richieste di dati che dimostrino l'attuazione di politiche di cybersicurezza, quali i risultati di *audit* sulla sicurezza effettuati da un controllore qualificato e i relativi elementi di prova.

Qualora, nell'ambito dello svolgimento delle attività sopra descritte, le autorità competenti accertino delle violazioni, si precisa che esse avranno il potere di emanare avvertimenti, adottare istruzioni vincolanti o ingiunzioni che impongano agli operatori di adottare le misure necessarie per porre fine alle violazioni riscontrate e, più in generale, di irrogare sanzioni.

5. Misure sanzionatorie

In relazione al quadro sanzionatorio, l'art. 34 prevede che ove i soggetti importanti violino l'art. 21 (Misure in materia di gestione dei rischi di cybersicurezza) o l'art. 23 (obblighi di segnalazione), essi saranno soggetti a sanzioni pecuniarie amministrative pari a un massimo di almeno 10.000.000 EUR o a un massimo di almeno il 2% del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto essenziale appartiene, se tale importo è superiore.

Laddove, invece, sia un soggetto importate a violare le suddette disposizioni, esso potrà essere sottoposto a sanzioni pecuniarie amministrative pari a un massimo di euro 7.000.000 o a un massimo di almeno l'1,4 % del totale del fatturato mondiale annuo per l'esercizio precedente dell'impresa cui il soggetto importante appartiene, se tale importo è superiore.

In aggiunta a quanto sopra, ai sensi dell'art. 35 della direttiva, qualora le autorità competenti, in sede di vigilanza o di esecuzione, vengano a conoscenza del fatto che la violazione degli obblighi di cui agli artt. 21 e 23 può comportare una violazione dei dati personali, ne informano senza indebito ritardo l'Autorità garante per la protezione dei dati personali. Laddove tale autorità di controllo irroghi una sanzione amministrativa ai sensi del GDPR, le autorità competenti non imporranno una sanzione amministrativa pecuniaria a norma dell'art. 34 della direttiva per una violazione imputabile al medesimo comportamento, già punito con l'ammenda amministrativa pecuniaria.

6. Conclusione

In conclusione, dall'analisi della direttiva risulta chiaro come un *corpus* normativo dalla

portata applicativa tanto ampia abbia certamente l'intento di migliorare le capacità di resilienza e di risposta agli incidenti da parte dei soggetti pubblici e privati, cercando di risolvere le criticità di forte frammentazione che la Direttiva NIS 1 aveva creato. Tuttavia, è necessario notare come la Direttiva NIS 2 complichi notevolmente il quadro normativo sulla sicurezza delle infrastrutture critiche in termini di coordinamento, rendendo lo svolgimento dei suoi adempimenti molto gravoso per gli operatori. Infatti, è necessario ricordare come nell'attesa che il legislatore europeo definisse il nuovo testo normativo, diversi parlamenti nazionali – come quello italiano con il d.l. 105/2019 che istituisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) – hanno provveduto a colmare l'allora sussistente lacuna normativa in ambito di *cybersecurity*. Ciò, se da un lato alimenta un virtuoso meccanismo che innalza l'attenzione sui temi della cybersicurezza, dall'altro può sovraccaricare gli attori privati e pubblici di costosi adempimenti normativi. Infatti, laddove non sussista un chiaro allineamento tra le previsioni del PSNC e le disposizioni nazionali di attuazione della direttiva, moltissimi grandi *player* europei e nazionali dovranno affrontare ingenti costi di *compliance*, conseguendo, tuttavia, obiettivi nella pratica già raggiunti – nel caso italiano – grazie al PSNC.

Pertanto, il recepimento della Direttiva NIS 2 negli ordinamenti nazionali rappresenta un'opportunità per ricomporre in modo coerente il mosaico delle normative in materia di *cybersecurity*. In tale contesto, è, dunque, auspicabile che questa opera di sistematizzazione venga compiuta di concerto con gli Stati membri dell'Unione europea, al fine di evitare che i margini di discrezionalità lasciati a ciascuno rischino di creare differenze normative e tecniche tali da ridurre o addirittura vanificare gli obiettivi fissati dalla normativa europea.

Dati personali e decisioni automatizzate: quale trasparenza?*

Gianluca Fasano

Abstract

Le tecnologie basate sull'intelligenza artificiale sono incredibilmente diffuse nelle società contemporanee e i vantaggi derivanti sono evidenti in qualsiasi settore dell'attività umana. Trattandosi di meccanismi in grado di condizionare la vita delle persone, essi sollevano numerosi interrogativi sul piano sociale, etico e giuridico. Nel campo delle decisioni automatizzate, in particolare, molto è stato fatto per la protezione dei dati personali e, in tale scenario, un ruolo fondamentale è stato riconosciuto al principio di trasparenza. Principio che, oggi, andrebbe rafforzato con nuovi contenuti e garanzie, abbandonando la narrazione di strumento per la mera comprensione del funzionamento dei sistemi automatizzati – sofisticati e alle volte incomprensibili - e ricostruendolo invece come mezzo per acquisire consapevolezza circa i condizionamenti derivanti dal loro utilizzo e per garantire la partecipazione attiva dell'interessato allo sviluppo della sua identità digitale.

Technologies based on artificial intelligence are incredibly widespread in contemporary societies and the resulting benefits are evident in any sector of human activity. Since these are mechanisms capable of conditioning people's lives, they raise numerous questions on a social, ethical and legal level. In the field of automated decisions, in particular, much has been done for the protection of personal data and, in this scenario, a fundamental role has been recognized to the principle of transparency. A principle that, today, should be strengthened with new contents and guarantees, abandoning the narrative of a tool for the mere understanding of the functioning of automated systems - sophisticated and sometimes incomprehensible - and reconstructing it instead as a means of gaining awareness about the conditioning deriving from their use and to ensure the active participation of the interested party in the development of his digital identity.

Sommario

1. Introduzione. - 2. La trasparenza delle decisioni automatizzate secondo la normativa del regolamento (UE) 679/2016. - 3. Il principio di non esclusività della decisione

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

automatizzata. - 4. Le eccezioni al principio di non esclusività: il consenso. - 5. Conclusioni

Keywords

consenso – trasparenza - intelligenza artificiale - decisione automatizzata - trustworthy AI.

1. Introduzione

L'utilizzo di sistemi intelligenti porta vantaggi evidenti in molti settori dell'attività umana: l'intelligenza artificiale (IA)[1] riconosce il volto di una persona identificando un soggetto per esigenze di sicurezza, supporta i medici nella lettura delle immagini radiografiche migliorando le diagnosi e la prevenzione, offre maggiore sicurezza alla guida di automobili e nei trasporti, concorre alla tutela dell'ambiente ed altro ancora. Può anche facilitare l'accesso all'informazione, all'istruzione e alla formazione: con l'epidemia di COVID-19 l'apprendimento a distanza è diventato una necessità.

Le ragioni per sostituire, in alcune attività, gli esseri umani con sistemi automatizzati solitamente vengono ricondotte a vantaggi di elaborazione dati su larga scala, velocità, volume e alle aspettative di tassi di errore inferiori rispetto agli esseri umani. Di fondo, viene riconosciuta loro una maggiore efficienza rispetto alle capacità analitiche umane: gli algoritmi predittivi sono infatti in grado di analizzare quantità elevatissime di dati, anche fra loro eterogenei sotto il profilo qualitativo, individuandone preziose correlazioni, rapporti, inferenze che nessuna valutazione umana sarebbe in grado di rilevare. Queste qualità destano immancabilmente riconoscimento e apprezzamento ma, ciò nonostante, v'è da considerare che esse pongono all'uomo moderno considerevoli sfide, per alcune comprensibili ragioni. Innanzitutto, i sistemi intelligenti sono legati al crescente sviluppo del fenomeno dei cd. *Big Data*[2], il substrato di alimentazione degli

[1] Per Intelligenza Artificiale (IA) si intende «la scienza che sviluppa modelli computazionali del comportamento intelligente, e quindi fa sì che gli elaboratori possano eseguire compiti che richiederebbero intelligenza da parte dell'uomo», così G. Sartor, *Intelligenza artificiale e diritto*, Milano, 1996, 10. Tra le definizioni più accreditate spicca quella dell'Università di Stanford, che la identifica come «una scienza e un insieme di tecniche computazionali che vengono ispirate - pur operando tipicamente in maniera diversa - dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire». Si veda *Artificial Intelligence and life in 2030, One hundred year study on Artificial Intelligence*, Stanford University, 2016, 5. L proposta di regolamento sull'utilizzo dei sistemi di intelligenza artificiale (IA) diffusa dalla Commissione europea il 21 aprile 2021 *[Proposal for a Regulation laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain unions legisative act,* COM(2021)206 final*]*, all'art. 3 reca la definizione di «sistema di intelligenza artificiale (sistema di IA): un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

[2] A. Mantelero, Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo, in *Il diritto dell'informazione e dell'informatica*, 2012, 135 ss. *Per una prospettiva internazionale volta alla tutela dei diritti* G. Della Morte, *Big Data e protezione internazionale dei diritti umani*, Napoli, 2018. Il concetto di big data è tradizionalmente spiegato facendo ricorso alla teoria delle cc.dd. 5V per indicare che tali dati sarebbero caratterizzati da: Volume (ossia grandi quantità di dati), Velocità (ossia la rapida disponibilità

algoritmi che, pur rappresentando una miniera di informazioni, ha bisogno di strumenti adeguati per poter essere sfruttato in tutto il loro potenziale, quali ad esempio «*modelli e metodi di recupero e filtraggio delle informazioni fondati su tecnologie semantiche e ontologie condivise*»[3].

