medialaws

Rivista di diritto dei media
2/2020 maggio

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)

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

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

REDAZIONE
EDITORIAL BOARD
Marco Bassini (*coordinatore*) (Università Bocconi)
Serena Sileoni (*vice coordinatore*) (Università S. Orsola Benincasa)
Gianluca Campus (Avvocato in Milano)
Nicola Canzian (Università di Milano - Bicocca)
Giovanni De Gregorio (Università di Milano - Bicocca)
Fabio Ferrari (Università di Verona)
Valerio Lubello (Università Bocconi)
Omar Makimov Pallotta (Università di Macerata)
Maria Chiara Meneghetti (Università Bocconi)
Silvia Vimercati (Università di Milano - Bicocca)
Paolo Zicchittu (Università di Milano - Bicocca)

COMITATO SCIENTIFICO- STEERING COMMITTEE
Shulamit Almog *(University of Haifa),* Mirzia Bianca *(La Sapienza – Università di Roma),* Elda Brogi *(European University Institute),* Giuseppe Busia *(Garante per la protezione dei dati personali),* Licia Califano *(Garante per la protezione dei dati personali),* Angelo Marcello Cardani *(Autorità per le garanzie nelle comunicazioni),* Marta Cartabia *(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),* 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 *(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),* 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, Fabio Basile, Marco Bellezza, Daniela Bifulco, Elena Bindi, Carlo Blengino, Monica Bonini, Manfredi Bontempelli, Fernando Bruno, Daniele Butturini, Irene Calboli, Simone Calzolaio, Quirino Camerlengo, Marina Caporale, Andrea Cardone, Corrado Caruso, Stefano Catalano, Adolfo Ceretti, Francesco Clementi,Roberto Cornelli, Giovanna Corrias Lucente, Filippo Danovi, Monica Delsignore, Giovanna De Minico, Gabriele Della Morte, Marius Dragomir, Fernanda Faini, Roberto Flor, Federico Furlan, Giovanni Battista Gallus, Marco Gambaro, Gianluca Gardini, Ottavio Grandinetti, Antonino Gullo, Simone Lonati, Erik Longo, Federico Lubian, Nicola Lupo, Paola Marsocci, Claudio Martinelli, Alberto Mattiacci, Alessandro Melchionda, Massimiliano Mezzanotte, Francesco Paolo Micozzi, Donatella Morana, Piergiuseppe Otranto, 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, Michelangela Verardi, Thomas Wischmeyer

ANNO 2020 - 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 Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei Garanti
Francesco Pizzetti

Saggi

35 Regolare Internet
Michela Manetti

52 Lo spazio digitale dei lavori parlamentari e l'emergenza sanitaria Covid-19
Paola Marsocci

81 La libertà di espressione dei partiti politici nello spazio pubblico digitale: alcuni spunti di attualità
Paolo Zicchittu

95 Media regulation at a distance: video-sharing platforms in AVMS Directive and the future of content regulation
Lubos Kuklis

111 A legal analysis of the use of blockchain technology for the formation of smart legal contracts
Giusella Finocchiaro - Chantal Bomprezzi

136 Verso la decisione amministrativa algoritmica?
Scilla Vernile

153 Proposal toward "no-fault" civil liability regulation following Artificial Intelligence evolution in health-care
Emiliano Marchisio

172 "Immuni". *Un'exposure notification* app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici
Marco Plutino

194 The PoSeID-on Blockchain-based platform meets the "right to be forgotten"
Giovanni Maria Riccio - Adriana Peduto - Fabiola Iraci Gambazza - Luigi Briguglio - Elena Sartini - Carmela Occhipinti - Iván Gutiérrez - Domenico Natale

212 Flussi migratori e protezione dei dati personali: alla ricerca di un punto di equilibrio tra sicurezza pubblica e tutela della privacy dei migranti e dei rifugiati all'interno del territorio europeo
Mirko Forti

231 Processo penale "a distanza" e diritto alla privacy: possibili profili di contrasto
Pietro Insolera - Stella Romano

247 Verso l'attuazione della direttiva (UE) 2019/1024 sul riutilizzo degli open data della PA: nuove opportunità per le imprese
Sara Gobbato

262 ICT e nuove forme di interazione tra cittadino e Pubblica Amministrazione
Cristiana Benetazzo

Note a sentenza
Sezione Italia

275 "*Res telematica*". La problematica corporeità del file ed il reato di appropriazione indebita
Maurizio Fumo

285 Diffamazione a mezzo stampa e diritto di critica: no alle aggressioni senza motivato dissenso
Jacopo Antonelli Dudan

Note a sentenza
Sezione Europa

289 Il caso Taormina e la Corte di Giustizia. Dalla libera espressione alla discriminazione
Palmina Tanzarella

305 Oltre il mero stoccaggio di prodotti in contraffazione di marchio: una riflessione sul caso *Amazon* deciso dalla Corte di giustizia dell'Unione europea
Alice Fratti – Riccardo Traina Chiarini

316 Utilizzo dei *cookie* e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di giustizia nel caso *Planet49*
Riccardo Cabazzi

323 Il bilanciamento tra libertà di espressione degli avvocati e tutela dell'autorità del potere giudiziario: un inquadramento sistematico degli interessi nella prospettiva della Corte europea dei diritti dell'uomo
Federico Ceci

Sezione comparata

340 Soluzioni tradizionali per piattaforme moderne: la *state action* (non) mostra i segni del tempo
Davide Zecca

347 Una stampa libera e pluralista è essenziale per garantire un giornalismo di qualità.
Il diritto d'autore e i diritti connessi tutelano il patrimonio culturale
Cecilia Trevisi

Commenti

360 Il potere senza responsabilità dei social media nelle campagne elettorali
Giuseppe Donato

367 Key findings of the Italian joint sector inquiry into Big Data
Enzo Marasà

Recensioni

387 Per chi vuol sapere tutto di un reato, "La diffamazione", di Vincenzo Pezzella
Carlo Melzi d'Eril

389 Recensione a Emilio Tosi (a cura di), *Privacy Digitale*, Giuffré Lefebvre, 2019
Giovanni Stella

392 A proposito di *fake news*: analisi e proposte per contrastare il dilagare del fenomeno. Recensione a Tommaso Guerini, *Fake news e diritto penale*
Giuseppina Ferro

Indice
Index

Editoriale

11 Contact tracing in the context of the Covid-19 pandemic: the safeguards under the GDPR and the shifting role of data protection authorities
Francesco Pizzetti

Articles

35 Regulating the Internet
Michela Manetti

52 The digital space for parliamentary work and the Covid-19 health emergencyc
Paola Marsocci

81 Political parties' freedom of expression in the digital public space: some topical remarks
Paolo Zicchittu

95 Media regulation at a distance: video-sharing platforms in AVMS Directive and the future of content regulation
Lubos Kuklis

111 A legal analysis of the use of blockchain technology for the formation of smart legal contracts
Giusella Finocchiaro - Chantal Bomprezzi

136 Towards the algorithmic administrative decision?
Scilla Vernile

153 Proposal toward "no-fault" civil liability regulation following Artificial Intelligence evolution in health-care
Emiliano Marchisio

172 Immuni. An exposure notification app at the crossroad between fundamental rights and public interests
Marco Plutino

194 The PoSeID-on Blockchain-based platform meets the "right to be forgotten"
Giovanni Maria Riccio - Adriana Peduto - Fabiola Iraci Gambazza - Luigi Briguglio - Elena Sartini - Carmela Occhipinti - Iván Gutiérrez - Domenico Natale

212 Mass migrations phenomena and data protection: finding a balance between national security and privacy rights of migrants and refugees
Mirko Forti

231 "Remote" criminal trial and right to privacy: possible constitutional infirmities
Pietro Insolera - Stella Romano

247 Towards the implementation of Directive (EU) 2019/1024 on open data and the re-use of public sector information: new business opportunities
Sara Gobbato

262 ICT and new forms of interaction between citizen and Public Administration
Cristiana Benetazzo

Notes and comments
Italy

275 The Italian Supreme Court rules the legal status of computer files
Maurizio Fumo

285 Right to criticism and defamation in a recent stance of the Italian Supreme Court
Jacopo Antonelli Dudan

Notes and comments
Europe

289 The Court of Justice perspective on the "Taormina" case. From Freedom of expression to Discrimination
Palmina Tanzarella

305 Beyond the mere storage of products infringing trademark rights: an analysis on the *Amazon* case decided by the Court of Justice of the European Union
Alice Fratti – Riccardo Traina Chiarini

316 Use of cookies and (new) protection of the user: the position adopted by the Court of Justice in the *Planet49* case
Riccardo Cabazzi

323 The balance between freedom of expression of lawyers and the protection of the authority of the judiciary: a systematic framing of interests in the perspective of the European Court of Human Rights
Federico Ceci

Comparative Law

340 Traditional remedies for modern platforms: the state action bears (no) signs of obsolescence
Davide Zecca

347 A free and pluralist press is essential to ensure quality journalism. Copyright and related rights preserve cultural heritage
Cecilia Trevisi

Debates

360 Power without responsibility of social media in the context of electoral campaigns
Giuseppe Donato

367 Key findings of the Italian joint sector inquiry into Big Data
Enzo Marasà

Book reviews

387 If one wishes to know everything about a crime: "La diffamazione", by Vincenzo Pezzella
Carlo Melzi d'Eril

389 Review to Emilio Tosi (a cura di), *Privacy Digitale*, Giuffré Lefebvre, 2019
Giovanni Stella

392 About fake news: some thoughts to counter the ever-growing spread of disinformation. Review to Tommaso Guerini, *Fake news e diritto penale*
Giuseppina Ferro

Il presente numero viene licenziato all'esito di un periodo eccezionale, che ha visto il nostro paese, come altri nel mondo, fronteggiare il dramma della pandemia. Le circostanze di fatto hanno costretto moltissime persone a rivisitare le tradizionali, frenetiche modalità lavorative, con esigenze di riconversione verso altre forme che hanno toccato larga parte delle professioni, compresa quella intellettuale e di ricerca scientifica. Nuove problematiche sono poi comparse sulla scena del dibattito pubblico, alimentando le riflessioni dei giuristi: la ricerca di nuove modalità di deliberazione per gli organi istituzionali nell'epoca dell'emergenza e la necessità di elaborare soluzioni tecnologiche per il contenimento del contagio sono soltanto alcuni dei temi che hanno attirato l'attenzione dei commentatori, e di cui anche il contenuto di questo fascicolo, a cominciare dall'editoriale di Franco Pizzetti, serba una traccia evidente.

Non sono mancate anche le buone notizie: siamo lieti di comunicare che, all'esito di una valutazione positiva, l'Agenzia Nazionale di Valutazione del Sistema Universitario e della Ricerca ha incluso la Rivista di diritto dei media tra le riviste scientifiche di area 12 rilevanti ai fini dell'Abilitazione Scientifica Nazionale (ASN). Il riconoscimento di scientificità è stato accordato retroattivamente a tutte le pubblicazioni a far data dal 1° gennaio 2016, quindi sin dalla costituzione della Rivista, che ha licenziato il suo primo fascicolo nel 2017. Riteniamo importante condividere questa notizia per ringraziare coloro che hanno reso questo primo traguardo possibile: i nostri autori, i membri della redazione, del Comitato scientifico e del Comitato degli esperti per la valutazione; ma soprattutto i nostri lettori, senza la cui fiducia gli sforzi profusi per garantire uno strumento di qualità al servizio della comunità scientifica e professionale risulterebbero in larga parte vani.

Milano, 8 luglio 2020

***

Su determinazione della direzione, in conformità al regolamento della Rivista, sono stati sottoposti a referaggio anonimo ovvero a referaggio anonimo a doppio cieco, come indicato in calce a ciascun contributo, i saggi di: Cristiana Benetazzo, Giusella Finocchiaro-Chantal Bomprezzi, Mirko Forti, Sara Gobbato, Pietro Insolera-Stella Romano, Michela Manetti, Emiliano Marchisio, Paola Marsocci, Marco Plutino, Giovanni Maria Riccio et alii*, Scilla Vernile, Paolo Zicchittu. È stata inoltre sottoposta a referaggio anonimo la nota a sentenza di Palmina Tanzarella.*

Editoriale

Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei Garanti

Francesco Pizzetti

1. Uno degli effetti più evidenti dell'epidemia provocata dal Covid-19 nel corso di questo anno è stato certamente quello di obbligare milioni di persone a misurarsi con la società digitale e con le opportunità, ma anche con i pericoli, che essa presenta rispetto ai servizi che mette a disposizione delle nostre società.
Per contro è chiaro a tutti che da questo punto di vista l'epidemia è un vero *turning point*, delle cui conseguenze oggi non abbiamo ancora adeguata consapevolezza.
È in questo quadro che, a me pare, il dibattito molto ampio svoltosi in questi mesi, in particolare Italia, sulla app Immuni deve essere collocato.
Al di là della legittimità del sistema di *tracing* proposto e, in particolare, della sua compatibilità con la normativa in materia di privacy, questo dibattito ha "sdoganato" nell'immaginario collettivo alcune prospettive, anche legate a specifiche tecnologie, delle quali fino a qualche mese fa pochi, fra il grande pubblico degli utenti del web, avevano consapevolezza.
Sul piano tecnologico l'aspetto più importante è stato quello di mettere tutti al corrente che i sistemi di *tracing*, intesi come sistemi che consentono il tracciamento dei devices, e in particolare degli smartphone, si dividono in sistemi accentrati e decentrati. La differenza tra le due famiglie di sistemi riguarda se i dati di tracciamento o quelli destinati a consentirlo in caso di bisogno, sono accentrati, ovvero conservati in una specifica struttura alla quale tutti i dati generati dai telefonini che entrano tra loro in contatto pervengono; o decentrati, ovvero conservati sugli stessi devices telefonici e analizzati ai fini di rilevare i contatti solo laddove ne sorga la necessità. Entrambi i sistemi possono superare lo scoglio di dover fare ricorso in via generale a tecniche di geolocalizzazione che, come tali, suscitano problemi di particolare rilievo, specialmente rispetto all'individuazione di chi abbia titolo per accedere a tali dati e trattarli, e quindi anche per quanto riguarda più da vicino la tutela dei dati personali relativi.
Di non minore importanza è stato anche rendere ampiamente diffusa la conoscenza della possibilità di fare in modo che i devices dialoghino tra loro attraverso la tecnologia Bluetooth, che consente ai devices stessi di trasmettersi l'un l'altro codici identificativi che attestano il fatto che i due strumenti si sono trovati in un ambito spaziale coincidente con quello, molto limitato, che i sistemi basati su questa tecnologia consentono di utilizzare, registrando anche il tempo durate il quale tale contatto è durato e la distanza alla quale è avvenuto. I dati relativi, se il sistema è decentrato, restano sui rispettivi devices, diminuendo così molto i rischi derivanti dalla loro concentrazione in un unico sito al quale sia possibile accedere, potendo venire così facilmente a cono-

scenza in modo illecito di un numero potenzialmente molto elevato di dati personali, quali sono quelli prodotti da devices riconducibili a utenti specifici, venuti in contatto tra loro. La compresenza di due devices nel raggio di azione compatibile con la tecnologia Bluetooth consente infatti, a sua volta, un tracciamento molto accurato della prossimità dei due strumenti e del tempo nel quale tale contatto è avvenuto, consentendo così di tracciare i contatti tra le persone alle quali i devices sono riconducibili.
Dal punto di vista giuridico, l'adozione di tecnologie di tracciamento dei contatti tra le persone (o dei devices usati dalle persone) è stata caldamente raccomandata, in particolare anche dalla Organizzazione Mondiale della Sanità, proprio al fine di combattere il contagio. La conoscenza degli avvenuti contatti in un raggio limitato e per un tempo definito può infatti consentire maggiore rapidità di interventi curativi da parte delle strutture sanitarie che siano messe al corrente del contatto. Di conseguenza è possibile accertare più rapidamente se si è verificato o no il contagio e gli interventi curativi possono avere maggiore efficacia, così come possono essere più efficaci le misure di contenimento del contagio. Per queste ragioni il ricorso a queste tecnologie è stato considerato particolarmente raccomandabile nell'ambito internazionale, e soprattutto il ricorso ad esse è stato suggerito dall'OMS, come uno strumento particolarmente efficace di lotta all'epidemia.
Sulla base di questi aspetti è stato possibile allo EDPB e, di conseguenza, ai singoli Garanti europei, superare con una certa agevolezza il tema del rapporto tra l'utilizzazione di queste tecnologie e la normativa a tutela dei dati personali, anche con riguardo a dati che, come nel caso, si riferiscono alla salute delle persone entrate tra loro in contatto.
È stato possibile, infatti, fare ricorso all'art. 9, lett. *i*), del GDPR, secondo il quale il trattamento di dati relativi alla salute è legittimo quando «è dichiarato necessario per motivi di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni o le garanzie del paragrafo 3».
Il par. 3 dell'art. 9, a sua volta, specifica che la lett. *h*) del primo paragrafo consente la legittimità dei trattamenti se «i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite da o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti».
Proprio all'art. 9 del GDPR hanno fatto riferimento le Autorità garanti che, riunite nello EDPB, hanno confermato con un documento contenente Linee guida chiare e ben scritte la posizione già assunta dalla Presidente Andrea Jelinek in più occasioni (fra le quali merita segnalare la lettera a Olivier Micol Capo della Unit European Commission DG for Justice and Consumers) e sulle indicazioni già formulate in varie occasioni dalle Autorità garanti nazionali, tra le quali anche la CNIL e il Garante italiano.
Essendo tutti documenti ben noti e ormai già citati in molte sedi sarà sufficiente qui richiamarne gli aspetti essenziali contenuti nelle Linee guida 04/2020 dello EDPB che consistono in alcuni punti molto chiari e molto fermi.

Il primo punto ribadisce che la tutela dei dati personali, conformemente all'art. 8 della Carta dei diritti fondamentali dell'UE, adottata con rango di trattato nel Trattato di Lisbona, è un diritto fondamentale della persona, come tale riconosciuto dall'Unione Europea. Ne consegue tuttavia che, pur essendo un diritto fondamentale, esso è comprimibile quando ciò sia necessario per tutelare altri non meno importanti diritti fondamentali riconosciuti come tali anche dalla medesima Carta. Non a caso nel parere dello EDPB si ripete, anche sulla traccia di una ormai consolidata giurisprudenza costituzionale fatta propria sia dalla Corte di giustizia che da molte Corti costituzionali degli Stati UE, che nell'ambito dei diritti fondamentali non può esservi alcun "diritto tiranno" la cui osservanza possa giustificare la compressione, anche fino all'annullamento, di altri diritti, parimenti fondamentali.