Peraltro, molte delle nuove tecnologie sono in fase di sviluppo iniziale e non se ne conoscono appieno le implicazioni per individui, ambiente e società. Trattasi di un tema in magmatica evoluzione che mette in crisi il legislatore, per la difficoltà di poter intervenire con una regolamentazione efficace, al netto dell'incertezza sulla capacità dei concetti giuridici tradizionali di cogliere adeguatamente le sfide inedite poste dalle nuove tecnologie[4].

Quanto poi al carattere dell'efficienza, occorre indugiare su un suo aspetto determinante, inerente ai canoni rispetto ai quali possa fondarsi l'assunto della maggiore efficienza della decisione algoritmica. In linea generale, l'efficienza esprime una capacità di rendimento e di rispondenza a determinati fini, quelli scelti in fase di progettazione e sviluppo del sistema intelligente, in quanto tale misurabile con strumenti e metodi oggettivi. In tale prospettiva potremmo ritenere che le finalità impresse ai sistemi intelligenti ne sanciscono anche l'efficienza.

Ma, se spostiamo l'angolo visuale su un altro fronte, ponendoci dalla parte di coloro che sono destinatari, sia individualmente come diretti interessati sia collettivamente come gruppo che subisce gli effetti di decisioni automatizzate, ci rendiamo conto dei limiti di tale assunto: l'efficienza perseguita dai progettisti non sempre collima con i bisogni e le aspettative dei destinatari.

In effetti, nella progettazione degli algoritmi la modellazione prende avvio con la scelta degli obiettivi, in tal senso potremmo dire che gli algoritmi sono ideologicamente orientati, secondo target di efficienza in linea con gli interessi di sviluppatori e progettisti piuttosto che di giustizia, equità o di interesse della comunità[5].

Peraltro, occorre considerare che essi non riflettono in modo incorrotto la realtà anzi, essendo progettati allo scopo di ottenere determinati risultati attesi, si fondano su una pre-determinata rappresentazione della realtà, sotto forma di problemi da risolvere, di variabili incidenti e di parametri opportunamente categorizzati[6].

Siffatto limite si presenta ancor più critico quando i sistemi decisionali automatizzati vengono sviluppati per dare attuazione ad una determinata disposizione legislativa o

---

e analisi degli stessi), Varietà (ossia, da un punto di vista qualitativo, l'enorme tipologia di dati presenti), Variabilità (il contenuto dei dati muta di significato a seconda dell'analisi a cui è sottoposto) e Valore (dipende dal crescente potenziale economico e dalla valenza sociale dei dati).

[3] Sul punto il Libro Bianco dell'Agenzia per l'Italia Digitale del marzo 2018, *L'intelligenza artificiale al servizio del cittadino,* p. 52.

[4] Sul tema M. Bassini - L. Liguori - O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 334. Gli autori riflettono sulle difficoltà dei regolatori nel tenere il passo di questa rapidissima evoluzione tecnologica, evidenziando che occorre «valutare se sia opportuno, per i legislatori, coniare delle regole ad hoc, nuove, ovvero persistere, non senza possibili forzature avallate, magari, sul piano giurisprudenziale, nell'applicazione delle norme preesistenti».

[5] C. O'neil, *Armi di distruzione matematica*, Firenze-Milano, 2017, 190.

[6] A.C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in Rivista di filosofia del diritto, 1, 2019, 109.

amministrativa. Siamo nel campo della dell'informatica giuridica[7], scienza che studia, tra l'altro, se e come si possa pervenire all'applicazione automatica delle norme da parte del computer stesso o, quanto meno, come il computer possa aiutare il legislatore, il giurista, e più in generale qualsiasi operatore del diritto, nella loro attività. In questo campo non si tratta di interpretare la realtà materica ma di utilizzare la regola giuridica come categoria per l'interpretazione della realtà e degli interessi amministrati, non prima di averla tradotta "una volta per tutte" in codici e criteri - privi di ambiguità - che possono esser digeriti da un sistema decisionale automatizzato. Ebbene, tale attività interpretativa determinerà il nascere di una quasi-legislazione "nascosta"[8], con evidente rischio di allontanarsi dal bagaglio di valori, condivisi dalla società in un determinato contesto storico, sintetizzato nella regola giuridica.

Inoltre, quando entrano in gioco algoritmi di *machine learning*, o anche di *deep learning*, capaci del cd. autoapprendimento, le decisioni vengono prese utilizzando dati prodotti dalla macchina medesima, per i quali l'uomo ha difficoltà ad individuare punti di connessione con la realtà. Nel caso delle cd *black box* alcuni passaggi sono invisibili all'esterno e resta imperscrutabile l'uso effettivo che viene fatto degli algoritmi e dei dati[9].

In definitiva, gli esiti di un processo algoritmico derivano da una molteplicità di fattori, non ultimo quello derivante dalla qualità dei dati coinvolti nel training del procedimento automatizzato, per cui discutere di efficienza dei sistemi decisionali automatizzati è riduttivo, così come motivare il loro utilizzo esclusivamente da considerazioni di efficienza o efficacia, se non addirittura in termini di rapporti costi benefici, è arbitrario. Piuttosto, occorre interrogarsi sulle conseguenze che tali sistemi producono sulla vita dell'uomo, sulla salute, sull'ambiente e sulla società, interpretando così l'innovazione tecnologica non soltanto come trasformazione di un processo esistente in chiave di maggiore efficacia ma come sviluppo etico e sostenibile[10] dell'innovazione medesima[11].

È questa la prospettiva per costruire una IA affidabile, in cui un ruolo chiave viene

---

[7] In tal senso vengono alla mente le parole di Borruso che nel delineare i tratti salienti e distintivi della nuova materia di studio "*informatica giuridica*", che si veniva a delineare dagli anni '60 in poi, la indicò come quella in cui il "*diritto diventa oggetto dell'informatica*".

[8] D.W. Schartum, *Law and algorithms in the public domain, in Etikk i praksis*, in *Nordic Journal of Applied Ethics*, 1, 2016, 15 ss. L'autore dimostra che nello sviluppo di un algoritmo deputato a dare attuazione a una norma di legge l'algoritmo finisce per contenere un livello normativo clandestino.

[9] F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge - London, 2015; D. Pedreschi et al., *Meaningful Explanations of Black Box AI Decision Systems*, 33rd AAAI Conference on Artificial Intelligence (AAAI 2019), 33, 9780 ss.; L. Vigano - D. Magazzeni, *Explainable Security*, 2018.

[10] Indispensabile, anche se non sufficiente, un approccio che dia rilevanza all'etica come argine alle criticità dei sistemi intelligenti. In tal senso si veda la Risoluzione del Parlamento Europeo del 20 gennaio 2021 sull'intelligenza artificiale, secondo cui «…gli orientamenti in materia di etica, quali i principi adottati dal gruppo di esperti ad alto livello sull'intelligenza artificiale, costituiscono un buon punto di partenza ma non sono sufficienti per garantire che le imprese agiscano in modo equo e assicurino una protezione efficace degli individui».

[11] Il Consiglio per i diritti umani delle Nazioni Unite, il 22 marzo 2017, ha osservato con preoccupazione «…che il trattamento automatico dei dati personali per la profilazione individuale può portare a discriminazioni o decisioni che altrimenti potrebbero incidere sul godimento di diritti umani, compresi i diritti economici, sociali e culturali».

riconosciuto al principio di trasparenza[12]. Nelle pagine a seguire si procederà ad una disamina di tale principio in chiave di rivisitazione, abbandonando la tentazione di interpretarlo come mero strumento per la comprensione del funzionamento dei sistemi automatizzati[13] - spesso indecifrabili per l'uomo - e ricostruendolo invece come mezzo per acquisire consapevolezza circa le conseguenze del loro utilizzo[14] e per garantire che il consenso diventi un momento di partecipazione dell'interessato allo sviluppo della sua identità digitale.