Del resto, questo costituisce anche la base dello stesso art. 9 del GDPR il quale, tuttavia, subordina il bilanciamento tra la tutela dei dati personali e altri diritti fondamentali che possano essere in gioco al verificarsi di una delle situazioni di cui dalla lett. *a*) alla lett. *j*) del suo par. 2.

Ovviamente il prodursi di una delle situazioni di cui alla norma citata implica il sorgere di una causa di legittimità del trattamento, in assenza della quale (o delle quali) il trattamento dei dati, a cominciare dalla loro raccolta, è da considerarsi illecito e dunque vietato. Peraltro, il sorgere di tale causa di legittimazione si limita, quanto agli effetti, ad autorizzare il decisore UE o i decisori nazionali ad effettuare il necessario bilanciamento tra il diritto alla protezione dei dati personali e gli altri diritti fondamentali in gioco, al fine di assicurare garanzie adeguate a tutti i diritti e agli interessi fondamentali dell'interessato.

Se si riflette attentamente sulle cause in presenza delle quali è considerata legittima la compressione del diritto alla tutela dei dati personali si può agevolmente constatare che pressoché tutte riguardano la tutela della persona alla quale si riferiscono i dati.

Tale riserva è evidentemente posta a tutela della persona, e costituisce quasi un aspetto essenziale della sua libertà, ben più che della sua "dignità". Non a caso la prima causa di legittimità della compressione della tutela dei dati personali, quella posta all'inizio del par. 2 dell'art. 9 del GDPR e indicata alla lett. *a*), consiste nel consenso dato dall'interessato stesso.

Il "consenso" è nel quadro della protezione dati di matrice europea lo strumento principale attraverso il quale l'interessato può esprimere la propria volontà e tutelare autonomamente la propria libertà personale nel mondo dei trattamenti dei dati che lo riguardano. Ovviamente l'esercizio del consenso è legato alla completezza dell'informativa che, non a caso, è oggetto di ben due articoli, il 13 e il 14, e che il GDPR vuole sia completa, chiara, ed espressa in linguaggio semplice e comprensibile da tutti, nel rispetto del principio di trasparenza al quale è dedicata tutta la Sezione I del Capo III del GDPR.

La stessa centralità della persona interessata è alla base anche delle altre ipotesi di restrizione della tutela dei dati personali.

È questa infatti la ragione della legittimità dei trattamenti di dati personali anche senza il consenso dell'interessato nei casi in cui questi trattamenti:

a. siano funzionali a consentire all'interessato di assolvere agli obblighi ed esercitare

i diritti specifici del titolare o dell'interessato in materia di diritto del lavoro, della sicurezza sociale e della protezione sociale, sempre che ciò sia previsto dal diritto dell'Unione o dal diritto nazionale e siano definite le garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. *b*);

b. siano necessari a tutelare interessi vitali dell'interessato o altra persona fisica e l'interessato non sia in grado di esprimere il proprio consenso (art. 9, par. 2, lett. *c*);
c. il trattamento avvenga nell'ambito di una associazione o fondazione che, senza scopo di lucro, persegua finalità politiche, filosofiche, religiose o sindacali, concorrendo così a rendere attivi altri diritti fondamentali riconosciuti alla persona, e anche in questi casi comunque operando con adeguate garanzie (art. 9, par. 2, lett. *d*);
d. il trattamento riguardi dati personali resi pubblici dall'interessato (art. 9, par. 2, lett. *e*);
e. il trattamento è necessario per difendere in sede giudiziaria diritti dell'interessato (art. 9, par. 2, lett. *f*);
f. il trattamento è necessario per motivi di interesse pubblico rilevanti, che devono però essere individuati dal diritto dell'Unione o degli Stati membri in un quadro che assicuri la proporzionalità tra la compressione della tutela e le finalità perseguite, prevedendo inoltre misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. *g*);
g. il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sociali sulla base del diritto dell'Unione o degli Stati membri, ovvero sulla base di un contratto con un professionista della sanità, o, ancora, sia conforme alle nome stabilite da organismi competenti di diritto dell'Unione o degli altri membri della sanità (art. 9, par. 2, lett. *h*) sempre che i dati personali siano trattati sotto la responsabilità di un professionista soggetto al segreto professionale ovvero per le gestione di sistemi o servizi sanitari o sociali conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri (art. 9, par. 3, richiamato dall'art. 9, par. 2, lett. *h*);
h. il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati che, anche in questi casi, devono prevedere misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. *i*);
i. infine, la protezione dei dati personali può trovare compressioni per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o a fini statistici in conformità all'art. 89, par. 1 del GDPR. Anche in questo caso, comunque, ciò deve avvenire «sulla base del diritto dell'Unione o nazionale che, a sua volta, deve essere proporzionato alle finalità perseguite, rispettare l'essenza del diritto alla protezione dei dati personali e prevedere misure appropriate e specifiche per tutelare i diritti e gli interessi dell'interessato» (art. 9, par. 3, lett. *j*).

In sostanza, se si legge con attenzione, lungimiranza, e capacità di visione prospettica l'art. 9, par. 2, del GDPR si vede con facilità che le ragioni per cui le regole relative alla tutela dei dati personali possono essere compresse riguardano due grandi categorie di casi e situazioni.

La prima, a carattere generale e perfettamente coerente con l'impianto complessivo del GDPR, è il consenso dell'interessato di cui all'art. 9 par. 1, lett. *a*) che ribadisce la sovranità della persona sui suoi dati, sia nel senso che il loro uso è legittimo solo col consenso dell'interessato sia nel senso che a tal fine l'interessato ha diritto a una informativa chiara e comprensibile che gli consenta tanto di esprimere un consenso libero e informato quanto di esercitare eventualmente il diritto a ritirarlo nel tempo.

La seconda linea è che il consenso è, in via generale, necessario solo ove i trattamenti abbiano finalità di tutela dell'interessato sia rispetto alla sua vita che alla tutela dei suoi diritti. In entrambe queste due prospettive è evidente la centralità della tutela della persona interessata che per un verso è strettamente connessa alla condizione del consenso, e quindi di una specifica manifestazione di volontà non condizionata né condizionabile e sempre revocabile, ovvero alla necessità di tutelare diritti e interessi dello stesso interessato.

Tuttavia, però, quando una di queste due prospettive non ricorra, e siano presenti invece ragioni di restrizione della tutela connesse all'interesse pubblico, sia esso di natura sanitaria o connessa alla salute collettiva o di natura statistica e conoscitiva, allora è sempre necessario l'intervento del legislatore unionale o statale.

Non solo: sulla base del testo delle norme citate è chiaro che la legittimità di una compressione della tutela dei dati personali non basata sul consenso ma sull'intervento unionale o statale relativo a una delle situazioni appena richiamate richiede sempre implicitamente una attenta valutazione dei diversi diritti in gioco, ed è legittima in quanto per un verso il decisore unionale o statale abbia ragione di ritenere, all'esito del bilanciamento, che sussistano ragioni adeguate alla compressione della tutela dei dati personali che devono essere collegate inevitabilmente alla tutela di altri diritti parimenti fondamentali. Inoltre, tutte le norme contenute nell'art. 9 che prevedono l'intervento unionale o statale stabiliscono con chiarezza che non basta un bilanciamento fra i diversi interessi e diritti in gioco che giustifichi tale compressione, ma che è necessario anche che il decisore unionale o statale adottino misure appropriate e specifiche per tutelare tutti i diversi diritti fondamentali in gioco, ivi compreso ovviamente il diritto alla tutela dei dati personali dell'interessato.

Non basta dunque una valutazione relativa ai diversi diritti fondamentali in gioco per giustificare la compressione della tutela ma occorre anche adottare, se necessario, ulteriori e nuove misure normative che assicurino la tutela dei diritti e degli interessi fondamentali dell'interessato.

Dunque, stando all'art. 9 del GDPR, appare chiaro che l'intervento del legislatore unionale o statale non può limitarsi a definire e circoscrivere le limitazioni della tutela dei dati personali relativamente a casi specifici e in rapporto ad altri diritti fondamentali ma deve indicare anche le forme di tutela dei dati personali, e in generale dei diritti fondamentali delle persone, adeguate ad assicurare che le compressioni relative alle norme generali adottate non pregiudichino comunque la tutela dei diritti fondamentali

e degli interessi dell'interessato.
Va da sé che nella logica dell'art. 9 questo implica anche che le scelte fatte dal decisore unionale o nazionale relative alla compressione della tutela generale e all'adozione di forme alternative di tutela dei diritti fondamentali possano essere soggette anche a un controllo giurisdizionale, rimesso alla Corte di giustizia, per quanto riguarda le decisioni unionali, e alle Corti nazionali, sulla base dell'ordinamento costituzionale interno di ciascun Stato membro, tenuto conto della competenza della Corte di Giustizia dell'Unione, per quanto riguarda le decisioni statali.

2. Merita inoltre sottolineare che il GDPR contiene anche una altra disposizione che ben avrebbe potuto essere utilizzata per giustificare interventi unionali o statali di limitazione della normativa a tutela dei dati personali e che, invece, non è mai stata presa in specifica considerazione nell'ambito relativo alla valutazione della compatibilità dell'utilizzazione di app di tracciamento rispetto al GDPR e a quanto in esso previsto. Il riferimento è all'art. 23 del GDPR stesso, che contiene in via generale la disposizione relativa, come specifica il titolo della norma, le "limitazioni" al GDPR, soprattutto con riguardo agli artt. da 12 a 22 e 34 nonché all'art. 5 (cfr. art. 253, par. 1). Il richiamo alla sostanziale trascuratezza di questa norma da parte dei Garanti è in questa sede importante sia perché merita sottolineare la rinuncia a richiamare anche tale articolo sia perché proprio tale rinuncia sembra ribadire il sostanziale interesse dello EDPB (e anche dei Garanti nazionali) a non sollecitare l'intervento del decisore unionale e di quelli nazionali.
Pare infatti chiaro che l'intervento del decisore unionale o statale anche nei casi dell'art. 23 ha lo scopo, pur non sottolineato con la stessa forza di quanto si fa nell'art. 9, di garantire che spetti ai decisori in questione sia verificare la necessità e, soprattutto, la ragionevolezza delle limitazioni rispetto ai tipi di trattamento e alle loro finalità sia individuare le eventuali garanzie adottabili per assicurare comunque la tutela del diritto alla protezione dei dati personali pur in un quadro di restrizione della normativa generale in materia.
Dunque, l'eventuale ed esplicito richiamo a tale articolo avrebbe ragionevolmente dovuto spingere sia i Garanti che lo EDPB a subordinare la legittimità della eventuale compressione delle norme in materia di tutela dei dati personali a un esplicito intervento del decisore unionale o nazionale, tanto ai sensi dell'art. 9 che dell'art. 23 del GDPR.
Questo non è avvenuto, malgrado che l'art. 9 sia stato ampiamente citato. Ed è proprio questo che impone di porsi alcuni degli interrogativi qui esaminati.

3. Il problema centrale è che sia le lettere della Presidente dello EDPB Andrea Jelinek, sia le Linee guida 04/2020 sull'uso dei dati di localizzazione per il tracciamento dei contatti nel contesto dell'emergenza legata al Covid-19, pur richiamando ampiamente in via generale le norme del GDPR, e in particolare, tra quelle qui citate l'art. 9, non vincolano affatto la legittimità della adozione delle app di tracciamento per combattere l'epidemia a specifiche previsioni normative dell'UE o degli Stati membri né tengono fermo il consenso come unica, o prevalente, causa di legittimità dei tratta-

menti anche in assenza di specifiche previsioni o di esigenze legate alla tutela dei diritti dell'interessato.
Il punto "forte" del Parere dello EDPB riguarda essenzialmente il condizionare la legittimità dell'uso di app di tracciamento, anche per finalità di lotta all'epidemia, al fatto che non sia reso in alcun modo obbligatorio o vincolato il loro scaricamento e il loro uso da parte degli utenti di telefonia mobile o comunque da parte dei cittadini interessati.
Si specifica, anzi, esplicitamente che in tanto l'uso di queste app (nel caso italiano di Immuni) è legittimo in quanto il loro uso implichi la libera scelta da parte degli utenti di smartphone in ordine alla decisione se scaricarle o meno e se farne o meno uso.
Si chiede poi che il sistema sia almeno interoperabile a livello di tutti gli Stati della UE e che le modalità di attuazione siano in grado di garantire la necessaria coerenza tra dati usati e tipologia di trattamenti e finalità che si vogliono raggiungere. Si chiede inoltre, in coerenza, con quanto previsto dall' art. 9, par. 2, lett. *h*), che i trattamenti dei dati sanitari siano posti in essere da professionisti della sanità, vincolati al rispetto delle norme sul segreto professionale oltre che dotati della competenza sanitaria necessaria a decidere sulla necessità dei trattamenti stessi.
Inoltre sia nelle Linee guida citate che nei pareri successivamente espressi, soprattutto dai Garanti nazionali, rispetto a specifiche app adottate nel territorio degli Stati membri (per l'Italia cfr. Garante privacy, *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19-App Immuni* (doc. web n. 9356568) del 1 giugno 2020) si specifica che se queste condizioni sono rispettate l'uso di applicazioni di tracciamento per finalità di lotta all'epidemia Covid-19 sono compatibili con la normativa di protezione dei dati personali.
Ovviamente ciascuno degli aspetti richiamati meriterebbe una analisi specifica, e certo colpisce che da un lato si chieda che la decisione se scaricare o no l'app sia rimessa unicamente agli utenti, pur sapendo che il numero di app effettivamente scaricate ed effettivamente funzionanti è elemento condizionante circa la probabilità di raggiungere le finalità che il sistema di cui la app fa parte e il suo uso si propongono e dall'altro si insista nel considerare, giustamente, condizione essenziale di legittimità dell'uso della app la coerenza con le finalità che con la sua utilizzazione si vogliono raggiungere.
In questa sede, però, merita richiamare l'attenzione su un altro aspetto delle Linee guida che a prima vista può sfuggire e, di fatto, sembra essere sfuggito in generale a tanti commentatori sia della tecnologia legata all'app Immuni che delle posizioni dei Garanti di protezione dei dati personali, Garante italiano compreso.

4. Il punto essenziale della posizione assunta dalle Autorità di protezione dei dati personali nelle Linee guida 04/2020 e già espresse anche nello Statement della Presidente dello EDP Andrea Jelinek del 16 marzo 2020, è infatti che, pur rinviando alle norme del GDPR che richiedono l'intervento dei decisori unionali e nazionali per consentire limitazioni della tutela dei dati personali al fine di assicurare adeguate garanzie per tutti i diritti e gli interessi fondamentali in gioco, esse sembrano accentuare la loro attenzione quasi esclusivamente sulla libertà (o se si preferisce la non obbligatorietà della scelta se avvalersi o meno di questa app).

Peraltro le Linee guida aggiungono anche altre specificazioni, legate essenzialmente alla necessità che, per assicurare il raggiungimento della finalità dichiarata, il sistema adottato da uno Stato sia compatibile e interoperabile con quelli adottati in altri Stati, in ragione del fatto che, come dicono specificamente anche le Linee guida, l'epidemia e i virus non conoscono frontiere e che comunque le modalità di funzionamento delle app adottate in ciascun Paese assicurino una ragionevole raggiungibilità delle finalità che la giustificano.

Inoltre, le Linee guida ricordano la necessità che sia garantito il rispetto dei principi di *privacy by design* e *by default*; una idonea valutazione di impatto di rischio; misure di sicurezza adeguate in ordine al funzionamento complessivo dei trattamenti, coerenti con i rischi che questi comportano e con la delicatezza dei dati trattati.

Su questi ultimi aspetti, rigorosamente richiamati anche dal Garante italiano, non si può che esprimere apprezzamento, così come non si può non apprezzare che il Garante italiano, chiamato a esprimersi sulla compatibilità di Immuni con il quadro europeo e nazionale di protezione dei dati personali, col Provvedimento del 1 giugno 2020 recante "autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di alert Covid-19-App Immuni" del 1 giugno 2020, abbia dedicato specifica attenzione proprio anche a questi aspetti, sottolineando in particolare la adeguatezza della DPIA presentata dal Governo e relativa alla app Immuni, compreso l'uso della piattaforma Google/Apple, nel frattempo resa disponibile dalle due multinazionali (cfr. Provvedimento citato, punto 7). Merita inoltre sottolineare che proprio rispetto al contenimento dei rischi e al contenuto della DPIA, il Provvedimento citato contiene importanti ulteriori indicazioni di cui al punto 7.3, con particolare riguardo alla conservazione, alla protezione e alla finale cancellazione dei dati, giungendo anche a specificare le misure da adottare rispetto agli amministratori di sistema e dando tempo trenta giorni al Ministero della salute per comunicare le misure adottate.

Tuttavia, pur riconoscendo la attenzione dedicata dal Garante ad adeguarsi alle Linee guida dello EDPB e a definire anche gli ulteriori vincoli appena richiamati, è necessario sottolineare che le modalità con le quali si è operato, sia a livello italiano che europeo rispetto alla valutazione della compatibilità delle app di *tracing* con la legislazione UE sollevano molte perplessità.

Si tratta di aspetti sui quali giova richiamare l'attenzione anche per evitare che l'evoluzione di app di *tracing* possa svilupparsi secondo itinerari palesemente in contrasto con il GDPR e i principi fondamentali della protezione dei dati personali in UE.

Merita osservare, infatti, che il GDPR anche rispetto a quanto previsto nell'art. 9, apre la strada a sistemi di regolazione della tutela dei dati personali "paralleli" rispetto al GDPR (come dimostra il fatto che la norma riguarda casi in cui le regole generali a tutela di questo diritto possono essere "compresse") ma definisce sia i soggetti che alcune modalità essenziali perché ciò possa avvenire e, in particolare, fissa alcuni "paletti" che devono essere rispettati, nel caso che ci interessa in particolare rispetto all'utilizzazione di app a fini di *tracing* degli interessati.