2. La trasparenza delle decisioni automatizzate secondo la normativa europea del regolamento (UE) 679/2016

Attualmente il tema della trasparenza dei processi decisionali automatizzati trova una sua puntuale disciplina all'interno del Regolamento Europeo sulla Protezione dei Dati Personali, regolamento (UE) 679/2016 (da ora in poi anche GDPR), in cui rintracciamo sia principi generali validi ad orientare il comportamento degli attori della protezione dei dati, sia specifiche disposizioni sui sistemi decisionali automatizzati[15]. Il paradigma concettuale è rappresentato dagli artt. 12, 13, 14, 15 e 22 del GDPR, in cui risultano condensati i principi di trasparenza, di non esclusività della decisione auto-

[12] Si possono certamente menzionare la "*Raccomandazione sull'intelligenza artificiale*" emanata dall'Organisation for Economic Co-operation and Development nel maggio 2019, e la Carta etica sull'uso dell'intelligenze artificiale nei sistemi giudiziari, adottata nel contesto del Consiglio d'Europa dall'European Commission for the Efficiency of Justice (CEPEJ), nel dicembre del 2018, che si occupa di definire i principi che i responsabili politici, i legislatori e i professionisti dovrebbero adottare nell'affrontare il rapido sviluppo dell'intelligenza artificiale nel campo della giustizia e, più in particolare, nei sistemi giudiziari nazionali. La Commissione europea nella Communication "Building Trust in Human-Centric Artificial Intelligence", COM(2019)168 final, 8 aprile 2019, ha sostenuto i requisiti fondamentali stabiliti negli Orientamenti etici per una Intelligenza artificiale affidabile predisposto dal Gruppo di Alti esperti sull'IA.

[13] Il tema della trasparenza assume un rilievo diverso nell'ambito del processo di digitalizzazione della pubblica amministrazione, funzionale ad un'inclusione di cittadini e imprese, a garanzia della loro partecipazione democratica al funzionamento dello Stato. In tale scenario, il ricorso ad esempio all'automazione delle decisioni amministrative rende prevalente l'esigenza di poter sindacare la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della "regola" che governa l'algoritmo. Sull'argomento sia consentito richiamare a G. Fasano, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica,* in questa *Rivista*, 3, 2019, 234 ss.

[14] Si veda, al riguardo, la recente legge francese sulla bioetica che ha imposto oneri informativi non soltanto sul funzionamento dei sistemi algoritmici ma anche «*de l'interprétation qui en résulte*», Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique, in particolare l'art. 17 che interviene a integrare il Codice della Sanità Pubblica.

[15] Sul tema delle decisioni automatizzate il GDPR può esser letto come il *trait d'union* tra la il primo trattato internazionale in materia di protezione dei dati personali, la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, nota anche come Convenzione 108, e la più recente Proposta di regolamento sull'utilizzo dei sistemi di intelligenza artificiale (IA,) diffusa dalla Commissione europea il 21 aprile 2021, cit. Il primo (con il successivo protocollo di modifica cd. Convenzione 108+) rappresenta uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali, poiché è l'unico strumento giuridicamente vincolante aperto anche a Stati non membri del Consiglio d'Europa. Il regolamento proposto in sede UE è destinato a disciplinare qualsiasi sistema di intelligenza artificiale anche qualora non sia previsto l'"utilizzo di dati personali.

matizzata e del consenso, tutti collegati tra di loro al fine di consentire all'interessato un controllo sui propri dati[16].

La prescrizione generale è introdotta nell'art. 12 del GDPR, il quale comporta l'obbligo per il titolare del trattamento di fornire all'interessato le informazioni relative al trattamento «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro»[17]. Il contenuto informativo da portare a disposizione dell'interessato riguarda, in particolare, l'identità del titolare del trattamento e le finalità del trattamento nonché i rischi, le garanzie e i diritti relativi al trattamento dei dati personali che gli interessati possono esercitare.

Passando al livello ulteriore delle decisioni automatizzate, la disciplina della trasparenza diventa più rigorosa: il titolare del trattamento ha l'obbligo di notificare all'interessato alcune informazioni ulteriori, quali «l'esistenza di un processo decisionale automatizzato» nonché a fornire «informazioni significative sulla logica utilizzata» e «l'importanza e le conseguenze previste di tale trattamento per l'interessato»[18]. L'art. 22 GDPR cita espressamente la profilazione quale fenomeno da ricondurre sotto la disciplina delle decisioni automatizzate, probabilmente perché si tratta dell'applicazione più diffusa nella pratica e che viene definita dall'art. 4 del GDPR come qualsiasi forma di trattamento automatizzato di dati «effettuato per valutare aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

La *ratio* di tali previsioni può esser ricondotta alla libertà di autodeterminazione delle persone[19], concetto che negli ultimi tempi, per via dell'incessante diffondersi di nuove tecnologie e delle relazioni che si istaurano tra queste ultime e le persone, è andato ad arricchirsi di nuovi significati. Se tradizionalmente esso poteva esser concepito nella

---

[16] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 34. Per l'Autore «si può dire che oggi la sequenza quantitativamente più rilevante è quella "persona-informazione-circolazione-controllo", e non più soltanto "persona-informazione-segretezza", intorno alla quale è stata costruita la nozione classica di privacy. Il titolare del diritto alla privacy può esigere forme di "circolazione controllata", e non solo interrompere il flusso delle informazioni che lo riguardano». Il Gruppo di lavoro Articolo 29 lega la libertà del consenso alla possibilità di avere il controllo dei dati personali, sostenendo che «Se ottenuto nel pieno rispetto del regolamento, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano», Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, 3.

[17] Per maggiori approfondimenti, Gruppo di lavoro Articolo 29, *Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679*, 11 aprile 2018, 6.

[18] Art. 13, par. 2, lett. f, e dell'art. 14, par. 2, lett. g, del GDPR. In forza del considerando 63 ogni interessato deve poter ottenere dal titolare del trattamento informazioni in particolare in relazione «alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento».

[19] S. Mangiameli, *Autodeterminazione: diritto di spessore costituzionale?*, in C. Navarini (a cura di), *Autonomia e autodeterminazione - Profili etici, bioetici e giuridici*, Roma, 2011, l'autore afferma che «la Costituzione non parla di autodeterminazione in alcuna delle sue disposizioni, e ciò nonostante che la nozione di persona, nelle sue diverse aggettivazione (personale, personalità), sia richiamata 21 volte, quella di uomo (o umano) ben 9 volte, in alcuni casi in reciproca combinazione (nell'art. 3, comma 2, e nell'art. 32, comma 2, Cost.) e la dignità è richiamata due volte (nell'art. 3, comma 1, come dignità sociale, e nell'art. 41, comma 2, come dignità umana)».

prospettiva dell'esercizio di un diritto, sulla base di un rafforzato onere informazionale in capo al titolare, finalizzato a garantire la liceità del trattamento dei dati personali, oggi l'autodeterminazione deve essere intesa come consapevolezza del condizionamento proveniente dall'altrui trattamento dati, e quindi come limite ai diritti e alle libertà degli interessati[20].

Quella stessa libertà che poi sostanzia la principale eccezione al divieto di esser sottoposto a una decisione basata unicamente sul trattamento automatizzato, vale a dire il consenso dell'interessato (art. 22, par. 2, lett. c) del GDPR). Si rileva come in precedenza la deroga del consenso esplicito dell'interessato non era prevista dall'abrogato art. 15 della direttiva 95/46/CE riguardante le «decisioni individuali automatizzate» e il suo inserimento nel GDPR deve ricondursi al ruolo centrale che viene attribuito al consenso nel modello di protezione dei dati dell'Unione europea: il consenso non solo rappresenta una delle basi giuridiche per assicurare la legittimità del trattamento dei dati personali (art. 6 GDPR) ma esprime il momento di libertà in cui la persona si assoggetta a un meccanismo decisionale automatizzato.

Resta però il dubbio che il consenso , quale costrutto giuridico, sia adeguato ad assicurare una protezione efficace contro i moderni processi decisionali automatizzati, considerato il rischio per l'interessato di raggiungere quel grado di consapevolezza indispensabile per esercitare un effettivo controllo sui propri dati. E ciò, per una serie di ragioni.