Fra questi paletti, sempre con riguardo all'uso di queste app, vi è innanzitutto la necessaria valutazione del punto di equilibrio ragionevole tra la tutela dei dati personali e quella della tutela di altri diritti della persona, parimenti fondamentali, che potrebbero

essere compromessi dal doveroso e integrale rispetto delle norme di protezione dei dati personali.

Dunque, l'art. 9 entra in gioco proprio quando è necessaria una applicazione della normativa di tutela dei dati personali che, per le modalità con le quali avviene e i criteri che adotta, rispetti e tuteli anche altri diritti fondamentali, altrimenti a rischio.

In secondo luogo va sottolineato che la norma del GDPR prevede obbligatoriamente che tale valutazione sia fatta dal regolatore europeo o nazionale, proprio perché esso, essendo dotato di poteri regolatori, rafforzati da quanto previsto appunto dall'art. 9, può garantire anche una regolazione integrativa che assicuri garanzie e tutele adeguate a tutti i diritti fondamentali in gioco, così come può e deve valutare il corretto punto di equilibrio fra i diversi diritti tra loro in tensione, tenendo conto anche dell'ordinamento costituzionale proprio di ciascun Stato membro che, rispetto a molti diritti, anche fondamentali, varia, sia pure quasi impercettibilmente, da Stato a Stato, e delle regole fondamentali UE con le quali le norme statali formano sistema.

Dunque il quadro disegnato dall'art. 9 ha una sua logica e un suo spessore preciso e profondo: sì alla compressione delle regole di tutela dei dati personali quando siano a rischio altri diritti fondamentali, ma solo a condizione che la compressione avvenga nel rispetto di garanzie appropriate per i diritti fondamentali degli interessati, fra i quali potrebbe essere anche la richiesta di un consenso specifico alla comunicazione dei dati all'esterno del circuito rispetto al quale la raccolta dei dati è consentita in ragione delle sue finalità, come prevede ad esempio l'art. 9, par. 2, lett. *d*).

Così ricostruito il sistema che è alla base di quanto previsto dall'art. 9 del GDPR, si comprende bene perché il potere di consentire la compressione della regolazione generale a tutela dei dati personali sia rimesso solo al decisore UE o a quello degli Stati membri, secondo le regole generali proprie di ciascun Paese.

In sostanza il richiamo al regolatore UE o nazionale come uniche fonti in grado di legittimare trattamenti di dati personali fondati su basi giuridiche diverse da quelle richiamate nell'art. 9 stesso, prima fra tutte il consenso dell'interessato, costituisce a sua volta una ulteriore garanzia delle persone e della tutela dei dati ad esse riferibili.

La valutazione relativa all'equilibrio fra i diversi diritti potenzialmente o concretamente in gioco, infatti, è rimessa ai soli soggetti che possono provvedere adeguatamente non solo a consentire la "restrizione" delle regole del GDPR ma anche ad assicurare, contemporaneamente, garanzie adeguate a tutelare i diritti fondamentali delle persone interessate.

Da questo punto di vista il fatto che *ex* art. 9 i dati personali possano essere trattati anche al di fuori delle regole fondamentali della protezione dei dati personali, prima delle quali il consenso dell'interessato stesso, non è fungibile con l'accertamento fatto dalle Autorità di tutela dei dati personali, proprio perché tali Autorità, pur dotate anche del potere di dettare Linee guida relative alle modalità di attuazione della normativa generale di protezione dati (cfr. art. 57 e, per quanto riguarda lo EDPB, l'art. 70 del GDPR) non hanno però il potere di dettare nuove regole generali derogatorie di quelle contenute nel GDPR.

Dunque, l'eventuale sostituirsi delle Autorità di garanzia (anche riunite nello EDPB) ai regolatori UE o nazionali al fine di consentire o di condizionare "restrizioni" dell'ap-

plicazione delle regole generali del GDPR assicurando tuttavia la tutela di altri diritti fondamentali che potrebbero altrimenti essere compromessi, non appare possibile né compatibile con la regolazione europea nella materia che ci interessa.
Il punto è molto rilevante perché ovviamente indica un limite chiaro ai poteri delle Autorità garanti, che come tali non possono derogare alla normativa di tutela dei dati personali né condizionare la loro attuazione, né autorizzare con i loro provvedimenti una violazione di tali regole.
In questo caso, poi, la sottolineatura è particolarmente necessaria perché di fatto il GDPR non consente alle Autorità garanti, pur dotate di grandi poteri in materia di applicazione di queste norme, di autorizzare o addirittura imporre una loro interpretazione, o attuazione, che sia derogatoria delle norme stesse, soprattutto nel quadro di una normativa che come lo stesso EDPB e la sua Presidente Jelinek hanno ricordato più volte, a tal fine contempla, all'art. 9, la necessità dell'intervento del regolatore UE o di quelli nazionali.

5. Per completare questa riflessione, e renderla anche più equilibrata, merita sottolineare tuttavia che lo EDPB afferma con fermezza e con forza che comunque l'utilizzazione da parte degli utenti di app di tracciamento non può essere imposta per legge ma deve essere rimessa alla libera volontà dei cittadini. Solo ad installazione avvenuta in modo libero e consapevole (sulla base cioè di una informativa completa ed esaustiva circa il funzionamento della app, i dati raccolti, soprattutto se riferiti ai contatti con persone che risultino malate di Coronavirus, possono essere utilizzati dalla app, e da tutto il sistema di tracciamento ad essa collegato anche senza alcun consenso degli interessati. Anche in questo caso, infatti, non è in alcun modo previsto un consenso specifico, e persino l'inserimento dei dati relativi alla salute nel sistema costruito intorno alla app è riservato a operatori sanitari, per rispettare in tal modo almeno quanto previsto dalla lettera i) dell'art. 9 GDPR.
Proprio questa specificazione relativa all'obbligo di riservare al personale sanitario l'inserimento dei dati relativi alla salute delle persone che abbiano scaricato liberamente la app e quindi siano entrate "liberamente" a far parte di questo sistema di tracciamento è particolarmente interessante e meritevole di attenzione.
Questo richiamo e questo vincolo imposto al punto 31 delle Linee guida 04/2020, adottate il 21 aprile 2020, soprattutto in quanto accompagnato dal vincolo a che l'inserimento nel sistema dei dati sanitari richieda comunque l'intervento di un operatore sanitario tenuto al segreto professionale (cfr. anche punto 36 delle Linee guida citate), dimostrano con chiarezza che lo EDPB non ha voluto solo esprimere un parere favorevole rispetto alla app denominata Immuni, che infatti non viene presa in considerazione espressamente.
In sostanza, infatti, con queste Linee guida lo EDPB ha voluto dettare, in via generale, criteri interpretativi delle norme del GDPR, incidendo in tal modo anche sulla loro applicazione e, quindi, rendendo di fatto potenzialmente residuale l'intervento esplicito del decisore UE o di quello statale previsto dall'art. 9 del GDPR.
In realtà, tuttavia, le Linee guida dello EDPB sono ancora più sofisticate. Esse, infatti, si incardinano con evidente chiarezza in quanto previsto al punto 31, laddove si chia-

risce che le app che consentono tracciamenti, anche per le ragioni previste dall'art. 9, sono compatibili con il GDPR solo a condizione che non ne sia reso obbligatorio l'uso. Proprio nell'obbligo di prevederne la totale libertà di scaricamento sul device telefonico si incentra il contenuto essenziale di queste Linee guida, come dimostra il fatto che, in base al punto 32, il consenso diventa una base puramente "eventuale" di legittimità del trattamento. Resta fermo, tuttavia, che se la legittimazione dei trattamenti si basa essenzialmente sul consenso da parte dell'interessato questo implica poi che siano soddisfatti i requisiti collegati a tale base giuridica, primo fra tutti la revocabilità in qualunque momento del consenso stesso.

In sostanza, par di capire, il ragionamento che sottostà alle Linee guida adottate dallo EDPB è che secondo questo organo l'art. 9 fonda proprio sul consenso, considerato come la prima base giuridica che legittima il trattamento di dati personali relativi alla persona che tale consenso esprime, la tutela della sovranità degli interessati rispetto ai loro dati personali e, dunque, il rispetto della tutela dei loro dati come fondamento della libertà, e condizione essenziale per la tutela di tutti i diritti fondamentali previsti dalla UE.

È una evidente conferma di questo il fatto che se il consenso non è richiesto o previsto, allora lo scaricamento della app deve essere libero e non può in alcun modo essere imposto dalla legge.

In sostanza lo EDPB sembra aver ragionato nel senso che è possibile consentire l'uso di una app di tracciamento anche senza richiedere l'esplicito consenso dell'interessato solo a condizione che il suo scaricamento sia libero e mai imposto obbligatoriamente per legge (né, sembra doversi dedurre, per obbligo imposto da altri).

È chiaro che, in questo modo, il mancato consenso esplicito, che per altro comporta anche la revocabilità del consenso stesso, può essere pretermesso perché l'interessato è totalmente libero di decidere se scaricare o no la app e di conseguenza rendere possibili i tracciamenti e l'utilizzazione a tal fine della app scaricata (sempre ovviamente che la persona sia stata adeguatamente informata delle modalità di funzionamento della app e delle tutele relative ai trattamenti che saranno posti in essere, ivi compresa l'avvenuta elaborazione di una adeguata DPIA).

A queste condizioni, infatti, lo scarico dell'applicazione, purché accompagnato da una informativa coerente con i criteri di cui agli artt. 13 e 14, e con quanto stabilito dalla Linee guida in questione, può tenere il posto del consenso, il che evita di dover predisporre le modalità da seguire per esercitare il diritto alla revoca di un consenso che, altrimenti, dovrebbe essere sempre revocabile.

Tutto questo è confermato dal punto 32 che, infatti, ricorda coerentemente che se però una app di tracciamento si basa sul consenso, e dunque rispetta esplicitamente il primo dei criteri indicati dall'art. 9 del GDPR, allora è necessario che il sistema assicuri anche la soddisfazione di tutti i requisiti collegati a tale base giuridica, primo fra tutti la revocabilità del consenso stesso.

L'aspetto fondamentale delle Linee guida dello EDPB, presente già anche nelle lettere della sua Presidente Andrea Jelinek, sta dunque nell'aver di fatto sostituito il principio del consenso, quale presidio "principe" della libertà della persona legata all'uso dei dati che la riguardano, col diverso principio della libera scelta e decisione relative all'uso di

app o altri sistemi tecnologici che consentano di utilizzare, anche senza esplicito consenso, i dati personali per tracciare la persona alla quale essi si riferiscono.
Per contro, ovviamente, la possibilità per le Autorità garanti di adottare (o meglio imporre) misure di garanzia e tutela dei dati personali in un quadro derogatorio rispetto al GDPR è molto limitata. Lo dimostrano anche le Linee guida richiamate che, infatti, sostanzialmente richiamano, anche a titolo di rafforzarne l'effetto, obblighi già previsti dal GDPR, quali ad esempio, il dover procedere a una accurata DPIA circa i trattamenti posti in essere dalle app scaricabili, senza però aggiungere, né poter aggi ungere, nuovi obblighi specifici, eventualmente ragionevolmente connessi alla specificità dei rischi che l'uso della app può comportare. Il punto è interessante perché proprio i primi giorni di uso della app Immuni hanno fatto rilevare casi di allarmi inviati a specifici interessati senza che i dati a disposizione del sistema lo richiedessero e giustificassero, come espone anche l'avv. Lisi nell'articolo "*E se Immuni impazzisse? I primi segnali ci sono e finiremmo tutti prigionieri*", in *Il Fatto quotidiano* del 26 giugno 2020.
Da questo punto di vista le Linee guida dello EDPB sono estremamente istruttive perché, sulla stessa scia del divieto di rendere obbligatoria la installazione della app, richiamano, in termini di raccomandazioni o di vincoli, elementi già contenuti nello stesso art. 9 o comunque strettamente legati alla logica del GDPR, come ad esempio il principio di minimizzazione, di finalità, di valutazione di impatto e anche di interoperabilità delle app a livello UE. In particolare, quest'ultimo principio legato alla interoperabilità è indicato come strettamente legato al principio di finalità legata alla lotta all'epidemia. Tuttavia, la raccomandazione relativa alla interoperabilità a livello UE è fondata anche sulla necessità di assicurare un «clima di fiducia» necessario a «creare le condizioni per l'accessibilità sociale di qualunque soluzione e garantire pertanto l'efficacia di tali misure» (cfr. punto 3 delle Linee guida). Proprio quest'ultimo punto è particolarmente importante perché testimonia che lo EDPB è molto attento a richiedere sempre anche il pieno rispetto del principio di accountability relativo alle soluzioni proposte, nella consapevolezza che solo una applicazione "*accountable*" rispetto alle finalità perseguite è compatibile col GDPR, Solo a queste condizioni, infatti, tale applicazione può soddisfare anche le condizioni di affidabilità necessarie a ottenere la fiducia degli interessati rispetto ai trattamenti dei loro dati. Uno dei punti, questo, più importanti del sistema regolatorio relativo ai trattamenti dei dati personali così come disegnato dal GDPR

6. In sostanza almeno quattro sono gli aspetti essenziali che caratterizzano le Linee guida dello EDPB, tutti meritevoli di essere sottolineati con forza.
La messa al centro di tutto il ragionamento svolto del principio di "responsabilizzazione" che, anche nel significato terminologico della espressione, ha un significato diverso dal consenso. Ed è proprio grazie al fatto che implicitamente si sostituisce il consenso col principio di responsabilizzazione che si può considerare equipollente a un consenso non richiesto la decisione di scaricare la app, purché ovviamente questa decisione non sia obbligata o imposta dalla legge, né, sembra di poter dire, da alcun altro soggetto.
È evidente tuttavia che la sostituzione del concetto di consenso con quella di responsabilizzazione comporta anche una riflessione sul ruolo della informativa che deve essere

data. Se questa informativa deve essere finalizzata al rendere effettivo il principio di responsabilizzazione deve consentire una scelta "responsabile", e dunque basata sulla piena consapevolezza non solo del funzionamento della app ma anche delle sue finalità e delle conseguenze che il tracciamento può comportare sia per le persone che la hanno scaricata che per quelle i cui dati personali sono trattati dalla app stessa.
Inoltre, deve essere chiaro che se il principio di responsabilizzazione è soddisfatto solo grazie alla decisione non vincolata dell'interessato di scaricare la app sul proprio device, allora solo l'interessato può decidere responsabilmente sull'uso dei propri dati. Tutti gli altri, i cui devices entreranno eventualmente in contatto nel tempo, consentendo quindi trattamenti dei loro dati personali grazie a questa app non possono incidere in alcun modo sui trattamenti che ne seguiranno. È qui che, come si vedrà più avanti, torna ad essere essenziale il ruolo della informativa adeguata, giacché solo una informativa chiara e pienamente esaustiva sul funzionamento della applicazione può consentire a tutti gli interessati aderenti al sistema di conoscere sia i trattamenti dei loro dati già possibili al momento della decisione di scaricare la app che quelli che potranno essere effettuati nel tempo, mano a mano che la rete dei soggetti coinvolti per loro libera scelta nell'uso dell'applicazione, decideranno a loro volta di scaricarla.
Dunque, il principio di responsabilizzazione, come è ovvio, riguarda non solo e tanto i trattamenti che in concreto potranno essere posti in essere a seguito dello scarico della app quanto, e soprattutto, la tecnologia utilizzata e le conseguenze che essa può comportare in termini di trattamento dei dati in futuro.
In sostanza la decisione relativa a consentire i trattamenti dei propri dati è qualitativamente e giuridicamente diversa da quella relativa all'accettare o meno di servirsi di una specifica tecnologia scaricando la app relativa.
È ragionevole dire che le Linee guida avrebbero dovuto essere più chiare ed esplicite di quanto siano anche rispetto a questo specifico punto, relativamente, cioè, alla informativa da dare prima che la app sia scaricata.
Questo profilo è tanto più importante giacché, come le Linee guida sottolineano più volte, al caso in esame si applica non solo il GDPR e, in particolare, l'art. 9, ma anche la Direttiva e-Privacy 2002/58/CE e in particolare l'art. 5, che prevede anche deroghe ulteriori rispetto alle norme di tutela dei dati personali che siano collegate a trattamenti nell'ambito delle comunicazioni elettroniche.
È proprio in virtù dell'art. 5 della direttiva 2002/58/CE che lo EDPB precisa che comunque il consenso deve restare un principio rispettato come fondamentale per quanto riguarda l'uso dei dati raccolti attraverso la app liberamente scaricata per i fini previsti dall'art. 23 del GDPR.
Dunque, il principio del consenso, uscito dalla porta per far spazio al principio di responsabilità, rientra attraverso l'art. 5 della direttiva 2002/58, a dimostrazione di quanto rilevanti siano le conseguenze relative al mancato aggiornamento di questa direttiva. Aggiornamento che, nei piani della Commissione, avrebbe dovuto avvenire contestualmente alla entrata in vigore del GDPR.
Inoltre, il richiamo all'art. 5 della direttiva mostra anche i limiti della prospettiva seguita dallo EDPB nel formulare queste Linee guida.
Le Linee guida richiamano tutto questo al punto 13, ma poi non approfondiscono

adeguatamente su come tale consenso dovrebbe specificamente essere comunicato e raccolto, e da chi a chi, e quando e come.
Le Linee guida, infatti, soprattutto con riguardo ai dati relativi all'ubicazione degli interessati, preferiscono accentuare il principio della anonimizzazione dei dati e le modalità della applicazione.
Temi, questi, che occupano di fatto tutti i punti da 14 a 23 delle Linee guida e che, se correttamente applicati, consentono di superare il principio del consenso rispetto ai singoli trattamenti proprio perché i dati anonimizzati non sono considerati sottoposti ai limiti di trattamento previsti dal GDPR.
Ne consegue, dunque, che mentre da un lato si afferma di voler sottolineare il principio di responsabilizzazione in luogo di quello del consenso, dall'altro, in ultima analisi, si nega l'applicazione del principio del consenso non solo in virtù degli effetti di responsabilizzazione delle modalità tecnologiche adottate seguendo le indicazione dello EDPB ma anche perché esse consentono la anonimizzazione dei dati oggetto di raccolta e di trattamento e, dunque, permettono di escludere dalla applicazione della normativa di protezione dei dati personali i trattamenti relativi alle modalità di funzionamento dell' applicazione.
Ovviamente, così facendo lo EDPB sposta nuovamente il focus delle Linee guida dagli aspetti giuridici a quelli tecnologici e ciò non può non richiedere e imporre una informativa specifica verso gli interessati. Informativa che, ovviamente, deve essere fornita prima che la app sia scaricata perché riguarda proprio la decisione di scaricare o no la app e dunque l'aspetto essenziale dell'attuazione del concetto di "responsabilizzazione" così come impostato dallo EDPB.
Infine, con riguardo al principio di finalità, elemento essenziale per valutare sia la legittimità della raccolta dei dati che quella dei loro trattamenti, lo EDPB ribadisce che la finalità è legata alla lotta all'epidemia Covid-19. Il che significa che i trattamenti in tanto sono legittimi in quanto i dati trattati, sia con riferimento alla loro raccolta che alla loro utilizzazione, devono essere coerenti col perseguimento di tale fine che, come si è detto, secondo lo EDPB richiede la interoperabilità tra i sistemi adottati nei diversi Paesi e la messa in campo di trattamenti a tale scopo finalizzati almeno con riferimento al territorio degli Stati membri della UE (cfr. punto 6 della Linee guida).
Anche di questo, se il quadro deve essere quello della responsabilizzazione della persona e del rafforzamento della sua assunzione di responsabilità, va data adeguata informativa prima che la app sia scaricata, indicando anche, sembra naturale ritenere, quali siano le app utilizzate negli altri Paesi, come i dati raccolti da ciascuna di esse possano essere utilizzati da tutte e con quali tecnologie di protezione e tutela delle informazioni.
Purtroppo anche di questi aspetti nelle Linee guida dello EDPB non vi è praticamente traccia, mentre è qui che avrebbe potuto trovare spazio una soddisfacente analisi degli effetti dell'uso, da parte della app Immuni della piattaforma tecnologica comune di Google e di Apple, anche superando i problemi, tutt'altro che irrilevanti, legati al trasferimento dei dati all'estero e la scarsa garanzia di tutela rispetto ai trattamenti di tali dati potenzialmente svolti dai due soggetti titolari della piattaforma comune.

7. Infine, merita tenere presente che non è chiaro chi sia il destinatario delle Linee

guida.
Infatti, mentre il destinatario della lettera della Presidente Jelinek del 14 aprile 2020 è direttamente la Commissione nella persona del dr. Micol, a una specifica richiesta del quale la lettera stessa intende rispondere, le Linee guida del 21 aprile sono una autonoma iniziativa dello EDPB anche se, ovviamente, finalizzata a fornire indicazioni relative al fatto che, come si dice al punto 1, «Governi e soggetti privati si stanno orientando verso l'uso di soluzioni basate sui dati nell'ambito della risposta alla pandemia causata dal Covid-19, e ciò suscita numerose preoccupazioni in materia di tutela della vita privata».
Dunque, le Linee guida sono una autonoma iniziativa dello EDPB, i cui destinatari sembrano essere non tanto i legislatori o i decisori UE o statali, quanto direttamente le Autorità garanti di protezione dei dati personali. Solo a questi, infatti, possono essere rivolte indicazioni che fissano paletti relativamente all'uso, *compliant* con il GDPR, di app finalizzate al tracciamento delle persone.
Va detto inoltre che nelle Linee guida dello EDPB lo stesso riferimento alla situazione di epidemia come causa giustificativa dell'uso di app di tracciamento è assai poco richiamato. Soprattutto è assai poco sottolineata la connessione tra l'uso delle app di tracciamento dei dati e le eventuali esigenze di sanità pubblica, richiamate invece con forza dall'art. 9, par. 2, lett. *i*).
Infatti, il punto 4 delle Linee guida, a giustificazione dell'adozione delle app di tracciamento, non si riferisce tanto la lotta alla epidemia e ai motivi di interesse sanitario quanto piuttosto al fatto di «dare maggiori strumenti alle persone, piuttosto che stigmatizzarle o reprimerne i comportamenti».
Inoltre, aggiunge lo EDPB, «mentre i dati e le tecnologie possono essere strumenti importanti, essi hanno limiti intrinseci e non possono far leva sull'efficacia di altre misure di sanità pubblica». Il che significa che la compatibilità tra i tracciamenti dei dati relativi alle persone e le regole di protezione dei dati personali deve basarsi sul rispetto dei «principi di efficacia, necessità e proporzionalità da valutare rispetto a qualsiasi misura adottata dagli Stati membri o dalle istituzioni della UE che comporti il trattamento di dati personali per combattere il COVID-19» (cfr. punto 4 delle Linee guida).
Le Linee guida sembrano dunque collocarsi in una prospettiva molto diversa dall'art. 9 del GDPR non solo perché sostituiscono il principio di responsabilità al principio del consenso ma anche perché rovesciano completamente il rapporto tra ruolo di tecnologie di tracciamento e misure sanitarie decise dalla UE o dagli Stati membri. Non sono infatti le misure sanitarie e l'efficacia delle tecnologie adottate a raggiungere l'obiettivo i parametri sui quali valutare gli effetti delle app rispetto alla loro compatibilità con la normativa di tutela dei dati personali (come sembra essere nell'art. 9, par. 2, lett. *i*). Quello che, secondo queste Linee guida, deve guidare nella valutazione della compatibilità tre le app e il GDPR della app è il rispetto in sé dei principi di efficacia, necessità e proporzionalità, come indicatori delle finalità di tutela della libertà degli interessati, che la app deve concorrer a garantire attraverso i trattamenti dei dati da loro consentiti. Questa sembra, infatti, la ragione per la quale le Linee guida specificano che le app adottate e i dati raccolti e trattati «devono guidare qualsiasi misura adottata dagli Stati membri o dalle istituzione della UE che comporti il trattamento di dati personali per

combattere il COVID-19». Ed è in questa prospettiva che si comprende perché si precisi che il rispetto di questi principi deve essere verificato per stabilire la compatibilità delle misure adottate con il GDPR.
Insomma, a una prima lettura le Linee guida dello EDPB del 21 aprile 2020 sono un documento il cui scopo principale pare essere quello di superare il principio del consenso sostituendolo con quello di responsabilità, declinato essenzialmente con attenzione alle modalità tecnologiche legate all'utilizzazione delle app di *tracing* e, ma molto meno, con riguardo al contenuto specifico delle informative da fornire.
A una lettura più attenta, tuttavia, il vero effetto delle Linee guida è di fatto quello di sganciare il collegamento tra la adozione delle app e il loro essere *compliant* con il GDPR dal ricorrere delle circostanze di cui al par. 2, lett. *i*), dell'art. 9 del GDPR, e dunque da una specifica valutazione dei decisori unionale e nazionali sulla necessità dei tracciamenti per «motivi di interesse pubblico nel settore della sanità pubblica» (come invece afferma l'art. 9, par. 2, lett. *i*). Il collegamento sul quale si fonda la compatibilità col GDPR si basa unicamente, o essenzialmente, sul fatto di «dare maggiori strumenti alle persone», nel rispetto dei principi fondamentali della protezione dei dati personali, che vengono puntualmente richiamati al punto 4 delle Linee guida.
I punti più deboli, almeno a mio parere, sono tuttavia quelli legati alla mancanza di indicazioni chiare ed esaurienti circa le informative da fornire e il loro contenuto. Aspetti, questi, essenziali anche e soprattutto nel quadro del principio di responsabilizzazione e di quello relativo alla affermata necessità di rispetto della direttiva relativa alla vita privata e alle comunicazioni elettroniche, soprattutto con riguardo all'art. 5 e alla necessità di dare e avere specifici consensi relativi ai diversi trattamenti.
Si potrebbero richiamare anche altri aspetti, già accennati nel corso di questa analisi, ma è possibile fermarsi qui, non senza richiamare il fatto che le Linee guida ribadiscono il principio di finalità, estendendolo addirittura a un uso su scala continentale della tecnologia di tracciamento, senza poi individuare alcuna concreta modalità da adottare al fine di accertare che tale condizione sia rispettata e senza specificare a chi spetti compiere tale verifica.
È evidente, dunque, che le Linee guida in esame, mentre da un lato dimostrano concretamente l'importanza delle norme relative alla protezione dei dati personali anche di fronte all'utilizzazione, ai fini di trattamenti specifici, di nuove tecnologie che possono esaltare il principio di responsabilizzazione dell'interessato, dimostrano contemporaneamente quanto fondata sia l'esigenza di porre particolare attenzione a una "rilettura" delle stesse norme europee e delle loro modalità di applicazione, al fine di verificare la compatibilità delle nuove tecnologie con un sistema regolatorio certamente in forte tensione fin dal momento della sua entrata in vigore rispetto all'evoluzione di una realtà digitale in continuo mutamento e sviluppo.

8. Peraltro, come si è sottolineato più volte nel corso di questa analisi, il GDPR è stato, fin dall'inizio, perfettamente consapevole della possibilità che le tecnologie, soprattutto se usate per finalità di particolare rilievo, quali quelle ben indicate nell'art. 9 secondo capoverso, potessero implicare o richiedere il superamento di specifiche norme in esso contenute, o almeno applicazioni delle norme coerenti con le caratteristiche tecnologi-

che dei trattamenti di volta in volta previsti o disponibili.
Del resto, dello stesso fenomeno era già stata consapevole la direttiva relativa alle comunicazioni elettroniche e la vita privata del 2002. Ancora di più: proprio l'elasticità e adattabilità all'evoluzione delle tipologie di trattamenti strettamente connesse a tutta l'architettura del GDPR non è che la manifestazione "sistemica" della consapevolezza che l'evoluzione tecnologia è destinata inevitabilmente a richiedere letture innovative delle disposizioni del GDPR, e comunque applicazioni attente a rispettare più la sostanza del contesto normativo che la lettera delle singole disposizioni, specialmente dove una lettura prevalentemente burocratica diventasse impeditiva del raggiungimento di finalità che lo stesso GDPR mostra di apprezzare.
Il punto essenziale è che entrambe le richiamate normative UE, e soprattutto l'art. 9 del GDPR, rimettevano e rimettono ai decisori UE e nazionali la valutazione circa il "giusto punto di equilibrio" tra diritti fondamentali tra loro in tensione e la decisione su come assicurare che la compressione delle norme europee non avvenga pregiudicando ogni tutela e garanzia della protezione dei dati personali.
Nelle Linee guida in esame, invece, lo EDPB, sostituendo al principio del consenso quello della responsabilizzazione come via maestra per tutelare la libertà delle persone, individua una strada che consente allo EDPB stesso e poi alle singole Autorità garanti, senza necessità di intervento dei decisori UE e nazionali, di operare tale bilanciamento e verificarne, anche sotto i profili tecnologici, il rispetto.
Operazioni, queste ultime, che le Linee guida fanno sia rispetto all'art. 9 del GDPR, sostituendo il principio di consenso col principio di responsabilizzazione; sia affermando che la tecnologia può consentire di conciliare il raggiungimento delle finalità perseguite anche con la anonimizzazione dei dati, escludendo in tal modo la applicabilità delle regole di protezione dati sia del GDPR che della direttiva del 2002 sulla vita privata e le comunicazioni elettroniche.
Inoltre, con le Linee guida in esame lo EDPB fissa anche specifici principii e criteri che le tecnologie adottate devono garantire, soprattutto con riguardo al rispetto del principio di finalità dei trattamenti. In tal modo si rende superfluo, anche su questo piano, l'intervento del decisore UE e di quelli nazionali.

9. In questo quadro, che poggia largamente da un lato su una rilettura, spesso "compiacente" ma non per questo "inappropriata", della normativa UE, e dall'altro su una "analisi aperta e costruttiva" delle potenzialità delle tecnologie adottate, lo EDPB (e soprattutto le Autorità garanti nazionali) diventano anche, sia pure nell'ambito della compatibilità tra dettato normativo e innovazione tecnologica, i tutori di fatto della libertà delle persone legata alla tutela dei loro dati personali. Una tutela che, nel quadro delle Linee guida, appare molto più fondata sui limiti e i vincoli posti alle tecnologie usate e al loro rapporto coi principi di responsabilità e di finalità che non sulla difesa del principio del consenso come strumento essenziale di libertà, in virtù del quale nessuno può usare i dati di una persona se non per finalità stabilite dalla legge, o per tutelare i diritti fondamentali stessi dell'interessato, o senza il consenso adeguatamente informato di questi, salvo che si tratti di casi in cui i trattamenti sono esplicitamente consentiti dal legislatore cui spetta anche fornire altre e adeguate garanzie e tutele.

È pacifico dunque che le Linee guida in questione, se ben lette e contestualizzate dentro il quadro complessivo della tutela dei dati personali, costituiscono un salto di qualità molto importante, sia rispetto al ruolo delle Autorità garanti (e in particolare dello EDPB), sia rispetto al ruolo della normativa di protezione dei dati personali.

10. Rispetto al ruolo della Autorità garanti il salto di qualità operato dalle Linee guida è del tutto evidente.
Mentre il GDPR definisce in termini molti ristretti e, soprattutto, molto specifici, l'ambito regolatorio proprio delle Autorità, la prospettiva aperta dalle Linee guida appare fare dello EDPB una sorta di Corte costituzionale settorialmente competente in materia di tutela dei dati personali. Allo stesso tempo fa implicitamente delle Autorità nazionali il tramite attraverso il quale assicurare che le decisioni e le indicazioni dello EDPB siano concretamente rispettate, anche al fine di aumentare la fiducia dei cittadini nella tutela delle loro libertà. Senonché proprio il ruolo della Autorità garanti resta troppo implicitamente definito e potenzialmente anche non sufficientemente omogeneo.
Di fatto, proprio perché le Linee guida si limitano a indicare i vincoli essenziali a tutela dei cittadini che le attività di tracciamento devono rispettare rimettendo poi prima agli operatori e infine ai Garanti nazionali il compito di garantire che tali indicazioni siano rispettate, si potrebbe verificare facilmente una sorta di "geopardizzazione" della tutela dei dati personali a seconda del modo col quale le Autorità garanti esercitassero in concreto i propri impliciti poteri di vigilanza. È vero che la medesima cosa potrebbe accadere anche se si desse piena attuazione all'art. 9 attraverso regolazioni nazionali dei principi richiamati in quella norma, ma è vero anche che in questo caso il controllo sul decisore UE e sui decisori nazionali potrebbe essere facilmente esercitato dalla Corte di giustizia o dalle Corti nazionali, a seconda dei casi, e comunque i cittadini avrebbero la loro tutela legata direttamente all'intervento dell'autorità giudiziaria anche ai fini di controllo della compatibilità tra legislazione nazionale e normativa UE. Controllo, questo, certamente più "robusto" di quello di fatto rimesso alle Autorità garanti, anche perché le Corti possono adottare criteri più generali e meno legati ai singoli casi concreti di quanto possano fare invece le Autorità, il cui intervento è sempre legato ai singoli casi. Inoltre, non va dimenticato che, comunque, in questa ipotesi oggetto del controllo del giudice sarebbe la compatibilità col GDPR di regole adottate in forma di legge o con fonte assimilabile, e non valutazioni relative alle verifiche poste in essere rispetto alla adozione di tecnologie specifiche e alle relative tutele adottate.

11. Questo effetto delle Linee guida adottate dallo EDPB in occasione delle app di tracciamento nel contesto della epidemia di Covid-19 è particolarmente rilevante proprio perché, come si è detto al paragrafo precedente, le Linee già hanno ad oggetto il rapporto tra l'utilizzazione di app di tracciamento dei comportamenti delle persone in via generale e non specificamente nell'ambito della lotta all'epidemia di Covid-19.
Proprio questo aspetto, del resto, rende particolarmente importanti le riflessioni qui svolte. Infatti, la conseguenza delle scelte operate con le Linee guida 04/2020 va ben oltre il quadro legato alla lotta all'epidemia. Di fatto esse sembrano orientate a definire la base sulla quale fondare i vincoli di ogni app di tracciamento delle persone, quali che

siano le finalità di volta in volta perseguite.