Nel campo della profilazione, settore applicativo in cui è più diffuso l'uso di sistemi decisionali automatizzati, spesso le conseguenze del processo medesimo sono invisibili all'interessato, nel senso che, comunicatagli l'esistenza del processo stesso, come prescritto dall'art. 13, co. 2, lett. f), l'elaborazione dei dati porta alla creazione di dati personali "nuovi", cioè dati inferenziali, la cui caratteristica è nel non esser forniti direttamente dagli interessati ma esser da essi derivati o desunti osservandone il comportamento. E anche partendo da dati qualificati anonimi o, comunque, non personali è possibile ricavare dati personali[21]. Rispetto a tali dati derivati non può esservi alcuna consapevolezza da parte dell'interessato[22] e, per conseguenza, nessuna forma di controllo da parte sua. La preoccupazione principale deriva dal rapporto di tali dati inferenziali rispetto allo sviluppo di nuove tecnologie, poiché più accelera il processo trasformazione digitale più aumenterà la produzione di dati inferenziali rispetto a quelli coperti dal consenso.

Connesso al fenomeno di dati inferenziali v'è che la trasparenza decisionale è solitamente concepita come trasparenza *ex ante*, nel senso che il titolare del trattamento

[20] M.S. Esposito, Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali, in Diritto dell'Informazione e dell'Informatica, 2019, 1071, sostiene che il «crescente ricorso ai dati ed alla loro elaborazione mediante algoritmi a fini decisionali può tuttavia condurre a conseguenze negative per i diritti e le libertà dei soggetti coinvolti, incidendo sulla libertà di autodeterminazione e sul diritto al rispetto della dignità umana ai medesimi riconosciuti».

[21] Al riguardo N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law, in Law, Innovation and Technology, 10(1), 2018, 40 ss.*

[22] Sull'argomento si veda C.B. Parker, *New Stanford research finds computers are better judges of personality than friends and family*, in *news.stanford.edu,* 12 gennaio 2015. La nuova ricerca di Stanford rileva che i computer giudicano meglio la personalità di amici e familiari.

informa in anticipo l'interessato che utilizzerà i suoi dati per un processo decisionale automatizzato. La mancanza di un'attività di *reporting*, che realizzerebbe una trasparenza post trattamento, conduce alla mancanza di consapevolezza circa le conseguenze effettive del trattamento automatizzato che, in alcuni casi, nemmeno il titolare era in grado di aspettarsi.

A ciò si aggiunga che le persone hanno gradi diversi di comprensione e nell'ambito delle nuove tecnologie è ancor più difficile esercitare l'arte del comprendere, trattandosi spesso di esperienze inedite per l'uomo e soprattutto in continua evoluzione[23]. Per alcune persone potrebbe essere difficile comprendere le logiche utilizzate nei processi decisionali automatizzati, peraltro sempre più complesse ed oscure[24]. Ciò determina l'inadeguatezza dell'adozione, da parte del titolare del trattamento, di un unico livello di trasparenza che possa raggiungere l'obiettivo della conoscenza e della consapevolezza indistintamente per tutti gli interessati.

Se ciò non bastasse, si consideri che spesso i processi automatizzati sono annidati all'interno delle cd *black box*, rispetto alle quali non si è sempre in grado di cogliere con esattezza quale sia il processo seguito dall'algoritmo per produrre il risultato finale. Un ulteriore freno alla conoscenza del processo interno deriva da esigenze di tutela della proprietà intellettuale, necessaria al fine di garantire la segretezza del know-how tecnico di un determinato sistema che verrebbe ingiustamente pregiudicata se l'algoritmo venisse reso accessibile, conoscibile e quindi divulgabile a chiunque.

Per tali ragioni non possiamo considerare *tout court* garantito il controllo dell'interessato sulla propria sfera informazionale e, di conseguenza, non possiamo considerare soddisfatti quei canoni di libertà al cui presidio è posto il principio di trasparenza.

Ma v'è di più. La carenza di un effettivo controllo sulla propria sfera informazionale si manifesta anche sotto altro aspetto, quella di un controllo senza partecipazione dell'interessato, di guisa da impedirgli di essere partecipe della individuazione della "parte disponibile" del proprio patrimonio informativo.

Al riguardo possiamo rilevare che le informative sempre più spesso sono dirette a tutelare il titolare del trattamento, piuttosto che l'interessato[25]. Quest'ultimo, al di là della difficoltà nel leggere e comprenderne il testo, è in una posizione debole non potendo negoziare nessun aspetto del trattamento, né di quali dati personali disporre né in che modalità. A rigori, più che di consenso sarebbe corretto parlare di un assenso al trattamento, inteso quale atto con cui si aderisce, più o meno scientemente, a un'impostazione già perfezionata da altri. In tal senso depone anche l'art. 4, n. 11), del GDPR che

[23] Nelle linee guida del Gruppo di lavoro Articolo 29 si pone in evidenza che «le persone fisiche hanno gradi diversi di comprensione e per alcune potrebbe essere difficile comprendere le complesse tecniche coinvolte nella profilazione e nei processi decisionali automatizzati»: *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018, 10.

[24] La criticità deriva non soltanto dalla diffusione di cd *black box* quanto dalla scarsa diffusione nella società di competenze digitali, settore in cui l'Italia è ancora in una posizione di svantaggio rispetto agli altri paesi avanzati, stando ai risultati del Rapporto Annuale 2020 dell'Istituto Nazionale di Statistica (*Rapporto annuale 2020. La situazione del Paese,* Istat, 3 luglio 2020).

[25] Pure se dettata nell'ambito della responsabilità medica in tema di cure è rilevante, per il suo contenuto assiologico che può esser esteso alla presente indagine, l'osservazione della Cass. Civ., sez. III, 9 febbraio 2010, n. 2847, p.to 3.4, secondo cui non è il consenso ad essere informato ma è l'interessato a dovere essere informato, cioè capace di aver compreso ciò a cui ha dato l'assenso.

definisce il consenso come una manifestazione di volontà libera, specifica, informata e inequivocabile con cui l'interessato «manifesta il proprio assenso» al trattamento deciso - in tutto e per tutto - dal titolare del trattamento: l'unico spazio di decisione che gli residua è rappresentato dalla scelta di non aderire. Uno scenario che non appartiene al paradigma del consenso, caratterizzato sul piano generale del diritto dall'incontro delle volontà di due o più soggetti che si contrappongono da posizioni formali analoghe e giungono a una composizione di interessi. Sul piano più settoriale della tutela dei dati personali, tale paradigma dovrebbe tradursi in un processo che riproduca un dialogo tra titolare e interessato, attraverso cui entrambi possano giungere, grazie all'esercizio di poteri omogenei, alla composizione dei reciproci bisogni.

Dunque, il fenomeno si caratterizza non soltanto per la difficoltà di raggiungere quel grado di consapevolezza indispensabile per esercitare un effettivo controllo sulla propria sfera informazionale, che potremmo definire asimmetria informativa, ma per l'impossibilità dell'interessato di partecipare alla individuazione della "parte disponibile" del patrimonio informativo, che caratterizza una tipica situazione di asimmetria di poteri.

Tali condizioni, non solo portano a compromettere il controllo dell'interessato sulla propria sfera informazionale ma, correlato ad un indiscriminato utilizzo degli stessi da parte di terzi, determinano una ricaduta sul livello di libertà di cui una persona può beneficiare[26], ciò in quanto il controllo sul proprio patrimonio informativo è un mezzo per assicurare all'individuo una protezione a tutela della «persona nella sua interezza»[27].

In effetti, con l'ingresso dell'individuo nell'economia digitale, caratterizzata da una rapidità dell'evoluzione tecnologica e dalla globalizzazione, aumentano significativamente la condivisione e la raccolta di dati personali. Ed ecco che il regolamento, nella prospettiva di assicurare l'effettività delle libertà classiche dell'individuo nel contesto dello sviluppo dell'economia digitale in tutto il mercato interno, enfatizza la stretta alleanza esistente tra la protezione dei dati e gli altri diritti fondamentali, incoraggiando la visione della *data protection* come ausilio delle libertà classiche[28]. In questo senso, la protezione dei dati si colloca a supporto degli altri diritti[29] e, grazie a questi, alla base

[26] Nell'ambito della 41st International Conference of Data Protection and Privacy Commissioners tenutasi a Tirana dal 21 al 24 ottobre 2019, è stata adottata la *International resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights*, per la quale «*the right to privacy as a fundamental right and its role in both informing and serving as a foundation to other inalienable rights*» e si rileva che «*privacy is a precondition for citizens' other freedoms as well as a keystone right for democracy and personal and social development*». Il considerando 4 del regolamento (UE) 2016/679 chiarisce che «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma […] va contemperato con altri diritti fondamentali».

[27] Cfr. C. Colapietro - A. Moretti, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali,* in *BioLaw Journal – Rivista di BioDiritto*, 3, 2020, 379.

[28] Il diritto dell'interessato al controllo delle proprie informazioni è tradizionalmente ricondotto alla libertà e segretezza della corrispondenza e di ogni altro mezzo di comunicazione, espressamente qualificate dall'art. 15 della Costituzione come diritto inviolabile, ed esso attiene, a voler usare la parola della Consulta del 91, «al nucleo essenziale dei valori di personalità» senza i quali la persona «non può esistere e svilupparsi in armonia con i postulati della dignità umana» (Corte Cost., sent. 366/1991).

[29] C. Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy,* Napoli, 2018, 34, secondo cui la privacy «assume il carattere di "garanzia presupposto" dell'esercizio di altri diritti fondamentali, al fine

dello sviluppo e della realizzazione personale[30].
Si comprende allora come un affievolimento del principio di trasparenza, che dovrebbe assicurare quel grado irrinunciabile di autonomia e di libertà di autodeterminazione correlate al proprio patrimonio informativo, si traduce in un indebolimento di una garanzia posta a presidio di tutte le libertà tradizionali[31].

3. Il principio di non esclusività della decisione automatizzata

Corollario del principio di trasparenza è il principio di non esclusività della decisione automatizzata, sancito nell'art. 22 del GDPR, secondo cui «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[32].
Si tratterebbe di un divieto rivolto al titolare del trattamento, nell'ottica della tutela *by default* sancita dal GDPR, senza la necessità che per la sua applicazione l'interessato sia onerato di un qualche comportamento. Almeno sul piano teorico.
Tuttavia, già nella sua formulazione, il principio porta con sé due condizioni "limitanti" che lo costringono a recedere quando: il trattamento automatizzato è accompagnato da un intervento umano; la decisione che ne scaturisce non incide in modo significativo sulla persona. Dunque, non siamo in presenza di un principio di carattere assoluto e l'atteggiarsi in concreto delle sue eccezioni consente di indugiare sulla sua effettiva efficacia applicativa.
Quanto al primo aspetto, quello dell'intervento umano, non è dato intendere come esso possa esser misurato per poterlo comparare all'altro elemento del trattamento automatizzato, al fine di stabilire in quale misura l'uno sia prevalente sull'altro e se, in definitiva, la decisione possa esser considerata lecita, cioè non basata «unicamente» sul trattamento automatizzato.
Senza considerare le difficoltà di valutare quelle ipotesi in cui l'intervento umano assu-

di rendere possibile lo sviluppo della persona, l'esplicazione reale ed effettiva delle sue libertà».

30 S. Wachter, *Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights*, 2017, 19-21, secondo cui la privacy è la base per lo sviluppo e la realizzazione personale e «*Notwithstanding that other human rights play an important role in our society, it is privacy that is needed to fully exercise many of them*».

31 Sul punto si rinvia a F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, I, Torino, 2016, 9-10, il quale afferma che «nella società digitale e delle comunicazioni elettroniche il diritto fondamentale alla protezione dei dati diventa anche il presidio irrinunciabile di tutte le libertà classiche delle nostre Costituzioni» e che «rinunciare alla protezione dei dati personali da ogni indebita ingerenza, significa rischiare di vanificare ogni forma di libertà e mettere in pericolo tutti i diritti fondamentali»; nonché a L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, 16, che evidenzia come la protezione dei dati personali concorra a realizzare una piena valorizzazione e garanzia sia della dignità umana sia della società democratica: in particolare, «il diritto fondamentale alla protezione dei dati diviene anche presidio irrinunciabile di tutte le altre libertà classiche costituzionalmente garantite, cioè funzionale al loro esercizio e, in ultima analisi, funzionale alla difesa della nostra stessa società democratica».

32 Art. 22, par. 1, del GDPR.

ma le connotazioni di un elemento marginale, se non addirittura fittizio.

Anche l'aspetto incidenza del trattamento sulla persona non è di facile valutazione. Anzitutto, la stessa formulazione del principio di non esclusività non esprime criteri oggettivi attraverso cui valutare quando un trattamento automatizzato sia destinato ad incidere «significativamente» sulla persona dell'interessato[33]. E, in mancanza, si è costretti a ricorrere a criteri soggettivi, cioè ad affidare siffatta valutazione al titolare del trattamento. Ma, la sua valutazione sarà comprensibilmente rivolta ad uno standard di tutela in cui non tutte le persone potrebbero identificarsi, per via dei loro differenti gradi di vulnerabilità e per via del fatto che il concetto di dignità della persona non è comprimibile in standard omogenei, per cui l'interessato si troverebbe costretto a dover eccepire le proprie ragioni opponendosi alla decisione automatizzata. E ciò potrà avvenire soltanto *ex post*, a decisione assunta e sacrificio ormai prodotto.

Per di più, ci sono casi in cui la incisività della decisione automatizzata è celata agli occhi dell'interessato per cui viene a mancare anche quell'ultimo baluardo di garanzia rappresentato dall'autodifesa. Si pensi alla pubblicità mirata che, apparentemente non incisiva dal momento che può essere ignorata, influenza il punto di vista e la libertà di scelta degli utenti. Attraverso messaggi inviati ai singoli individui, e personalizzati grazie a sofisticati modelli predittivi computazionali di *microtargeting*[34], di cui la maggior parte degli utenti ignora l'esistenza e il funzionamento, si creano delle vere e proprie *filter bubbles*[35], ovvero delle bolle in cui l'utente viene rinchiuso ricevendo soltanto informazioni conformi alle proprie opinioni e pregiudizi[36].

Ecco perché sul piano applicativo l'efficacia di tale principio è discutibile, a prescindere dai casi di aggiramento voluto del principio di non esclusività[37]. Per tali ragioni si è fatta

---

[33] Un'indicazione viene fornita nei considerando (71) laddove si cita a titolo esemplificativo «il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani». Anche il Gruppo di lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 24, è intervenuto sull'argomento, enucleando quali situazioni significative quelle che influenzano le condizioni finanziarie di una persona (ammissibilità al credito), ovvero l'accesso ai servizi sanitari, che negano un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio; decisioni che influenzano l'accesso di una persona all'istruzione, ad esempio le ammissioni universitarie.

[34] Il *microtargeting* è una tecnica che analizza i dati personali per prevedere gli interessi di un pubblico specifico: una pratica che costituisce il modello di business fondamentale di diverse grandi piattaforme di social media e che è diventata nota al grande pubblico con lo scandalo Cambridge Analytica del 2016.

[35] E. Pariser, *The filter bubble: What the Internet is hiding from you,* London, 2011, e più di recente K. Shaffer, *Data versus Democracy: How Big Data Algorithms Shape Opinions and Alter the Course of History, Apress*, Colorado, 2019; E. Longo, *Dai big data alle «bolle filtro»: nuovi rischi per i sistemi democratici,* in *Percorsi costituzionali*, 2, 2019, 29 ss.; R. Montaldo, L*e dinamiche della rappresentanza tra nuove tecnologie, populismo, e riforme costituzionali*, in *Quaderni costituzionali,* 4, 2019, 790 ss.

[36] Sulla questione si è pronunciato anche il garante della protezione dei dati dell'UE (GEPD) sulle proposte della Commissione europea per il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA), per il quale «Data la moltitudine di rischi associati alla pubblicità mirata online, il GEPD esorta i colegislatori a prendere in considerazione norme aggiuntive che vadano oltre la trasparenza».

[37] La Commissione europea, nella *Communication "Building Trust in Human-Centric Artificial Intelligence*", COM(2019)168 final, 8 aprile 2019, 4, al fine di circoscrivere uno spazio di intervento dell'uomo ha individuato almeno tre diverse intensità: "*Human-in-the-loop*" l'intervento umano in ogni ciclo decisionale del sistema; "*Human-on-the-loop*" l'intervento umano a monte del design del sistema e durante il suo funzionamento; "*Human-in-command*" l'intervento capace di decidere come e quando usare l'IA in una situazione particolare. V. anche D. Amoroso – G. Tamburrini, *I sistemi robotici ad autonomia crescente tra etica*

strada una interpretazione sostanziale del principio di non esclusività, nel senso di considerare soddisfatto il principio laddove l'intervento dell'essere umano non è solamente formale ma esprime una vera e propria valutazione attiva[38]. Nello stesso senso si è mosso anche il Parlamento Europeo che nella Risoluzione sugli aspetti etici dell'IA (20 ottobre 2020) evidenziano che nei casi in cui siano in gioco le libertà fondamentali gli Stati membri dovrebbero ricorrere a tali tecnologie soltanto «quando sono possibili o sistematici un intervento e una verifica sostanziali da parte dell'uomo». Analoga stretta si rintraccia nella giurisprudenza più recente del TAR Lazio, il quale ha relegato l'uso di decisione completamente automatizzare nell'ambito dell'istruttoria amministrativa ad un «ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo»[39].