12. Proprio queste ultime riflessioni giustificano che si chieda sia allo EDPB che ai Garanti nazionali maggiore cautela nel sostituirsi ai legislatori o, se si preferisce, ai decisori, soprattutto quando è la stessa normativa di protezione dei dati personali che rimette a questi ultimi il compito di garantire adeguate tutele agli interessati.
Su questo punto merita essere chiari. Per un verso la linea seguita dallo EDPB con la adozione delle Linee guida 04/2020 è assolutamente apprezzabile perché apre la strada a una ulteriore, e necessaria, flessibilità del GDPR, che in futuro potrà estendersi anche ad altre applicazioni tecnologiche, come ad esempio la blockchain e l'utilizzazione di forme più strutturate di bitcoin o di pagamenti in modalità telematica, anche ampliando l'uso della *privacy by design* o *by default*. Principi, questi ultimi, di carattere tecnologico di grande potenzialità, che il GDPR prevede ma che non hanno ancora trovato pieno sviluppo nel corso del biennio dalla sua entrata in vigore.
Inoltre, è assolutamente condivisibile e apprezzabile lo sforzo esplicito fatto dallo EDPB di sostituire, quasi senza dare a ciò troppa importanza, il principio di tutela della responsabilità della persona rispetto al principio del consenso come garanzia basica della possibilità di autotutela da parte degli interessati rispetto ai loro dati.
Non vi è dubbio, infatti, che il principio del "consenso", certamente molto efficace nella fase iniziale della normativa di protezione dei dati personali anche per il suo significato sostanziale, che ha sempre consentito di sottolineare che, almeno in via generale e salvo le eccezioni legislativamente specificate, nessuno può trattare dati di un altro senza il suo consenso, proprio perché i dati personali sono della persona alla quale si riferiscono, è venuto via via mostrando tutti i suoi limiti, soprattutto dal punto di vista della inevitabile connessione col principio secondo il quale laddove il consenso è necessario questo deve poter essere sempre revocabile.
È ovvio che, in un contesto nel quale le tecnologie evolvono continuamente, la possibilità di revocare in qualunque momento il consenso già dato al trattamento di propri dati personali può determinare conseguenze negative nei confronti di un numero indefinito di interessati, come certamente avverrebbe nel caso di immuni, soprattutto laddove il sistema nel suo complesso riuscisse davvero, una volta a regime, a garantire una forte tutela nei confronti di tutti coloro che avessero deciso di aderire ad esso scaricando di conseguenza la app Immuni.
Va detto che, anche per questo, appare anche particolarmente "sottile" e "interessante" la scelta di puntare tutto sul principio di responsabilità piuttosto che sul consenso, imponendo a tal fine che la scelta di scaricare o meno la app sia riservata gelosamente e unicamente ai potenziali interessati. Una scelta che in questo caso è resa possibile dalla necessità di scaricare la app, che non è preinstallata sui devices. Si tratta tuttavia di una linea che appare difficilmente conciliabile col fatto, che le Linee guida sottolineano, secondo il quale perché il sistema sia efficace è fondamentale che un ampio numero di interessati abbiano scaricato sui loro devices la app (cfr. Linee guida, n. 6).
Appare dunque particolarmente "forte" il collegamento fatto dalle Linee guida tra la assoluta volontarietà dell'installazione della app di tracciamento sul proprio telefonino e il principio di responsabilità. Il collegamento, per la verità non troppo esplicito, tra

questi due aspetti è molto rilevante anche in prospettiva, tanto più perché è applicato anche in un contesto nel quale, perché il sistema raggiunga in modo affidabile le sue finalità e i suoi scopi, è necessario che la app sia scaricata da una percentuale molto elevata di cittadini: cosa quest'ultima che avrebbe caso mai potuto spingere a chiedersi se, perché tutto il sistema sia davvero efficace e raggiunga i propri scopi, non si sarebbe caso mai dovuto ragionare in modo opposto, superando il principi del consenso in favore della obbligatorietà piuttosto che della piena e autonoma libertà di scaricamento. Anche per questo è evidente l'attenzione che lo EDPB ha riservato alla gelosa tutela della salvaguardia della libertà e della autonomia delle persone. Ed è proprio da questo punto di vita che le Linee guida in esame possono avere specifico rilievo anche in futuro, rispetto a ulteriori e diverse utilizzazioni di altre innovazioni tecnologiche, ivi comprese ovviamente nuove e divere app di tracciamento per finalità diverse da quelle del caso in esame.
È evidente, insomma, che lo EDPB ha ritenuto opportuno cogliere questa occasione non solo per indicare i vincoli che il ricorso al tracciamento di dati personali tramite app deve rispettare, ma anche per riaffermare la necessità di una interpretazione e applicazione "flessibile" delle norme di protezione dati, irrobustendo nell'occasione la più rigorosa tutela della libertà della persona e del principio di responsabilità, assicurato in questo caso grazie alla libertà di scelta dell'interessato di avvalersi o meno della app.
È chiaro inoltre che queste Linee guida, che pure rimettono a ciascuna app il compito di adeguarsi alle indicazioni date, adottando DPIA efficaci a valutare i rischi e ad assicurando misure conseguenti, anche con riguardo ai punti specifici analizzati dalle Linee guida stesse (cfr. soprattutto la parte 3.2. delle Linee guida), aprono la via a una evoluzione futura molto importante del ruolo dei poteri dello EDPB e elle Autorità garanti nazionali.

13. In sostanza, la decisione di sostituire con indicazioni date dallo EDPB e dai Garanti nazionali, ai quali spetta poi verificarne anche il rispetto, le indicazioni che invece, sia *ex* art. 9 che art. 23 del GDPR sarebbero spettate caso mai al decisore unionale o a quelli statali, costituisce un salto in avanti molto forte rispetto alla lettura finora data della flessibilità del GDPR e del ruolo delle Autorità di Garanzia.
Di fatto queste Linee guida trasformano la flessibilità propria del GDPR nel fondamento di una attività multifunzionale delle Autorità garanti. Ne deriva una espansione molto forte del ruolo delle Autorità e dei poteri consultivi loro riconosciuti, che è già in parte adombrata in numerose norme del GDPR ma che trova ora in queste Linee guida le premesse, anche teoriche, di un suo rapido sviluppo.
Di tutto questo ci accorgeremo rapidamente e probabilmente in modo particolare proprio con riguardo alle app di tracciamento che sono certamente destinate a moltiplicarsi e il cui uso potrà interessare molti settori diversi, anche lontani dal settore sanitario e, ancor più, dal fenomeno epidemico.
A questo si deve aggiungere fin da ora la prevedibilissima espansione delle premesse già indicate in queste Linee guida, che potranno essere utilizzate per ampliare il ruolo delle Autorità garanti e delle loro Linee guida anche a nuove, già oggi prevedibili e in atto, innovazioni tecnologiche, a partire proprio dalla precisazione di come attuare i

principi di *privacy by design* e *by default* nei settori di maggior sviluppo tecnologico nei prossimi anni.
Né è difficile pensate che sulla strada aperta dalle Linee guida in commento le Autorità garanti saranno tentate (e forse anche richieste) di dare indicazioni importanti sia sull'uso delle applicazioni basate sull'Intelligenza Artificiale che di quelle funzionali a una espansione ampia, e già in pieno sviluppo in mezzo a noi, della robotica "intelligente", che può andare dalle macchine a guida autonoma fino ai robot antropomorfi.

14. Tutte le considerazioni svolte spingono dunque a richiamare con forza l'attenzione sulle Linee guida 04/2020 dello EDPB, non solo e non tanto per gli aspetti relativi alla app Immuni o alle app di tracciamento quanto, e soprattutto, per il rilevante mutamento che esse comportano sia rispetto al ruolo dei Garanti che alle modalità di evoluzione della normativa di protezione dei dati personali e delle sue applicazioni rispetto alla prevedibilissima e inevitabile crescita della società digitale e delle sue applicazioni future.
Né è possibile affermare che questo fenomeno sia censurabile giacché è sempre più evidente che lo sviluppo del mondo digitale e dei trattamenti dei dati ha subito una enorme accelerazione con il verificarsi dell'epidemia, aprendo così la strada al passaggio del mondo e degli esseri umani che lo abitano a una fase del tutto nuova, nella quale è chiara la centralità dei dati e delle loro modalità di analisi, da un lato, la continua difficoltà di individuare il punto di equilibrio corretto tra la tutela del diritto fondamentale alla tutela dei dati, specialmente personali, che nella società digitale è l'architrave di ogni libertà, con la tutela non solo degli altri interessi e diritti fondamentali individuali (da quello alla salute a quello della difesa della vita stessa) ma anche dei diritti fondamentali collettivi, che spesso possono trovare nel trattamento di quantità sempre crescenti di dati la condizione per la loro piena espansione e per l'ottimizzazione dell'uso delle nuove tecnologie per la sicurezza e la tutela dei valori fondamentali sia degli individui che delle collettività sociali alle quali essi appartengono.
Di qui non solo l'enorme accelerazione che lo sviluppo della società digitale avrà nei prossimi anni ma anche il manifestarsi sempre più evidente che a una nuova fase della storia del mondo deve accompagnarsi un profondo ripensamento delle sue regole giuridiche e un forte rafforzamento delle tutele essenziali per le libertà fondamentali degli esseri umani.
In pericolo c'è certamente la libertà individuale ma c'è anche, e molto e molto di più, la natura ontologica stessa della libertà degli esseri umani, almeno così come la percepisce la cultura, la filosofia e la scienza di matrice occidentale.
Tutto questo consente di dire che non solo sarà molto importante seguire con attenzione come i principi e le regole contenuti in queste Linee guida saranno sviluppati e troveranno attuazione rispetto alle app di tracciamento (a partire ovviamente da Immuni). Sarà anche molto importante osservare se e come le Autorità garanti e lo EDPB intenderanno nel prossimo futuro sviluppare i principi che sottostanno a queste Linee guida, anche allo scopo di aprire una nuova stagione nella quale le Autorità devono essere impegnate anche a garantire non solo una adeguata flessibilità della protezione dei dati personali di fronte allo sviluppo delle tecnologie, ma anche e soprattutto un

crescente, importante e prezioso ampliamento del loro ruolo di Autorità garanti.
Autorità che nel nuovo mondo digitale dovranno sempre meno essere guidate da una visione burocratica di controllo sull' applicazione delle norme per privilegiare invece sempre di più una tutela dinamica della salvaguardia dei loro contenuti e dei valori che vi sottostanno. Una attività capace di sviluppare e adeguare i principi fondamentali della tutela di questo diritto (essenziale per la libertà di tutti e di ciascuno) alla nuova fase della storia nella quale, anche come effetto del Coronavirus, ormai tutto il mondo è coinvolto.
Non vi è dubbio che tutto questo è perfettamente coerente allo spirito e all'ampiezza di visione del GDPR, che non a caso ha così fortemente rafforzato i poteri regolatori delle Autorità e il ruolo dello EDPB come garante dell'omogeneità dello sviluppo delle attività proprie dei Garanti. Non vi è nemmeno dubbio, tuttavia, che tutto questo comporta che anche le Autorità e i cultori della protezione dei dati personali sappiano rapidamente sviluppare forme nuove e proattive di approccio ai temi che sono e saranno chiamati ad affrontare.
Il tempo futuro non può essere quello dominato da un diritto minuziosamente prescrittivo e da norme descrittive e regolatrici di ogni profilo possibile dei beni e dei valori fondamentali che intendono proteggere. Il mondo nuovo, e tanto più la sua dimensione digitale, comportano, come il GDPR dimostra in ogni sua prescrizione, un atteggiamento assai più attento a tutelare i valori fondamentali della libertà delle persone, garantendo il controllo sui loro comportamenti e la salvaguardia dei loro dati da usi illeciti o così invasivi da privare le persone di ogni effettiva libertà, spesso senza neanche garantire davvero nuove sicurezze.

15. Il mondo nuovo ha bisogno un diritto che di molta più attenzione ai valori in gioco e alla loro tutela, in sostanza ha bisogno di un "diritto per valori".
Ma un "diritto per valori" ha a sua volta bisogno inevitabilmente di strutture di enforcement e di tutela delle legalità agili; capaci di adattare velocemente le regole al modificarsi delle situazioni; attente ad arginare gli sviluppi della tecnologia senza impedirne i progressi; capaci di tutelare le libertà, non negandole ma regolandole.
In questo quadro sono da temere tutti gli atteggiamenti che mettano al centro i divieti e i vincoli, anche perché spesso, come ha detto il giudice Calabresi in un importante Convegno dell'Osservatorio Giordano dell'Amore tenutosi a Milano l'11 ottobre 2017 dal titolo "*Fake news e allarme sociale*: *responsabilità non censura*", il mondo attuale, e tanto più quello digitale in evoluzione, non hanno bisogno di eventuali divieti imposti sulla base di una realtà in continuo cambiamento. Al contrario: hanno bisogno di chi sappia accompagnare la tumultuosa evoluzione della società salvaguardandone i valori fondamentali e agendo sempre in modo da non pregiudicare con i divieti di oggi i progressi di domani.
In una parola: in un mondo caratterizzato dal cambiamento accelerato e continuo non abbiamo bisogno di regole ma di regolatori e i regolatori di cui abbiamo bisogno non sono quelli che sanno meglio applicare regole formalistiche a realtà in continuo cambiamento ma quelli che sanno guidare, regolare, inseguire i cambiamenti, mettendo sempre al centro gli uomini e le donne e i loro diritti fondamentali, primo dei quali è

in assoluto la libertà degli esseri umani di scegliere e decidere in modo responsabile, sapendo valutare gli effetti delle loro decisioni e avendo sempre presente che di questi effetti sono responsabili a seconda del ruolo e dei poteri esercitati, e dunque possono in qualunque momento essere chiamati a rispondere.

Lette in questa prospettiva le Linee guida 04/2020 sono particolarmente importanti ed è interesse e dovere di tutti vigilare sulla loro attuazione e su come le Autorità sapranno interpretare il ruolo che esse stesse si sono date approvandole.

Insomma, la protezione dei dati personali e con essa le Autorità che ne sono garanzia sono all'inizio di una nuova stagione, entusiasmante e complessa, così come certamente entusiasmante ma anche molto complessa è la nuova fase nella storia del mondo che da anni stiano vivendo e che l'epidemia del Coronavirus ha accelerato ogni oltre previsione.

Saggi

Regolare Internet*

Michela Manetti

Abstract

Il saggio affronta due temi che mettono in luce la tendenziale coincidenza tra due modelli – quello europeo e quello statunitense – tradizionalmente ritenuti assai diversi riguardo alla disciplina della libertà di pensiero. Da un lato viene esaminata la repressione dei messaggi di odio, in particolare della propaganda del nazismo e del terrorismo; dall'altro l'abbandono ai privati della gestione della Rete, e in particolare l'esenzione da responsabilità dei proprietari delle piattaforme, oggi messa in discussione, almeno in parte, dalla dottrina statunitense e dalla disciplina eurounitaria.

The paper addresses two themes that highlight how two different models of protection of free speech – namely the European and the US ones – tend to coincide, despite being inherently considered very different. The paper examines, on one hand, the contrast of hate speech, particularly of Nazi and terrorist propaganda; on the other hand, it looks at how the governance of the Internet has been left completely to the private sector, being centered on the liability exemptions applicable to digital platforms, the adequacy of which is currently called into question by both US scholars and European regulators.

Sommario

1. L'inversione di tendenza. – 2. Il pensiero estremo e le sue diverse manifestazioni. – 3. (segue): le politiche di odio e di disinformazione in Rete. – 4. Potere economico e libertà di pensiero. – 5. L'imposizione di obblighi di sorveglianza e i rischi della censura privata. – 6. La manipolazione degli utenti.

Keywords

libertà di espressione – Internet – Internet service provider – censura privata – *hate speech*

1. L'inversione di tendenza

L'esplosione della pandemia ha reso se possibile ancora più importante il ruolo della Rete, amplificandone a dismisura l'influenza su tutti gli aspetti della vita quotidiana. Ciò rende indispensabile una riflessione aggiornata, che tenga conto della rapidissima

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

obsolescenza cui sono andate incontro le visioni originarie del fenomeno.
In pochi anni è crollata l'idea della Rete come luogo di appagamento sia del bisogno di comunicazione interpersonale, sia della sete di conoscenza, in quanto tale destinata a divenire anche il luogo di elezione del dibattito democratico. Dopo l'avvento dei *social media* il tema si è per così dire rovesciato, concentrandosi sugli aspetti meno benefici della libertà di comunicazione-diffusione del pensiero; tema che a sua volta si staglia sullo sfondo (in precedenza oscurato dalla pretesa gratuità della Rete) dell'eterno conflitto tra mercato e democrazia.
Sicché oggi in tutto il mondo, e non da ultimo negli Stati Uniti, si discute accanitamente non più sulla necessità, ma sui modi con i quali regolare efficacemente l'uso di Internet[1]. Per alcuni questo non significa negare il paradigma del *marketplace of ideas*, dove al pensiero spetta una speciale tutela in vista della sua funzione sociale, ma sconfessare la retorica deregolatoria della quale il I emendamento è stato arbitrariamente elevato a simbolo[2]. Per altri ciò rappresenta invece la dimostrazione del fatto che è il modello stesso del *marketplace* ad essere sbagliato, in quanto nel dibattito la verità non sarebbe affatto destinata a trionfare[3].
Si tratta di un dibattito che l'esplosione della pandemia ha reso se possibile ancora più decisivo, amplificando a dismisura l'influenza di Internet su tutti gli aspetti della vita quotidiana.

2. Il pensiero estremo e le sue diverse manifestazioni

Si deve senza dubbio all'uso della Rete se, dopo un lungo periodo nel quale sembrava che nessun messaggio potesse più veramente scandalizzare, né mettere in pericolo l'assetto democratico, è risorto ovunque il tema dei discorsi che aggrediscono in forme estreme e intollerabili i principi culturali, prima ancora che giuridici, delle democrazie fondate sui diritti: per un verso, il messaggio pedo-pornografico, per l'altro, l'incitamento all'odio razziale. Ma risorto è anche il tema della propaganda diretta al sovvertimento violento dello *status quo* tramite l'esaltazione del terrorismo[4].
L'esperienza vissuta a quest'ultimo riguardo dai diversi ordinamenti ha confermato la chiave di lettura che era stata proposta nel 1988, quando la distinzione tra i due modelli

[1] V. ad es. i contributi raccolti da L.C. Bollinger-G.R. Stone (a cura di), *The Free Speech Century*, Oxford, 2019, che (tranne quello dovuto a Monica Bickert, dirigente di Facebook) convergono tutti nel ritenere necessaria una regolazione delle piattaforme, sia pure di diverso tenore a seconda delle opinioni.

[2] Ivi, G.R. Stone, *Epilogue*, 295, ammette che la Rete, se lasciata libera, non corrisponde affatto al paradigma del *marketplace of ideas*, ma anzi rappresenta una minaccia per la democrazia. F. Schauer, *Every Possible Use of Language?*, ivi, 45, ricorda opportunamente che secondo questo paradigma il pensiero va tutelato non perché non sia pericoloso, ma nonostante lo sia, in quanto può tradursi in azione. Sulla "retorica deregolatoria" del I emendamento v. *amplius infra* il par. 4.

[3] Per un approccio dichiaratamente ostile al paradigma del *marketplace of ideas* v. A. Koltaj, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere,* Oxford-Chicago, 2019, 10, secondo il quale l'apertura del dibattito non porta necessariamente né alla verità, né alla individuazione della migliore decisione nelle materie di pubblico interesse.

[4] Cfr. la tematizzazione operata da I. Hare-J. Weinstein (a cura di), *Extreme speech and democracy,* Oxford, 2009.

astrattamente comparabili (nordamericano ed europeo) veniva ricondotta non tanto a una diversa e opposta visione del mondo, quanto a un atteggiamento e a un sentimento di ottimismo, anziché di pessimismo, liberale[5]. Dal punto di vista costituzionalistico il volgersi dell'ordinamento al pessimismo veniva comunque limitato al ricorrere di circostanze eccezionali, ovvero alla "enormità dei valori costituzionali" che debbono essere protetti a ogni costo attraverso l'imposizione di un ordine pubblico ideale democratico[6].

In effetti l'ottimismo statunitense di un tempo, esemplato dal test del pericolo imminente che era stato introdotto nel 1969 dalla famosa sentenza *Brandenburg v. Ohio*[7], ha lasciato spazio a un pessimismo non meno profondo, quando si è trattato di valutare la legittimità delle disposizioni che permettono di classificare come forme di *material support* al terrorismo non solo determinati comportamenti, ma anche semplici manifestazioni del pensiero. Nel caso *Humanitarian Law Project* si trattava dell'attività di consulenza legale rivolta a gruppi terroristi[8]; nel successivo caso *Tarek Mehanna* si trattava invece della traduzione di messaggi diffusi da un'organizzazione terroristica, svolta peraltro di propria iniziativa dall'imputato[9].