La consapevolezza che si tratta di una previsione di difficile interpretazione ha reso l'interprete consapevole che nella pratica possano rinvenirsi situazioni di non facile qualificazione. Per tale ragione il Gruppo di lavoro Articolo 29 ha identificato almeno due elementi da considerarsi rappresentativi di un intervento umano: vale a dire che il coinvolgimento umano sia opera di «una persona che dispone dell'autorità e della competenza per modificare la decisione» e che «tale persona dovrebbe prendere in considerazione tutti i dati pertinenti»[40]. Resta, tuttavia, il dubbio di come una persona, per quanto autorevole e competente, possa «prendere in considerazione tutti i dati pertinenti» che soltanto sofisticati sistemi di IA sono in grado di analizzare ed elaborare.

Sebbene venga prestata notevole attenzione affinché i trattamenti automatizzati non siano affidati soltanto all'algoritmo ma contemplino anche un effettivo coinvolgimento umano e nonostante gli sforzi interpretativi a ciò dedicati, l'effettività del principio stesso resta nel dubbio, complice anche la «travolgente forza pratica dell'algoritmo»[41], quella capacità dell'algoritmo di indurre la persona coinvolta ad affidarsi e a delegare per intero l'attività valutativa e decisionale assegnatale.

Per arginare il rischio di vanificare l'effettività del principio, il Parlamento Europeo si è mosso nella direzione di ritagliare alle decisioni automatizzate un ruolo di supporto o

e diritto: quale ruolo per il controllo umano?, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 33 ss., 51.

[38] L.A. Bygrave, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, in *Computer Law & Security Review*, 17, 2001, 20; G. Malgieri - G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law,* 7(4), 2017, 251.

[39] Vedi Tar Lazio, sez. III-bis, 10 settembre 2018, n. 9227, in cui si stabilisce che «le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere». Sul rapporto tra PA e IA, D.U. Galetta - J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019. Sia consentito infine richiamare G. Fasano, *L'intelligenza artificiale nella cura dell'interesse generale*, in *Giornale di Diritto Amministrativo,* 6, 2020, 715 ss.

[40] Gruppo di lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 23.

[41] A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 81, che puntualizza come tale forza non dipenda da ragioni di valore scientifico, di accuratezza predittiva o di affidabilità tecnica dell'automatismo, ma – appunto – da mera convenienza pratica.

strumentale alla decisione presa dall'agente umano, almeno in ambiti particolarmente delicati come quello medico. In effetti, nel campo dell'assistenza sanitaria l'intelligenza artificiale svolge un ruolo sempre più cruciale, si pensi agli algoritmi di supporto alla diagnosi, la chirurgia robotica, le protesi intelligenti e i robot sociali per l'assistenza agli anziani la cui diffusione potrebbe inficiare la parità di trattamento dei pazienti in termini di accesso alle cure e alterare il rapporto tra paziente e medico. Nella Risoluzione del 20 gennaio 2021 il Parlamento ha voluto stigmatizzare la responsabilità del professionista evidenziando come egli deve aver sempre presente la possibilità di discostarsi dalla soluzione proposta dall'IA[42]. La questione viene così affrontata dal punto di vista della responsabilità, quasi a monito di un utilizzo spesso ossequioso e conformativo alle risultanze del sistema automatizzato.

In esito a questa breve analisi, pare evidente che il principio di non esclusività, inestricabilmente connesso a quello della trasparenza, si presti ad esser poco efficace come garanzia dei diritti e libertà fondamentali, e non soltanto per via dei suoi connaturati limiti strutturali ma anche a causa della presenza di numerose cause derogatorie che ne indeboliscono la portata effettiva, prima tra tutte, l'eccezione del consenso.

4. Le eccezioni al principio di non esclusività: il consenso

Come anticipato, il GDPR prevede delle eccezioni al divieto di decisioni completamente automatizzate, quali la loro necessità per la conclusione o l'esecuzione di un contratto, l'autorizzazione da parte del diritto dell'UE o dello Stato membro[43], oppure il consenso esplicito dell'interessato. La presenza di tali e tante eccezioni, molto frequenti nella pratica, rende il principio di non esclusività, di fatto, un principio debole.

Tra queste eccezioni il consenso del soggetto destinatario della decisione automatizzata presenta la principale criticità, imponendo di riflettere sulla sua efficacia di fronte alla forza di questi meccanismi[44].

Per un verso, occorre riconoscere che il principio del consenso, nell'ecosistema introdotto dal GDPR, rappresenta uno dei pilastri su cui si fonda l'intera disciplina europea sulla protezione dei dati: oltre ad esser annoverato quale prima condizione di liceità del trattamento (art. 6), viene rappresentato come momento di manifestazione di una «intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano» (considerando 32)[45].

[42] Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale, par 65. In tal senso si veda anche l'art. 11 della Loi n° 2021-1017 cit.

[43] I. Mendoza - L. A. Byg Rave, *The Right Not to be Subject to Automated Decisions Based on Profiling*, in T. Synodinou - P. Jougleux - C. Markou - T. Prastitou (eds.), *EU Internet Law. Regulation and Enforcement*, London, 2017, 95, osservano che la possibilità per la legislazione nazionale di legalizzare specifici trattamenti interamente automatizzati incide sull'obiettivo del regolamento (UE) 2016/679 di favorire una maggiore armonizzazione della disciplina tra gli Stati membri.

[44] Si rileva come la deroga del consenso esplicito dell'interessato, riconosciuta all'art. 22, par. 2, lett. c) del regolamento (UE) 2016/679, non era prevista in precedenza all'interno dell'abrogato art. 15 della direttiva 95/46/CE riguardante le "Decisioni individuali automatizzate".

[45] La centralità del ruolo del consenso ha tradizionalmente ispirato gli stessi padri della privacy, S. D. Warren - L. Brandeis, *The Right to Privacy*, in *Harvard Law Review,* 4(5), 1890, 193 ss. Stefano Rodotà

Nell'ambito dei sistemi decisionali automatizzati, inoltre, il consenso dell'interessato acquisisce una differente e maggiore portata: il principio del trattamento trasparente comporta una dilatazione degli oneri informativi, per cui non è sufficiente che l'interessato riceva informazioni sull'esistenza del trattamento e sulle sue finalità, egli deve esser destinatario di «informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato» (art. 13, par 2, lett. f) e art. 14, par 2, lett. g)). Ecco che la trasparenza, e dunque il consenso che sulla base di essa viene espresso, involve aspetti inediti ampliando la portata della manifestazione di volontà, in vista della realizzazione piena dell'autodeterminazione informativa. Tuttavia, tale scopo rischia di cedere a fronte di meccanismi altamente sofisticati in cui le decisioni automatizzate non lasciano comprendere la loro rilevanza in termini di compressione delle libertà fondamentali.

Ciò accade per una serie di ragioni. *In primis*, la finalità del trattamento e l'uso che potenzialmente potrebbe esser fatto dei dati rischiano di non essere determinabili al momento iniziale di espressione del consenso alla raccolta, o comunque a priori, vincolando il consenso ad una prospettazione infedele delle finalità e dell'utilizzo dei dati. In tale condizione non potrebbe esprimersi un consenso consapevole. Si pensi ai sistemi di machine learning, i quali generano essi stesi nuovi dati, rispetto ai quali non può esservi spazio per alcun consenso, visto che al momento della raccolta, momento in cui va espresso un consenso consapevole, quei dati non esistono.

La valutazione circa «l'importanza e le conseguenze» del trattamento automatizzato non può esser frutto dell'analisi solitaria effettuata da una sola parte e, peraltro, in chiave meramente prospettica. Il principio dell'autodeterminazione è declinato, ancora una volta, come assenso ad un'attività valutativa - foriera della decisione finale - rimessa ad esclusivo appannaggio del titolare del trattamento dati. Ma, senza la partecipazione attiva dell'interessato, con la sua unicità, con le sue vulnerabilità, con la sua identità dignitaria[46], non può giungersi ad una prospettazione verosimile circa l'importanza e le conseguenze del trattamento automatizzato. Sulla base della quale, questa volta sì, si può esprimere un consenso informato.

La stessa complessità dei sistemi di IA non è d'aiuto in termini di esercizio dell'autodeterminazione, considerata la difficoltà di comprendere le conseguenze di un trattamento quando i dati sono destinati ad essere processati con sistemi di IA di cui si ignorano le logiche di funzionamento interno. Si parla di *black box* per indicare quei processi automatizzati che impediscono di comprendere il funzionamento, rendendo le decisioni imperscrutabili e indecifrabili – non solo - per il destinatario. In ragione di ciò, l'interessato finisce per ricevere informazioni generiche sulle modalità di elaborazione dei propri dati ovvero indicazioni talmente tecniche da risultare incomprensibili. E la mancata comprensione si traduce in un mancato controllo su tali sistemi.

La complessità si manifesta anche per effetto dei livelli di sofisticatezza raggiunti da

considerava il consenso la massima espressione del controllo da parte dell'individuo sulle proprie informazioni, S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Bari, 2004.

[46] A. Oddenino, *Decisioni algoritmiche e prospettive internazionali di valorizzazione dell'intervento umano*, in *DPCE online*, 2020, 1, 213, il quale identifica «la dignità umana come elemento fondativo dello stesso concetto di privacy».

alcuni sistemi, si pensi alle tecniche di profilazione e di predizione che da dati apparentemente neutrali possono ricavare dati sensibili. Recenti studi hanno dimostrato come, grazie alle tecniche di correlazione statistica, analizzando i semplici *like* di Facebook è possibile desumere con una ragionevole certezza informazioni sulla personalità dei singoli individui[47], cioè a dire orientamento sessuale, politico e religioso.

In tali circostanze l'asimmetria informativa non è tanto un condizionamento nell'esercizio di un potere, quello sottostante il consenso, bensì un vero e proprio stato di soggezione in cui sono relegati gli interessati al trattamento dei dati[48].

A tentare di porre rimedi a tali criticità è intervenuto anche il Gruppo di lavoro Articolo 29[49] ma, ancora una volta, la soluzione è stata individuata attorno all'istituto del consenso onerando il titolare del trattamento, che voglia basare la profilazione sul consenso, di un obbligo specifico, quello di «dimostrare che gli interessati comprendono esattamente a cosa stanno acconsentendo».

Resta evidente la difficoltà operativa di tale misura, in primis, poiché non vi sono elementi oggettivi di misurazione del grado di consapevolezza e, inoltre, perché qualora il titolare non riesca a fornir prova della consapevolezza raggiunta dagli interessati le conseguenze nocive di un trattamento automatizzato rimarrebbero in piedi, riversandosi sulla parte debole del rapporto e determinando una lacuna nella tutela effettiva degli interessati. Consapevole di ciò, lo stesso Gruppo di lavoro rammenta che «il consenso non è sempre una base appropriata per il trattamento», con ciò riconoscendo i suoi limiti intrinseci sul piano delle tutele effettive.

La preoccupazione che il principio del consenso possa non bastare come tutela nell'ambito delle decisioni automatizzate è stata presente anche nel legislatore unionale. Per tale ragione viene ampliato il novero degli obblighi assegnati al titolare del trattamento. In effetti, la prescrizione unionale impone a questi l'adozione di «misure appropriate» ulteriori rispetto al consenso per tutelare i diritti, le libertà e i legittimi interessi dell'interessato qualora si proceda al trattamento automatizzato, specificando che il corredo minimo di tali garanzie sia costituito dal «diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione».

Tradurre tali «misure appropriate» sul piano concreto non è affatto scontato. A partire dalla garanzia circa l'intervento umano, che se dovesse esprimersi sempre e comunque non consentirebbe di raggiungere i vantaggi connessi all'automazione delle decisioni, e senza contare quei processi automatizzati che non consentono, per loro natura, di

---

47 M. Kosinski - D. Stillwell - T. Graepel, *Private traits and attributes are predictable from digital records of human behavior,* in *PNAS*, 110, 15, 2013, 5802 ss. Secondo questi studi condotti dall'Università di Cambridge, sono sufficienti meno di 70 *like* di Facebook per determinare il colore della pelle dell'utente (con il 95% di precisione), l'orientamento sessuale (con l'88% di precisione), l'afferenza al partito politico (con il 95% di precisione). Ma a partire da queste rilevazioni sarebbe possibile anche risalire al credo religioso, al consumo di alcolici, sigarette o droghe, sino alla circostanza che i genitori abbiano convissuto o meno fino a che l'interessato abbia raggiunto i 21 anni.

48 L. Mitrou, *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?,* in *SSRN*, aprile 2019, 41.

49 Gruppo di lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679,* cit., 14.

comprendere le logiche di funzionamento interno (*black box*)[50].

Nel settore della sanità pubblica, ad esempio, il presidio dell'intervento umano viene garantito attraverso una responsabilizzazione di *default* del medico. Questi, qualora faccia ricorso a sistemi di IA nello svolgimento delle proprie attività, viene considerato responsabile di qualsiasi decisione fondata su sistemi decisionali automatizzati, salva comunque la «possibilità di discostarsi dalla soluzione proposta dall'IA»[51]. Non potendo consentire l'intervento diretto dell'uomo nella elaborazione della decisione automatizzata, irrealizzabile in presenza di analisi e studio dei cd *big data*, la tutela dell'intervento umano viene realizzata imputando all'uomo la responsabilità della decisione automatizzata.

Lo stesso approccio viene utilizzato nel settore delle armi automatizzate prevedendo che «i sistemi basati sull'IA devono consentire alla leadership militare di assumere la piena responsabilità e rendicontabilità per ... azioni letali o distruttive su larga scala mediante tali sistemi»[52]. Pur non rilevando tali prescrizioni in tema di dati personali, ciò che rileva in questa sede è individuare la tendenza dei regolatori a realizzare la garanzia dell'intervento umano spostando l'asse sulla responsabilità della persona che utilizza siffatti sistemi decisionali, a causa della difficoltà concreta di consentire l'intervento umano nella elaborazione della decisione automatizzata[53].

Il rimedio della responsabilizzazione, però, lascia aperto il tema della democraticità di tali sistemi, soprattutto laddove i meccanismi di *machine learning* riducono, se non eliminano del tutto, la contendibilità delle loro decisioni, intesa come la «*lack of an obvious means to challenge them when they produce unexpected, damaging, unfair or discriminatory results*»[54].

La non facile formulazione della norma (art. 22) e la delicatezza del tema trattato ha originato anche un dibattito tra chi sostiene che il GDPR riconosce soltanto un diritto di accesso e informazione[55], seppur ampliato per effetto della maggior trasparenza

---

[50] Come riferito nella *Communication "Building Trust in Human-Centric Artificial Intelligence"*, COM(2019) 168 final, 8 aprile 2019, 4, "*Human-in-the-loop*" si riferisce all'intervento umano in ogni ciclo decisionale del sistema, che in certi casi può non essere desiderabile; "Human-on-the-loop" si riferisce alla possibilità che l'intervento umano avvenga durante il design del sistema e come monitoraggio durante il suo funzionamento; "*Human-in-command*" si riferisce invece alla possibilità di vigilare sull'attività complessiva del sistema di IA (compreso il più ampio impatto economico, sociale, etico e legale) e alla capacità di decidere come e quando usare il sistema in una situazione particolare. Sul punto riassuntivamente B. Mittelstadt - P. Allo - M. Taddeo - S. Wachter - L. Floridi, *The ethics of algorithms: Mapping the debate,* in *Big Data & Society,* 3, 2016, 1 ss.

[51] Risoluzione del parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale, par. 65.

[52] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)).

[53] L'attenzione verso l'intervento umano è particolarmente sentita in tema di sorveglianza umana tant'è che in tale ambito l'High-Level Expert Group on Al selezionato dalla Comunità europea, nelle *Ethics Guidelines for trusthworty AI,* par. 65, indica di predisporre «meccanismi di governance che consentano un approccio con intervento umano (*human in the loop*), con supervisione umana (*human on the loop*) o con controllo umano (*human in command*)»

[54] L. Edwards - M. Veale, *Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking For*, in *Duke Law and Tech Review*, 16, 2017, 18 ss. Sempre in tema di contestabilità della decisione algoritmica M. Hildebrandt, *The new imbroglio. Living with machine algorithms,* in L. Janssens (hg.), *The Art of Ethics in the Information Society,* Amsterdam, 2016, 55 ss.

[55] S. Wachter - B. Mittelstadt - L. Floridi, *Why a right to explanation of automated decision making does not exist*

richiesta in tali casi, e chi sostiene invece l'esistenza di un vero e proprio diritto alla spiegazione[56]. Questi ultimi attribuiscono natura vincolante al considerando 71 per il quale il trattamento automatizzato «dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione».