Come molta dottrina ha notato, la Corte Suprema non ha minimamente pensato di applicare a tali casi il criterio del pericolo imminente, grazie al quale la sua giurisprudenza è conosciuta in tutto il mondo, ma al contrario ha permesso l'incriminazione di una "semplice simpatia" verso l'ideologia dei terroristi musulmani: qualcosa di molto simile al *bad tendency test* che a tanti anni di distanza da *Brandenburg v. Ohio* sembrava morto e sepolto. Il periodico riemergere dell'isteria popolare alla quale i tribunali non vogliono o non riescono ad opporsi può considerarsi a questo punto una caratteristica costante del sistema statunitense, che smentisce l'impressione di un progressivo e inarrestabile ampliamento della libertà di pensiero.

Mentre il nemico mortale era un tempo il comunismo, oggi lo è il terrorismo – non a caso definito da un tribunale nordamericano "la peste bubbonica dei tempi odierni"[10] – al punto da richiedere la messa al bando di qualsiasi messaggio anche indirettamente o debolmente apologetico. E se un tempo si citava la formula coniata dal giudice

---

5 A. Di Giovine, *I confini della libertà di manifestazione del pensiero*, Milano, 1988. Ma sulla sostanziale convergenza dei due modelli v. già A. Baldassarre, *Privacy e Costituzione: l'esperienza statunitense*, Roma, 1974, 178 ss.

6 V. ancora A. Di Giovine, *Il passato che non passa*: *"Eichmann di carta" e repressione penale*, in *DPCE,* 2006, XIII ss.

7 395 U.S. 444 (1969).

8 Corte Suprema, *Holder v. Humanitarian Law project*, 561 U.S. 1 (2010). Imputata era un'organizzazione di consulenza che seguiva il Partito Curdo dei Lavoratori e le Tigri per la liberazione del Tamil – entrambi presenti nella lista statunitense dei gruppi terroristi – sia nell'opera di compilazione dei ricorsi per la violazione dei diritti umani presso l'ONU, sia nella conduzione di negoziati di pace con i rispettivi governi.

9 Court of Appeals, First Circuit., *U.S. v. Mehanna*, 735 F.3d 32 (2013), del 13 novembre 2013. V. al riguardo la rassegna di E. Grande*, I mobili confini della libertà di espressione negli Stati Uniti e il metro della paura,* in *Questione giustizia*, 4, 2015, 47 ss. V. anche M. Monti, *L'hate spech jiahdista e l'ordinamento giuridico statunitense post 11 settembre: un maccartismo culturalmente orientato*? in S. Prisco - F. Abbondante (a cura di), *Diritto e pluralismo culturale. I mille volti della convivenza*, Napoli, 2016, 287 ss.

10 Cit. da E. Grande, *I mobili confini della libertà di espressione negli Stati Uniti e il metro della paura,* cit., 57.

Learned Hand[11], oggi si preferisce il più sintetico motto intestato ad Abramo Lincoln, secondo il quale «la Costituzione non è un patto suicida»[12].

Uguale e contrario è stato il percorso seguito dalla Repubblica federale tedesca, la quale ha progressivamente rinunciato a difendersi da qualsiasi messaggio che contesti "i principi fondamentali dell'ordinamento liberal-democratico". Nel 2017 il Tribunale costituzionale federale si è spinto invero a condizionare lo scioglimento di un partito di ispirazione nazista alla sua effettiva pericolosità, instaurando un esplicito bilanciamento tra la scelta in favore della democrazia militante, da un lato, e la scelta tesa invece all'apertura del processo politico, dall'altro. Attribuendo carattere eccezionale alla misura dello scioglimento prevista dall'art. 21, c. 2, della Legge fondamentale per i partiti dichiarati incostituzionali, questa sentenza si pone a ben vedere in continuità con l'altra risalente a dieci anni fa, nella quale lo stesso Tribunale aveva bensì ribadito l'intollerabilità per l'ordinamento tedesco dell'esaltazione del nazismo, ma aveva al contempo tenuto a sottolineare che questo limite alla libertà di pensiero ha carattere eccezionale, trovando radice nell'unicità e irripetibilità dell'esperienza subita dai tedeschi sotto il Terzo Reich[13].

In entrambe i casi il giudice costituzionale fa ottimisticamente propria la natura derogatoria dei limiti imposti alle libertà costituzionali in nome dell'ordine pubblico democratico, dimostrando di saper rivolgere la barra ai principi dello Stato di diritto pur in una temperie burrascosa. Su questa strada sa di non essere solo, come dimostra la più recente giurisprudenza della Corte EDU in tema di negazionismo[14], che fa eco a sua volta alla presa di posizione del Tribunale costituzionale spagnolo[15], nonché al (più contorto) pronunciamento del Consiglio costituzionale francese in favore della libertà di pensiero e di ricerca storica [16].

---

[11] Standard poi accettato dalla Corte Suprema nel caso *Dennis v. U.S.*, 341 U.S. 494 (1951): «*In each case courts must ask whether the gravity of the evil, discounted by its improbability, justifies such invasion of free speech as necessary to avoid the danger*».

[12] Al motto ha ridato lustro il volume di R.A. Posner, *Not a Suicide Pact. The Constitution in a Time of National Emergency*, Oxford, 2006.

[13] Sentenza del 4 novembre 2009, in *BVerfGE* 124, 300-347, che ha ritenuto legittimo il divieto di una riunione convocata per celebrare la memoria di Rudolf Hess.

[14] V. la sentenza resa in *Grande Chambre* il 15 ottobre 2015 sul caso *Perinçek c. Svizzera*, ric. 27510/08, con la quale la Corte EDU – discostandosi dalla giurisprudenza riguardante l'Olocausto − ha ritenuto che la negazione del genocidio armeno possa rappresentare un messaggio protetto, ove non crei in concreto pericolo di violenza né rappresenti istigazione all'odio nei confronti delle vittime e dei loro discendenti.

[15] Cfr. *Tribunal constitucional*, sentenza n. 235/2007, che ha ritenuto incostituzionale la incriminazione del mero "negare" la esistenza dei delitti di genocidio, lasciando peraltro intatte le sanzioni previste per coloro che giustifichino tali delitti o pretendano la riabilitazione dei regimi o istituzioni che supportano dette pratiche. A seguito di tale pronuncia il legislatore spagnolo ha modificato le norme penali in materia, suscitando tuttavia numerose critiche: cfr. G.M. Teruel Lozano, *La libertad de expresión frente a los delitos de negacionismo y de provocación al odio y a la violencia: sombras sin luces en la reforma del código penal*, in *indret.com*, 2015.

[16] *Conseil constitutionnel*, sentenza n. 2012-647 DC, con la quale è stata dichiarata illegittima non la incriminazione della negazione del genocidio, bensì la pretesa delle *lois mémorielles* di riconoscere come verità storica determinati genocidi (a differenza di quanto l'ordinamento francese prevede riguardo all'Olocausto, che viene riconosciuto dall'ordinamento francese in osservanza delle sentenze pronunciate dalla giurisdizione internazionale appositamente istituita dopo la Seconda Guerra mondiale). Tale

Non bisogna del resto dimenticare che il *Bundesverfassungsgericht*, nel mandare indenne da sanzione il partito neonazista ha altresì auspicato, con successo, l'introduzione di una norma costituzionale *ad hoc* che privasse del finanziamento pubblico i partiti miranti ad attentare all'ordinamento costituzionale democratico e liberale, o a mettere in pericolo l'esistenza della Repubblica federale tedesca: una fattispecie più ampia e quindi di più facile applicazione rispetto a quella prevista per la dichiarazione di incostituzionalità del partito[17]. Tale esito, che sancisce non solo la condanna dell'ideologia del partito, ma ne rende più difficile l'attività di propaganda, privandolo di risorse, appare molto più efficace della mera sanzione dello scioglimento, la quale in base all'esperienza non è mai servita a impedire la nascita di partiti identici sotto nome diverso[18].
In controluce si legge la valutazione di opportunità politico-costituzionale svolta dal Tribunale: il rifiuto di incriminare l'"atteggiamento interiore" o "la visione del mondo" degli aderenti al partito neonazista[19] procede evidentemente dalla volontà di dimostrare la superiorità del sistema democratico, oltre all'ampiezza del consenso che lo sostiene. Non diversamente molti anni fa la Corte costituzionale italiana mandò indenni da sanzione l'apologia di fascismo e le manifestazioni fasciste che non risultino idonee a minacciare l'ordine democratico ai sensi della XII disp. trans. fin. Cost.[20]. Bisogna insomma tenere presente che – soprattutto in tempi di populismo dilagante – le manifestazioni di forza possono apparire sintomi di debolezza dell'intero *establishment*. Fermo restando che, quando non si tratti di personaggi politici conosciuti dal grande pubblico o, peggio, di rappresentanti delle istituzioni (cui la libertà di pensiero individuale è in pratica difficilmente riconoscibile, tanto più se essi scelgono di utilizzare mezzi accessibili a tutti, come i social media) la diffusione di messaggi anti-sistema non si sconfigge con le troppo facili incriminazioni penali. Tanto si è fatto, invece, nel nostro Paese con l'introduzione dell'aggravante di negazionismo[21], e tanto

riconoscimento non rappresenterebbe infatti esercizio del potere normativo «in senso sostanziale» che la Costituzione francese attribuisce alle Assemblee rappresentative. In altri termini, il *Conseil* ha negato che spetti alla legge dettare la storia: per una riflessione generale su questo tema v. G. Resta-V. Zeno Zencovich, *La storia "giuridificata"*, in G. Resta-V. Zeno Zencovich (a cura di), *Riparare Risarcire Ricordare*, Napoli, 2012, 3 ss.

17 Sul significato del nuovo c. 3 dell'art. 21 della Legge fondamentale, e in particolare sul verbo "*darauf ausgerichtet sein*" (mirare) che viene qui usato in contrapposizione a "*daraus augehen*" (adoperarsi per) cui il c. 2 fa seguire la messa fuori legge del partito v. l'ottima discussione di E. Caterina, *La metamorfosi della democrazia militante in Germania*, in *DPCE*, 1, 2018, 239 ss.

18 In tal senso non sembra di poter condividere lo sgomento provato davanti alla sentenza in esame da M. Bonini, *La democrazia alla prova dei suoi valori: ripudiare il partito neonazista tedesco senza scioglierlo,* in *Osservatorio AIC*, 2, 2017, 17.

19 Nelle parole del Presidente Voßkuhle: «*Das Parteiverbot ist kein Gesinnungs- oder Weltanschauungsverbot*».

20 Cfr. le sentenze Corte cost., 26 gennaio 1957, n. 1 e 6 dicembre 1958, n. 74. V. altresì la Corte cost., 6 giugno 1973, n. 73, nella quale si ribadisce che la legge Scelba «intende vietare e punire unicamente quelle manifestazioni che, in relazione alle circostanze di tempo, di luogo e ambiente in cui si svolgono e per le loro obbiettive caratteristiche, siano comunque idonee a far sorgere la situazione di pericolo di ricostituzione del partito [fascista]».

21 G. Sacerdoti, *Intervento*, in *sidiblog.org,* 15 gennaio 2014, pur dichiarandosi favorevole alla detta aggravante ha osservato come nella fretta suscitata dall'emozione per le reazioni nostalgiche seguite alla morte di Priebke il testo trascuri di menzionare il requisito secondo il quale le manifestazioni di negazionismo sono perseguibili in quanto atte ad incitare alla violenza o all'odio, o a turbare l'ordine pubblico (tale requisito è d'altronde menzionato nella decisione quadro 2008/913/GAI, cui la legge

si è tentato di fare con la punizione di manifestazioni fasciste già incriminate[22], mosse entrambe dall'emozione legata a fatti di cronaca.
Il consenso intorno ai valori costituzionali fondanti non può – purtroppo – essere dato per scontato, né essere imposto a norma di legge, specialmente nei confronti delle nuove generazioni, ma richiede l'attivazione di strategie svolte su diversi registri nei diversi ambiti sociali[23]. E questo oggi comporta non solo l'adozione di leggi della memoria, ma di misure capaci di affrontare la "grande regressione", economica, sociale e morale, che ha investito le nostre democrazie[24].

3. (*segue*): le politiche di odio e di disinformazione in Rete

Se gli ordinamenti di democrazia costituzionale appaiono accomunati dall'altalenante apertura e chiusura verso il pensiero ostile, i temi sensibili non sono tuttavia gli stessi sulle due sponde dell'Atlantico : in particolare, il divieto di incitamento all'odio razziale, che esprime una scelta di civiltà comune a tutti i Paesi europei (e al Canada), non ha mai superato lo "scrutinio stretto" di compatibilità con il I emendamento, se non quando sia stato accompagnato dal pericolo imminente di violenza e/o dalla intenzione di diffondere una autentica minaccia[25].
La *viewpoint neutrality* che lo Stato deve osservare, secondo l'ormai consolidata giurisprudenza della Corte Suprema, farebbe invero divieto di favorire le idee e i discorsi ispirati all'eguaglianza tra tutti gli esseri umani rispetto a quelli basati sulla superiorità di una razza o di una religione (così come farebbe divieto di promuovere l'idea della parità tra i sessi a scapito dell'idea che la donna sia inferiore all'uomo)[26].
Il rifiuto del paternalismo statale si spinge in quest'ambito a livelli intollerabili per la sensibilità europea. Eppure una forma analoga, se non più efficiente, di censura viene praticata e accettata sotto la veste della *political correctness*, che è oggetto di una convenzione condivisa tra tutti i media tradizionali.
Certo i moduli del politicamente corretto possono risultare stucchevoli; ma non si può dimenticare come essi contrastino il c.d. effetto di silenziamento che il discorso pubblico produce nei confronti dei soggetti più deboli. Almeno in una, memorabile, circo-

italiana ha dato attuazione).

[22] Sul carattere esclusivamente simbolico della proposta di legge avanzata nella scorsa legislatura v. M. Manetti, *Lacune vere e presunte nella repressione della propaganda nazifascista. A proposito del d.d.l. Fiano*, in *Quaderni Costituzionali*, 4, 2017, 883 ss.

[23] V. in tal senso, con dovizia di svolgimenti, G.E. Vigevani, *Origine e attualità del dibattito sulla XII Disposizione finale della Costituzione: i limiti della tutela della democrazia*, in *questa Rivista*, 1, 2019, 25 ss.

[24] V. al riguardo la panoramica offerta da H. Geiselberger (a cura di), *The Great Regression,* Berlino, 2017. Sull'affossamento degli ideali di solidarietà, sostituiti dal precetto della *Selst-Optimizierung* v. O. Nachtwey, *Die Abstiegsgesellschaft,* Frankfurt a. M., 2016.

[25] V. rispettivamente le sentenze *Brandenburg v. Ohio*, cit., e *Virginia v. Black*, 538 U.S. 343 (2003), sulle quali riflette da ultimo I. Spigno, *Discorsi d'odio. Modelli costituzionali a confronto,* Milano, 2018, 74 ss.

[26] Torna da ultimo a criticare questo indirizzo della Corte Suprema C. A. Mac Kinnon, *The First Amendment. An Equality Reading*, in L.C. Bollinger-G. R. Stone (a cura di), *The Free Speech Century*, cit., 140 ss.

stanza essi hanno inoltre contribuito a proteggere la sensibilità di un gruppo etnico/religioso ben più efficacemente delle multiformi discipline vigenti nei Paesi europei.
In occasione della pubblicazione delle vignette su Maometto da parte del *Jilland's Post*, tutti i giornali statunitensi furono d'accordo nel ritenere che esse potevano bensì essere descritte a parole, ma non riprodotte, dal momento che per i musulmani è sacrilegio rappresentare il Profeta, prima ancora che farne oggetto di satira. Nei Paesi europei dove le vignette furono contestate in giudizio nessuna tutela fu riconosciuta ai dogmi religiosi, appuntando invece l'attenzione sulla configurabilità dell'incitamento all'odio verso la minoranza musulmana (che fu peraltro unanimemente esclusa).
Anche questo episodio rivela la sensibilità molto diversa che alberga sulle due sponde dell'Atlantico[27]. Ma dal punto di vista giuridico le esperienze dei diversi ordinamenti tornano ad avvicinarsi, grazie alla coincidenza almeno parziale tra il ruolo svolto in Europa dal codice penale e negli Stati Uniti dalle regole deontologiche del giornalismo professionale.
Il quadro appena tracciato appare peraltro idilliaco rispetto all'attuale prassi della Rete, dove l'intermediazione offerta dai professionisti dell'informazione, per quanto criticabile, è stata accantonata in favore della comunicazione di stati d'animo e di emozioni, più che di pensieri intesi al dibattito pubblico[28]. L'anonimato, che sarebbe dovuto servire a valorizzare l'opinione espressa indipendentemente da chi ne fosse l'autore, è diventato un accorgimento propizio non solo al linguaggio scurrile ma anche al pettegolezzo malevolo e alle dottrine scientifiche inventate di sana pianta[29].
L'uso dei social media ha poi incentivato non solo la propensione dell'essere umano ad accodarsi, espressa dai *follower*, ma anche l'opposta tendenza a disprezzare e perseguitare, espressa dagli *hater,* dai *cyberbully* e dai *troll*[30]. E come la Rete ha reso possibili i movimenti politici che si proponevano di sconfiggere regimi dittatoriali, così è servita a propalare messaggi razzisti e negazionisti.
Prima di recriminare sul risveglio dell'irrazionalità che il nuovo ordine ideale instaurato dopo la Seconda Guerra mondiale mirava ad impedire, bisognerebbe considerare il quadro normativo all'interno del quale tale tendenza ha potuto proliferare indisturbata. La scelta iniziale e determinante è stata quella di negare ai poteri pubblici – pur responsabili della predisposizione delle infrastrutture (le c.d. autostrade dell'informazione) – qualsiasi ruolo nella gestione della Rete, consegnata per così dire "chiavi in mano" ai privati. Per fomentare lo sviluppo delle loro attività economiche questi sono stati altresì dotati di una speciale immunità, grazie alla quale non rispondono dei

[27] Lo dimostra la posizione di R. Post, *Religion and Freedom of Speech: Portraits of Muhammad*, in *Constellations*, 1, 2007, 72 ss., che pur essendo in linea di principio contrario alla protezione dei sentimenti altrui (persino di quelli radicati nelle *civility rules*, ovvero nelle più elementari regole della convivenza sociale) si mostra dubbioso sulla opportunità di pubblicare le vignette in esame.