Al di là delle difficoltà ermeneutiche derivanti dal quadro formale, e in disparte il rischio che il consenso venga reso come un automatismo[57], perché spesso gli utenti non sono portati a leggere con attenzione l'informativa sul consenso per poi esprimere una «intenzione libera, specifica, informata» sul trattamento[58], nell'ambito delle decisioni automatizzate si palesa evidente la debolezza della costruzione giuridica del consenso. Proprio laddove il consenso abbisogna di elementi di rinforzo esogeni per poter mantenere la centralità del ruolo costruito dal regolatore europeo, attraverso l'adozione di «misure appropriate» complementari che possano raggiungere l'obiettivo della tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, esso finisce per restar solo a operare non come momento di consapevolezza nell'esercizio della libertà di autodeterminazione ma, piuttosto, quale rinuncia inconsapevole alla tutela dei propri diritti.

5. Conclusioni

La regolamentazione sulla trasparenza e sui processi decisionali automatizzati mostra come il legislatore europeo si sia mosso con le migliori intenzioni, ponendosi l'obiettivo della tutela dei dati personali quale strumento per tutelare la persona nella sua interezza. Tale strategia è basata sulla riduzione del dato personale a "bene", da destinare alla libera circolazione in un mercato digitale senza confini: l'interessato viene tutelato per esser parte fondamentale del mercato digitale, unitamente all'imprenditore, in un mercato inteso come luogo nel quale si realizza la persona grazie al bilanciamento degli interessi e dei valori coinvolti.

Ma, il dato-bene non è rappresentativo della realtà personale, è frutto di una rappresentazione ideologicamente orientata e predeterminata da progettisti e sviluppatori, mentre la riduzione *tout court* della persona ai suoi dati è orientata da una scelta di convenienza, di guisa che la costruzione giuridica del consenso, attorno al quale ruota il sistema di legalità della *data protection,* non sempre è garanzia di autodeterminazione individuale. Inoltre, attraverso l'immissione continua dei dati personali nel mondo digitale si acconsente a che lo sviluppo della stessa personalità dell'individuo avvenga lì, nel

in the general data protection regulation, in *International Data Privacy Law*, 7(2), 2017, 76 ss.

[56] A. D. Selbst - J. Powles, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 7, 2017, 233.

[57] M.L. Jones - E. Kaufman - E. Edenberg, *AI and the Ethics of Automating Consent*, in *IEEE Security & Privacy*, 16, 3, 2018, 64 ss.

[58] E. Carolan, *The continuing problems with online consent under the EU's emerging data protection principles*, in *Computer Law & Security Review,* 32(3), 2016, 462 ss.; M. Butterworth, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, in *Computer Law and Security Review*, 34, 2018, 262.

mondo snervato e artefatto del digitale, che poi ha la forza di riverberarsi nel mondo materico potendo determinare forti condizionamenti dei comportamenti: gli algoritmi non solo predicono le azioni ma le producono[59]. Nel processo di formazione di tale personalità assume fondamentale rilievo la scelta dei dati che le danno forma, scelta che non è affidata all'individuo bensì al "titolare del trattamento", colui che ne decide scopi e finalità[60].

A fronte di tale scenario occorre sviluppare una riflessione di sistema sul significato che deve assumere il principio di trasparenza, sempre più cruciale per soddisfare l'esigenza, ormai largamente condivisa, della *trustworthy AI*[61]. È necessario indugiare sui profili critici emergenti nonché su possibili soluzioni tecnico-giuridiche, in una prospettiva *de jure condendo*. Non che questo tipo di riflessione possa dirsi agevole da percorrere: la sfida più difficile per i regolatori consiste nel riuscire a sviluppare modelli normativi dinamici, che possano metter le regole del sistema al riparo da un'obsolescenza scaturente da un incalzante processo tecnologico.

E così, il principio di trasparenza deve esser ancorato alle vulnerabilità delle singole persone, ciascuna con un proprio portato di competenze e conoscenze che deve condizionare l'assolvimento degli obblighi informativi da parte del titolare. Non una, ma tante trasparenze quanti sono i profili di rischio degli interessati, assecondando le esigenze di tutela delle vulnerabilità dei singoli, perché la vulnerabilità delle persone è l'unica chiave per mostrar loro quella lealtà fondamentale che può fondare una *trustworthy AI*.

Ancora, attraverso una trasparenza post trattamento, che indichi le conseguenze effettive del trattamento automatizzato, la trasparenza decisionale non sarebbe più un punto statico per l'ancoraggio del consenso ma consentirebbe all'individuo di poter costruire nel tempo, arricchendolo con la conoscenza ad esempio dei dati inferenziali, il proprio punto di vista, le proprie scelte in piena libertà.

La persona deve esser partecipe non tanto della logica imperscrutabile di sofisticati meccanismi che governano i sistemi decisionali automatizzati, quanto dello scopo dell'intero processo di automazione e delle sue conseguenze, prodotte sugli individui, sulla società e sull'ambiente.

Ecco che, messa in chiaro questa base informativa, si potrà costruire un consenso non soltanto libero e informato ma, soprattutto, partecipato, reintegrando l'individuo nel potere di definire quella parte del proprio patrimonio informativo da rendere disponibile nel mondo digitale, così da restituire alla persona umana la decisione sugli aspetti

[59] Ciò varrebbe a confermare l'intuizione di Stefano Rodotà, il quale sosteneva una accezione del diritto alla privacy più estesa che nel passato, di pretesa da parte dell'interessato di stabilire in piena autonomia le «*modalità di costruzione della propria sfera privata*» *S. Rodotà, Tecnologie e diritti, cit., 1995, 122.*

[60] Sul tema dei poteri privati che potrebbero incidere sullo sviluppo della personalità umana, segnatamente della libertà di espressione, si veda M. Bassini, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione, in questa Rivista, 2, 2021, 76. L'autore parla «claim normativo» e muove dalla constatazione che la sospensione della possibilità di accesso ai social network, sulla scorta di regole di ingaggio predisposte unilateralmente dal regolatore privato, può determinare «un vero e proprio impedimento, a seconda dei casi» nell'esercizio della libertà di espressione.*

[61] La strategia per trasformare l'Europa in un hub globale ruota attorno al fulcro della fiducia, vale a dire che per consentire lo sviluppo dei sistemi di intelligenza artificiale (IA) è indispensabile lavorare sulla loro affidabilità. V. l'High-Level Expert Group on Al, *Ethics Guidelines for trustworthy AI,* cit.

più significativi legati alla propria intima vita.

Elenco autori

Enrico Albanesi
professore associato di diritto costituzionale, Università degli Studi di Genova
Flavia Bavetta
dottoranda di ricerca in Legal Studies - International and European Law, Università Bocconi
Giampaolo Berni Ferretti
avvocato in Milano
Maria Esmeralda Bucalo
professoressa associata di diritto costituzionale, Università degli Studi di Palermo
Federica Casarosa
part-time professor, Centre for Judicial Cooperation, European University Institute
Marina Castellaneta
professoressa ordinaria di diritto internazionale, Università degli Stud di Bari "A. Moro"
Silvia Cereda
dottoressa magistrale in Giurisprudenza
Carlotta Cherchi
avvocato in Milano
Ferruccio de Bortoli
già direttore del Corriere della Sera e de Il Sole 24 Ore
Gianluca Fasano
dirigente tecnologo, CNR
Chiara Gallese
guest researcher, Department of Electrical Engineering, Eindhoven University of Technology
Matteo Gozzi
Avvocato in Milano
Sarah Lattanzi
ricercatrice di diritto dell'Unione europea, Università degli Studi di Napoli "Parthenope"
Giuseppina Lofaro
assegnista di ricerca di diritto amministrativo, Università degli Studi Mediterranea di Reggio Calabria
Simone Lonati
professore associato di diritto processuale penale, Università Bocconi
Giuseppe Muto
avvocato praticante in Milano
Marco Orofino
professore ordinario di diritto costituzionale, Università degli Studi di Milano
Federica Paolucci
dottoranda di ricerca in Legal Studies - International and European Law, Università Bocconi
Sabrina Peron
avvocato in Milano
Rosario Petruso
ricercatore di diritto privato comparato, Università degli Studi di Palermo
Margherita Pisapia
avvocato in Milano
Oreste Pollicino
professore ordinario di diritto costituzionale, Università Bocconi
Sveva Ruggiero
LL.M. candidate, LL.M. in Law of Internet Technology, Università Bocconi
Agostino Sola
avvocato in Roma
Alessandro Toschi Tedeschi
avvocato in Milano

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

mediaLAWS

ANNO 2022 - CODICE ISSN 2532-9146