[28] Sull'attuale prevalere della chiave sentimentale ed emotiva nella lettura della libertà individuale, che era invece dominata in precedenza dalla razionalità, v. H. Biung-Chul, *Psicopolitica*, Milano, 2016, 51 ss.

[29] Sulla necessità di mantenere nondimeno la liceità dell'anonimato, imponendo peraltro agli operatori della Rete il rispetto di regole che rendano possibile l'identificazione degli autori delle comunicazioni illecite anche quando essi ricorrano ad apposite tecniche di mascheramento v. E. Barendt, *Anonymous speech. Literature, Law and Politics*, Oxford, 2016, 125 ss.

[30] V. in generale S. Levimore-M.C. Nussbaum, *The Offensive Internet. Speech, Privacy, and Reputation,* Cambridge, 2012.

contenuti immessi dagli utenti. Come è noto, grazie alla *Good Samaritan clause*[31], sostanzialmente riprodotta negli artt. 12-15 della direttiva 2000/31/CE sul commercio elettronico, la sorveglianza sui messaggi contrari alle norme penali o civili è stata in via di principio rimessa alla platea degli utenti, alle segnalazioni dei quali la piattaforma fa seguire (se lo ritiene) il blocco del messaggio.

In tal modo il divieto del *prior restraint* è stato sostanzialmente esteso dalla stampa alla Rete: qui lo Stato ha rinunciato a svolgere persino il proverbiale ruolo di guardiano notturno, che nessun fautore delle libertà individuali ha mai pensato di contestare. Oggi sembra quasi impossibile che nessuno abbia previsto o immaginato gli eccessi e gli abusi cui questa assenza avrebbe condotto, e che anzi la stessa Corte Suprema nella sua prima pronuncia in materia abbia difeso la libertà di usare un linguaggio indecente, considerandola un'estrinsecazione della libertà di partecipare al dibattito pubblico che la Rete per la prima volta offre senza speciali costi o difficoltà[32]. L'argomento di natura giuridico-costituzionale è stato del resto affiancato all'altro, di natura tecnica, secondo il quale il controllo o filtraggio dei messaggi da parte delle piattaforme sarebbe stato materialmente impossibile.

Se dunque la democrazia ha tutto il diritto di difendersi dai propri nemici, si può ben dire che la difesa avrebbe dovuto essere esercitata alla fonte, anziché rivolgersi, in modo tardivo e inefficace, contro i singoli e i gruppi che approfittano della sconfinata libertà della Rete. In altre parole, anziché indurire o estendere i reati di opinione, si sarebbe trattato di prevedere una qualche forma di responsabilità *ex ante* a carico dei titolari delle piattaforme (come quelle recentemente introdotte tanto in Europa che negli Stati Uniti[33]).

Sono state invece necessarie molte battaglie giudiziarie per superare, tra ardue difficoltà giuridiche e tecniche (delle quali rimangono emblematiche *Yahoo! c. France*, in ordine alla vendita online di cimeli nazisti, e *Google c. Vividown*, sulla tardiva cancellazione di un video che riprendeva l'aggressione fisica e verbale condotta ai danni di un disabile da parte di alcuni compagni di scuola), la iniziale allegazione di totale neutralità e irresponsabilità delle piattaforme rispetto ai contenuti immessi[34].

L'ultima novità è rappresentata in Europa (sulle orme di un precedente canadese[35]) dalla sentenza della Corte di giustizia secondo la quale la citata direttiva 2000/31/CE sul commercio elettronico "non osta" a che un giudice di uno Stato membro possa or-

[31] Art. 230 del Communications Decency Act. Il nomignolo nasce in realtà dall'obbiettivo iniziale del legislatore, che era quello di permettere la censura dei provider nei confronti di materiale sessualmente esplicito. Sulla necessità di modificare tale previsione, che ha invece garantito l'immunità alle piattaforme che si dedicano ad attività illecite o che le tollerano deliberatamente v. D. Keats Citron-B. Wittes, *The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity*, University of Maryland Legal Studies Research Paper No. 2017-22, in *ssrn.com.*

[32] *Reno v. ACLU*, 521 U.S. 844 (1997). Sull'esercizio delle libertà in Rete v. almeno T.E. Frosini, *Liberté, egalité, Internet,* Napoli, 2015; M. Cuniberti, *Potere e libertà nella rete*, in M. Manetti-R. Borrello (a cura di), *Libertà di informazione. Temi e problemi*, Modena, 2019, 21 ss.

[33] V. *infra* il par. 5.

[34] V. M.R. Allegri, *Ubi social. Fondamenti costituzionali dei social media e profili giuridici della responsabilità dei provider,* Milano, 2018.

[35] Corte Suprema del Canada, *Google Inc. v. Equustech Solutions,* sentenza del 28 giugno 2017, che ha ordinato di rimuovere globalmente i contenuti ritenuti illegali dalla Corte della Colombia britannica.

dinare a una piattaforma di rimuovere messaggi di contenuto sostanzialmente identico a quello già dichiarato illecito, e di bloccarne l'accesso, «a livello mondiale»[36].
Più oscillante è − come al solito − la ormai copiosa giurisprudenza della Corte EDU, che ritiene rilevante sia la natura del sito (proteggendo i piccoli siti non profit), sia la gravità del messaggio lesivo (secondo che attinga il livello di *hate speech*), sia infine la prontezza con la quale il messaggio è stato rimosso[37].

4. Potere economico e libertà di pensiero

L'esperienza di Internet ripresenta sotto altre spoglie il fenomeno già denunziato con riguardo ai mass media tradizionali: la mutazione del potere economico (e tecnologico) in libertà civile[38].
Quando le piattaforme non hanno più potuto negare di svolgere nel proprio interesse una qualche forma di selezione o filtraggio dei messaggi, hanno sostenuto che si trattava di attività totalmente neutrali, in quanto guidate da algoritmi. E quando si è opposto che gli algoritmi sono pur sempre frutto di scelte *lato sensu* politiche effettuate a monte, le piattaforme hanno richiesto che essi vengano equiparati alle attività editoriali svolte dai comuni mass media.
Risale alla fine del 2016 la dichiarazione con la quale, dopo anni di strenua resistenza, il più importante *social medium* ha accettato di paragonarsi ai tradizionali mezzi di comunicazione di massa, precisando peraltro che le scelte editoriali sono svolte al suo interno da avvocati e da esperti di diritto[39]. Si è ribadita così la pretesa della piattaforma di essere e di mantenersi neutrale (in quanto orienterebbe la propria sorveglianza unicamente dal fine di rispettare le leggi in vigore), pur aspirando ad ottenere la massima protezione garantita dalle democrazie costituzionali.
Le attività di indicizzazione e/o segnalazione di determinati messaggi che le piattaforme normalmente svolgono sono invero apparse paragonabili alle attività editoriali svolte dai comuni mass media, tanto più che anch'esse sono guidate dallo scopo di profitto[40]. È così che i risultati dei motori di ricerca o la lista delle notizie che viene quotidianamente presentata all'utente hanno potuto godere della più ampia tutela accordata alla manifestazione del pensiero rispetto alla libertà di iniziativa economica, in analogia con le attività editoriali tradizionali. All'algoritmo usato da un motore di

[36] CGUE, C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Ltd.* (2019). Si trattava di messaggi lesivi dell'onore di una parlamentare austriaca, inizialmente pubblicati su Facebook e poi "rimbalzati" in altri siti.

[37] V. al riguardo la disamina di A. Koltaj, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere.,* cit., 216 ss.

[38] Cfr. A. Di Giovine*, Libertà di informazione. O potere*?, in M. Bovero (a cura di), *Quale libertà*, Roma-Bari, 2004, 134.

[39] V. la dichiarazione di M. Zuckerberg riportata da *repubblica.it* il 22 dicembre 2016. Gli sviluppi successivi dimostrano che la nuova identità di *media company* corrisponde a una svolta nella politica aziendale, nella quale il social medium, ormai diffuso a livello mondiale, serve da volano per altre e più redditizie attività.

[40] V. al riguardo V. Zeno Zencovich, *Cosa intendiamo, oggi, per* media*?,* in M. Manetti-R. Borrello (a cura di), *Libertà di informazione. Temi e problemi*, cit., 11 ss.

ricerca un tribunale ha invero ritenuto di applicare «la fondamentale protezione del I emendamento, secondo il quale chi parla ha il diritto di scegliere in piena autonomia il contenuto del suo messaggio» [41].

A prima vista questo paradigma appare contestabile: come è possibile paragonare le decisioni compiute giorno per giorno dal direttore di un giornale alle priorità accordate semplicemente sulla base delle entrate pubblicitarie e/o sulla base delle preferenze espresse in passato dall'utente? La finalità di profitto sembra senz'altro assorbente.

Chi conosce la giurisprudenza statunitense degli ultimi vent'anni non può tuttavia ignorare come l'espansione riconosciuta in passato alla libertà di pensiero sia stata trasformata dalla Corte Suprema nel più efficace strumento di protezione degli interessi economici e commerciali. Così almeno ritiene molta dottrina statunitense, denunziando la "lochnerizzazione" del I emendamento[42].

Il problema è che sulle piattaforme domina la scelta di applicare all'informazione la stessa segmentazione e personalizzazione che vale per la vendita dei prodotti, confezionando quello che Cass Sunstein ha efficacemente battezzato il "*daily me*", ossia una lista di notizie appositamente creata per ciascun utente a partire da quelle fonti o opinioni che ha già mostrato di gradire, con l'effetto di frantumare in milioni di pezzi autoreferenziali il dibattito pubblico[43].

Molta dottrina sembra disposta ad accettare queste scelte come se fossero indiscutibili, anche quando ne denunzia l'effetto distorsivo sui funzionamenti della nostra democrazia[44]. Ma chi ritiene che in virtù delle *filter bubble* il nostro regime politico – già mutatosi nella declinante democrazia c.d. del pubblico – abbia subito l'ulteriore negativa trasformazione in *bubble democracy* non può non interrogarsi sulla necessità di limitare o regolare l'uso di questa pratica[45].

---

[41] Cfr. United States District Court, New York, 28 marzo 2014 (10 F. Supp. 3d 433), *J. Zhang v. Baidu, Inc.*, che ha rigettato il ricorso diretto contro la piattaforma cinese Baidu a causa del blocco praticato dal suo motore di ricerca nei confronti di articoli e informazioni riguardanti i movimenti democratici cinesi. Secondo i ricorrenti, che avevano pubblicato articoli di questo tipo, Baidu ne avrebbe bloccato la visibilità negli Stati Uniti a richiesta della Repubblica popolare cinese (non comparsa in giudizio). La Corte ritenne che l'algoritmo con il quale vengono orientati i risultati delle ricerche per motivi politici sia in sostanza un giudizio editoriale, espressione di *core political speech* protetto dal I emendamento. Per l'approfondita discussione dei problemi riguardanti i motori di ricerca v. A. Koltaj, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere,* cit., 115 ss.

[42] Il riferimento è alla sentenza *Lochner v. New York*, 198 U.S. 45 (1905), che simboleggia il periodo nel quale la Corte Suprema difendeva la libertà contrattuale degli imprenditori dalla legislazione di tutela del lavoro. V. ancora F. Schauer, *Every Possible Use of Language?,* cit. Per un'esauriente discussione della dottrina e della giurisprudenza relative v. A. Shanon, *The New Lochner*, in *Wisconsin L. Rev.,* 2016, 133 ss.

[43] C. R. Sunstein, *Republic.com. Cittadini informati o consumatori di informazioni*? trad. it., Bologna, 2003. L'A. ha sviluppato il tema delle "cascate informative" in Id., *On Rumors. How Falsehood Spread, Why We believe Them, and What Can Be Done,* Princeton, 2014.

[44] Per non parlare degli effetti sul funzionamento del nostro cervello, che sono dimostrati, anche se la valutazione ne è ancora discussa.

[45] V. invece, per tutti, G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *questa Rivista,* 1, 2018, 32 ss., spec. 36. Si può del resto registrare una diffusa atmosfera di resa alla decadenza della democrazia, tanto in chi la imputa alle aspirazioni di cambiamento sociale accolte dai regimi democratici nel Dopoguerra (v. da punti di vista diversi M. Tushnet, *Comparing Right-Wing and Left-Wing Populism e* M.A. Graber, *What's in Crisis ? The Postwar Constitutional Paradigm, Transformative Constitutionalism, and the Fate of Constitutional Democracy,* in M.A. Graber-S. Levinson-M. Tushnet (a cura di), *Constitutional Democracy in Crisis?* New York, 2018, rispettivamente 639 ss., 665 ss.), quanto in chi (rispolverando invero argomenti

Altrettanto scottante è la questione della neutralità della Rete, intesa come l'eguale diritto di tutti gli utenti a connettersi ai siti che preferiscono, senza subire rallentamenti o blocchi imposti dalle piattaforme per motivi di profitto. Queste ultime vorrebbero invece poter escludere o scoraggiare la connessione ai siti che non sono in grado di pagare corrispettivi più elevati (o magari ai siti che diffondono critiche alle piattaforme stesse), oltre che differenziare il trattamento riservato ai diversi tipi di dati (per esempio ai dati video rispetto ai dati voce), sempre per motivi commerciali.
Notoriamente il principio di neutralità della Rete è stato affermato dalla *Federal Communications Commission* sotto la presidenza Obama, per essere nello stesso anno recepito, con notevole ampiezza di svolgimenti, dal regolamento (UE) 2120/2015 dell'Unione europea[46]. La nuova FCC nominata sotto la presidenza Trump ha revocato la propria decisione alla fine del 2017[47].
In definitiva, le piattaforme hanno il potere di condizionare in mille modi diversi l'andamento del dibattito pubblico: non solo in nome del profitto, ma anche delle proprie malcelate preferenze politiche e ideologiche. E la progressiva riduzione del numero di tali piattaforme, intervenuta a seguito di ripetute operazioni di concentrazione, rende ancora più temibile l'ipoteca che esse hanno acceso sul funzionamento della democrazia.
Un significativo cambio di passo, e sia pure limitato, si è avuto, grazie alla direttiva (UE) 1808/2018, in relazione ai (soli) servizi di *video-sharing*, ovvero ai «servizi di piattaforma per la condivisione di video generati dagli utenti», quando la loro organizzazione sia frutto delle scelte editoriali operate dalle piattaforme «con mezzi automatici o algoritmi, in particolare mediante visualizzazione, attribuzione di *tag* e sequenziamento»[48].
Tali servizi sono stati equiparati ai servizi di media audiovisivi, in considerazione del fatto che anch'essi, da un lato, hanno il fine di informare, istruire e intrattenere, mentre dall'altro hanno un "impatto significativo" sul pubblico, in quanto possono modellare o influenzare i pareri degli utenti, e soprattutto dei giovani
Su questa base è stato imposto ai titolari delle piattaforme l'obbligo di assicurare con misure adeguate tanto la protezione dei minori da messaggi che possano nuocere al

d'altri tempi) mette sotto accusa la "iperdemocrazia" che discenderebbe dalla promessa di sconfinata auto-determinazione individuale: così G. Orsina*, La democrazia del narcisismo. Breve storia dell'antipolitica*, Venezia, 2018.

[46] Il regolamento (UE) 2015/2120 del 25 novembre 2015, che stabilisce misure riguardanti l'accesso a un'Internet aperta, all'art. 3, par. 3, impone ai fornitori di servizi di accesso a Internet di trattare tutto il traffico allo stesso modo, precisando che questi «in particolare, non bloccano, rallentano, alterano, limitano, interferiscono con, degradano o discriminano tra specifici contenuti, applicazioni o servizi, o loro specifiche categorie, salvo ove necessario e solo per il tempo necessario» ai fini indicati dal medesimo comma. Il par. 4 prevede inoltre che se i fornitori medesimi vogliono «fornire servizi di comunicazione elettronica diversi da quelli di accesso a Internet, per cui sono necessari livelli specifici di qualità del servizio o di ottimizzazione, possono farlo soltanto se la capacità della rete è sufficiente a fornirli in aggiunta a tutti i servizi di accesso a Internet prestati, e senza andare a discapito della disponibilità o della qualità generale dei servizi di accesso a Internet per gli utenti finali».

[47] Il 7 ottobre 2019 la *D.C. Circuit Court of Appeals* ha ritenuto valida la decisione della FCC. Una legge che mira a ripristinare la neutralità della Rete *(Save the Internet Act)* è stata approvata dal Congresso lo scorso aprile, ma non ha molte speranze di passare al Senato.

[48] Art. 1 della direttiva (UE) 2018/1808 del 14 novembre 2018 recante modifica della direttiva 2010/13/UE (direttiva sui servizi di media audiovisivi, o Direttiva SMAV).

loro sviluppo fisico o mentale, quanto il "grande pubblico" da messaggi che istighino alla violenza o all'odio, o che integrino i reati di pubblica provocazione a commettere reati di terrorismo ai sensi dell'articolo 5 della direttiva (UE) 2017/541, o reati di pedo-pornografia ai sensi dell'art. 5, par. 4, della direttiva 2011/93/UE o infine reati di stampo razzista o xenofobo ai sensi dell'art. 1 della decisione quadro 2008/913/GAI[49].
Fintanto che non si affermi la piena equiparazione con i mass media, non sarà tuttavia applicabile all'intera attività dei giganti della Rete né questa disciplina, né la timida novità contenuta nella stessa direttiva, che finalmente riconosce la connessione tra la trasparenza della proprietà dei media e la libertà di espressione, "fondamento dei sistemi democratici". Assumendo esattamente che fornire informazioni in merito all'assetto proprietario dei fornitori di servizi di media consenta agli utenti di elaborare un giudizio informato circa il contenuto dei messaggi trasmessi sotto l'influenza o il controllo di questi[50].
Si tratta a ben vedere di un tardivo omaggio all'art. 21, c. 5 della Costituzione italiana, che si rivela sul punto niente affatto obsoleta[51]. Le cautele mostrate sessant'anni fa dalla nostra Carta vengono peraltro ulteriormente rafforzate, come se l'esperienza non avesse dimostrato quanto sia pregiudizievole la concentrazione in poche mani dei mezzi di comunicazione di massa. La Direttiva prevede invero che gli Stati possano adottare misure legislative in cui si prevede che i fornitori di servizi di media rendano accessibili informazioni sul loro assetto proprietario, purché tali misure siano necessarie, proporzionate, finalizzate al perseguimento di un obiettivo di interesse generale (il che sembrava implicito nella premessa) e purché rispettino i diritti fondamentali relativi alla vita privata e alla vita familiare dei proprietari effettivi[52].

5. L'imposizione di obblighi di sorveglianza e i rischi della censura privata

Per timore di essere accomunate ai regimi autoritari che disinvoltamente censurano la Rete, le democrazie occidentali sembrano dunque disposte a gettare al vento le proprie fonti di legittimazione, che risiedono nel dibattito pubblico. Al di là delle sanzioni che possono irrogare e irrogano alle piattaforme per violazione delle regole concorrenziali (veicolate dall'indiscussa preminenza dello *ius mercatorum*), esse appaiono ancora ipnotizzate dal mito positivo della tecnologia[53].
In sintonia con la ricordata espansione delle responsabilità dei provider, si sta affermando peraltro la tendenza a superare l'esenzione delle piattaforme da qualsiasi obbligo di sorveglianza sui contenuti generati dagli utenti. Anche se il dovere del fornitore

[49] Art. 28-*ter* della direttiva (UE) 2018/1808, cit.

[50] V. il considerando 15 della direttiva (UE) 2018/1808, cit.

[51] Sulla vitalità dell'art. 21 Cost. v. da ultimo M. Betzu, *Libertà di espressione e poteri privati nel cyberspazio*, in *Diritto costituzionale,* 1, 2020, 117 ss.

[52] Art. 5, par. 2, della Direttiva SMAV, come modificato dalla citata direttiva (UE) 2018/1808.

[53] Sulla vocazione autoritaria della tecnologia della rete v. ora M. Ainis, *Il regno dell'uroboro*, Milano, 2018, 71 ss.

dei servizi di filtrare i messaggi onde impedirne la diffusione in caso di illiceità è tuttora considerato un'eccezione alla regola, e tale rimane non solo nella legislazione degli Stati Uniti[54], ma anche dell'Unione europea.

I singoli Stati hanno invero previsto obblighi del genere per varie finalità, tra le quali primeggiano la lotta alla pedo-pornografia, alle scommesse illegali, al terrorismo, per un verso; la protezione della proprietà intellettuale, dell'onore e dei dati personali, dall'altro. Fatti salvi tali obblighi, l'Unione europea si affida dichiaratamente alla volontà di auto-regolamentazione delle stesse piattaforme, ovvero a forme di co-regolamentazione che ricalcano quelle in uso tra Stati sovrani[55].

In Germania è stata peraltro approvata la *Netzwerkdurchsetzungsgesetz*, che dal 1° ottobre 2017 si applica ai social media cui siano registrati almeno due milioni di utenti tedeschi. Pur rispettando le limitazioni di responsabilità previste dalla normativa eurounitaria, tale legge ha previsto l'obbligo dei social media di nominare un soggetto incaricato di ricevere le segnalazioni relative a messaggi (ritenuti) illeciti, e ha previsto sanzioni nel caso in cui la piattaforma non dia adeguato e sollecito séguito alle segnalazioni medesime[56].

La regola rimane quella che accolla agli utenti la responsabilità di segnalare gli illeciti, chiedendo alla piattaforma di rimuoverli: ma spetta a quest'ultima decidere discrezionalmente sulla rimozione, così come le spetta – da sempre – il potere di censurare alla fonte i messaggi che ritiene illeciti[57]. È fatto salvo, in entrambi i casi, il ricorso dell'interessato ad autorità indipendenti o ai tribunali: ma è evidente come questo controllo, rimesso *ex post* all'iniziativa dei privati, non sia sufficiente ad assicurare che le piattaforme agiscano nel rispetto dei diritti degli utenti, che siano autori o destinatari dei messaggi in discussione.

Di fatto gli Stati che inizialmente hanno rinunziato - in nome della libertà della Rete - a regolarla e a controllarla, hanno in seguito delegato tale compito alle piattaforme, col rischio che queste ultime sottopongano a censura anche contenuti protetti dalla libertà

[54] Negli USA l'obbligo di filtraggio è imposto con riguardo ai messaggi che promuovano il traffico di esseri umani a scopo di sfruttamento sessuale (*Fight Online Sex Trafficking Act* del 2017). Su altri casi nei quali alle piattaforme non è assicurata l'immunità v. la lett. e) della *Good Samaritan Clause*, sottoposta peraltro ad una interpretazione molto restrittiva da parte dei tribunali.

[55] Ad es. l'Unione europea nel 2016 ha chiesto a Facebook, Microsoft, Twitter e Youtube di sottoscrivere un "Codice di condotta per lottare contro le forme illegali di incitamento all'odio online".

[56] Ai sensi dell'art. 3 della legge in esame la piattaforma deve rimuovere o bloccare l'accesso a un contenuto "manifestamente illecito" entro 24 ore dalla ricezione della segnalazione, salvo che abbia concordato con l'autorità giudiziaria competente un periodo più lungo. Inoltre deve rimuovere o bloccare i messaggi (semplicemente) "illeciti" entro sette giorni dalla ricezione della segnalazione. Tale termine può essere superato in due casi: se la decisione sull'illiceità del contenuto dipende dalla falsità di una dichiarazione o "dipende chiaramente dalle circostanze di fatto" (in tali casi, il gestore del social network può dare all'utente l'opportunità di replicare alla segnalazione prima che venga adottata una decisione); se il social network entro sette giorni dalla ricezione della segnalazione rimette la decisione sull'illiceità a un organo di autoregolamentazione riconosciuto ai termini di legge, accettando di conformarsi alla decisione di tale organo (traduzione a cura di G. Giannone Codiglione, in *questa Rivista*, 2017, 185 ss.).

[57] Tra le tante v. la disavventura del settimanale satirico Titanic, che nel gennaio 2018 si è visto sospendere il proprio account Twitter per un messaggio nel quale parodiava un discorso di odio diffuso dalla estrema destra tedesca.

di pensiero e di informazione[58]. Quanto alla necessità di controllare lo svolgimento di ciò che è da ritenere un vero e proprio esercizio di pubbliche funzioni, è prevalsa l'obiezione, che riecheggia quella usata all'inizio della storia di Internet, secondo la quale non sarebbe "materialmente possibile" per i poteri pubblici verificare quali sono le regole effettivamente applicate dalle piattaforme ai messaggi che diffondono[59].
In effetti uno Stato che aspira a essere minimo, e ha perciò appaltato ai privati molte delle sue funzioni caratterizzanti, non può non trovarsi in difficoltà di fronte a un compito del genere. Ma esso appare nondimeno irrinunziabile di fronte ai "crimini informativi" che la Rete, novello vaso di Pandora, continua a sfornare.

6. La manipolazione degli utenti

Veniamo infine agli sviluppi che, a differenza di quelli precedentemente ricordati, erano più difficili da immaginare. In particolare, due episodi (tra mille altri che forse non conosciamo[60]) sono ormai assurti a simbolo della manipolazione cui gli utenti sono esposti attraverso le piattaforme[61].
Quando Facebook, da un lato, e Google, dall'altro, hanno deciso di postergare le notizie di attualità ad altri tipi di messaggi, molti movimenti che, agendo sotto regimi autoritari, facevano prevalente affidamento sulle piattaforme per diffondere la propria contro-informazione hanno perso gran parte della propria visibilità; così come molti siti di giornalismo che lavoravano principalmente per la pubblicazione via Internet[62].
Per converso, le stesse piattaforme non hanno potuto o voluto impedire la diffusione di migliaia di messaggi falsi, generati automaticamente, che hanno inondato il sito della FCC in occasione della consultazione da essa indetta, secondo la legge, prima di varare il già citato provvedimento di revoca della *Net Neutrality*. Si trattava di messaggi favorevoli alla revoca prodotti in modo automatico, alcuni dei quali a quanto pare provenivano a loro insaputa dall'*account* di persone che erano state in precedenza derubate dei propri dati[63].

[58] Sia il Consiglio d'Europa che la Commissione europea hanno da ultimo sottolineato la necessità che le piattaforme rispettino nella loro opera le libertà di pensiero e di informazione, come riporta A. Koltaj, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere,* cit., 98, 104.

[59] Questa è la tesi ribadita da M. Bickert (Head of Policy Management di Facebook), *Defining the Boundaries of Free Speech on Social Media,* in L.C. Bollinger-G.R. Stone (a cura di), *The Free Speech Century,* cit., 254 ss., che sostiene altresì la perfetta coincidenza tra l'interesse degli utenti a veder applicare corretti criteri di selezione dei contenuti e quello delle piattaforme a fare buoni affari. Ma v. infra il *par.* successivo.

[60] Secondo A. Koltay, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere.,* cit., 23, Facebook avrebbe condotto anche un "infame esperimento" basato sulla manipolazione delle notizie messe a disposizione degli utenti, verificando come riusciva ad influenzarne l'umore attraverso la scelta del tipo di notizie destinate a ciascuno di essi.

[61] Sul tema v. in generale G. Pitruzzella-O. Pollicino-S. Quintarelli, *Parole e potere. Libertà d'espressione*, hate speech *e* fake news, Milano, 2017.

[62] Cfr. E. Bell, *The Unintentional Press,* in L.C. Bollinger-G.R. Stone (a cura di), *The Free Speech Century*, cit., 235 ss.

[63] Secondo *Buzzfeednews.com*, il Procuratore generale di New York avrebbe ritenuto presumibilmente

Di fronte a queste e altre forme di manipolazione della democrazia si deve riflettere amaramente sulle sorti del contrappeso che avrebbe dovuto contrastare il potere di chi diffonde le notizie : il principio del pluralismo informativo, ovvero il "diritto ad essere informati".

Per un breve tratto è sembrato che questo fosse automaticamente garantito dall'accesso ad Internet, grazie alla virtuosa sinergia tra i cittadini-giornalisti che a migliaia diffondono in Rete le notizie raccolte di prima mano, da un lato, e i cittadini-utenti che possono accedervi a costo zero, dall'altro[64]. L'unico tassello ancora mancante per rendere effettivo il diritto in esame sarebbe stato il riconoscimento del diritto (sociale) di accesso alla Rete (cui la disciplina eurounitaria ha porto omaggio, sia pure in termini limitati)[65].

Il trionfo del pluralismo esterno, inteso come disponibilità delle fonti informative più varie e diverse, avrebbe spazzato via le fastidiose questioni giuridiche che il diritto all'informazione pone, in termini di vincolo alla libertà di chi sceglie e presenta le notizie. Tale vincolo, se inteso – come dev'essere – in senso propriamente giuridico e perciò giudiziariamente azionabile, appare invero incompatibile con quella libertà[66].

L'idea della Rete come spontaneo luogo di pluralismo ha subito tuttavia due successive contestazioni: la più antica, fondata sulla creazione delle c.d. cascate informative o *echo chambers*, nelle quali l'utente è esposto soltanto a un certo tipo di messaggi[67], è stata di recente rivista e corretta. Si è constatato che oggi non vi è più scarsità, ma semmai eccesso di informazioni, anche a causa della pratica definita *reverse censorship*, che consiste nell'"affogare" i messaggi sgraditi in un mare di altre informazioni più o meno autentiche (o semplicemente in un profluvio di pettegolezzi)[68]. Il fenomeno è disastrosamente aggravato dalla tecnica consistente nel diffondere messaggi che non provengono da autentici esseri umani ma da robot, onde creare una fittizia popolarità a favore di determinate opinioni (come sembra essere successo nella già citata vicenda della consultazione svolta in rete dalla FCC, all'esito della quale la maggioranza dei messaggi risultava favorevole alla revoca, mentre secondo i sondaggi i cittadini statunitensi erano quasi totalmente contrari).

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[69]. Su tali basi si è argomentata la necessità

falsi circa 9,6 milioni dei commenti in esame.

64 V. al riguardo le ottimistiche prospettive di E. Volokh, *Cheap Speech And What It Will Do*, in *Yale L. J.,* 1995, 1805 ss., e la risposta (a vent'anni di distanza) di R.L. Hasen, *Cheap Speech And What It Has Done (To American Democracy),* in *First Amend. L. Rev.*, 16, 2017-18, 200 ss.

65 V. le critiche svolte al riguardo da G. De Minico, *Internet. Regola e anarchia*, Napoli, 2012, 154 ss.

66 Lo ribadisce da ultimo A. Pace, *Libertà di informazione e Costituzione*, in S. Merlini (a cura di), *L'informazione. Il percorso di una libertà*, Firenze, 2011, 49 ss. Ma v. Anche A. Di Giovine, *Libertà di informazione,* cit., 127.

67 V. le opere di C. R. Sunstein cit. *supra* alla nt. 43.

68 Così T. Wu, *Is the First Amendment Obsolete?*, in L.C. Bollinger-G.R. Stone (a cura di), *The Free Speech Century*, cit. 272 ss., che sottolinea come il *free speech* sia diventato paradossalmente strumento di censura.

69 Si tratta di una constatazione ampiamente diffusa: v. ad es. G. Pitruzzella, *La libertà di informazione*

di restaurare nei confronti dei social media una "*fairness doctrine*" quale era inizialmente applicata dalla FCC ai canali televisivi, e quale la Corte Suprema aveva validato nella storica sentenza *Red Lion*[70].

La posizione ora descritta è molto lontana da quella dominante oggi negli Stati Uniti, secondo la quale nessuno può imporre a chi detiene il mezzo (foss'anche la busta che contiene la bolletta del gas[71]) l'obbligo di esporre una opinione che non condivide o che non ha scelto di diffondere. Persino il diritto di rettifica che il nostro ordinamento prevede a tutela del singolo sarebbe da ritenere un'inammissibile violazione della libertà spettante a chi dispone del mezzo[72].

Va detto che la situazione non è molto più rosea nei Paesi europei e in particolare in Italia, dove l'esposizione del cittadino ad una vera pluralità di opinioni è garantita soltanto in televisione, e soltanto nella materia politico-parlamentare (non certo in quella religiosa[73]).

Fino a qualche tempo fa, ciò poteva essere considerato comunque un bel vantaggio rispetto al *money is speech* imperante negli Stati Uniti, considerata l'influenza mantenuta dal mezzo televisivo sugli utenti. Ma di fronte ai mezzi usati da *Cambridge Analytica*[74] - l'azienda che tramite la Rete inviava ai cittadini statunitensi messaggi elettorali ritagliati sui loro interessi e desideri (desunti dall'illecita sottrazione di dati personali sensibili) - la *par condicio* televisiva si è ridotta a pulce sul dorso dell'elefante.

Nel frattempo, le risorse pubblicitarie di Google hanno superato quelle ricevute dalla stampa di tutto il mondo, mettendo alle strette il mezzo che più di altri è in grado di alimentare un dibattito pubblico adeguatamente informato (utilizzando a tal fine anche la Rete, senza tuttavia rimanere vittima delle sue peggiori scorciatoie).

Per tale motivo appare preoccupante che la nostra Corte costituzionale appaia ancora succube del mito dell'informazione online, come sembra emergere dal suo marcato disinteresse verso la stampa e verso l'ormai gravissimo inaridimento delle sue fonti di finanziamento. Alla richiesta degli editori di poter contare su criteri predeterminati ed imparziali nella distribuzione dei finanziamenti statali il giudice costituzionale si è invero limitato ad opporre che essi non hanno nessun diritto ad ottenere detti finanziamen-

nell'era di Internet, cit.

[70] T. Wu, *Is the First Amendment Obsolete*, cit. Come è noto, la Corte Suprema, nella sentenza *Red Lion Broadcasting Co. v. Federal Communications Commission*, 395 U.S. 367 (1969) stabilì che, per rimediare alla scarsità del mezzo-etere, al pubblico andava riconosciuto il diritto di accedere - tramite ciascun canale televisivo - a diverse idee ed esperienze "sociali, politiche, estetiche e morali".

[71] Nella sentenza *Pacific Gas & Electric v. Public Utilities Commission*, 475 U.S. 1 (1986) la Corte Suprema ritenne che la compagnia erogatrice del gas (che pure era concessionaria del potere pubblico) non poteva essere costretta ad ospitare sulla busta contenente la bolletta i commenti di una associazione di utenti del servizio.

[72] Cfr. la ricostruzione di J.A. Barron, *Access To The Media - A Contemporary Appraisal*, in *Hofstra L. Rev.*, 2007, 937 ss.

[73] Una prima apertura si registra oggi in Cass. civ., sez. I, ord. 17 aprile 2020, n. 7893, riguardante la discriminatorietà del divieto opposto dal Comune di Verona all'affissione di un manifesto di propaganda dell'Unione atei e agnostici razionalisti.

[74] Per non parlare delle supposte interferenze telematiche russe nell'ultima campagna presidenziale statunitense: v. A. Koltaj, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere.,* cit., 157 ss.

ti, salva la discrezionalità del legislatore di disporre diversamente. Dimenticando che quando lo Stato eroga denari pubblici deve evitare in ogni modo forme anche indirette e involontarie di pressione sulla stampa (quali evidentemente possono derivare dalla discrezionalità del Governo sull'ammontare dei contributi)[75]; e che il pluralismo della stampa non è un lusso, ma una necessità, come lo stesso giudice ha sempre sottolineato in passato[76], e come è tanto più vero oggi, quando il giornalismo investigativo o di denunzia rischia di scomparire.

In realtà, a parte i tentativi di imporre alle piattaforme obblighi di sorveglianza (gravati dal rischio di rafforzare una censura privata incontrollabile), gli unici rimedi che sembrano effettivamente opponibili alla deriva antidemocratica della Rete sono due: a monte, il rafforzamento della pubblica istruzione, che deve comprendere la consapevolezza nell'uso dei media; a valle, la creazione di siti, pubblici o garantiti dai poteri pubblici, cui il cittadino possa rivolgersi per valutare la qualità e la credibilità delle notizie che riceve. La stessa dottrina statunitense ha accolto, almeno in parte, la necessità di un più deciso intervento pubblico, da ottenere mediante l'erogazione di finanziamenti statali ai siti privati che promuovano il dibattito pubblico, ovvero a siti di servizio pubblico[77].

Una volta archiviata la retorica deregolatoria (come ha richiesto la grande crisi economica iniziata nel 2008), e una volta ridimensionata la frontiera che separava le piattaforme dai veri e propri mass media, non vi è invero motivo di non immaginare, accanto alle televisioni di servizio pubblico, siti web destinati parimenti ad informare, educare e intrattenere, cui potrebbero rivolgersi soprattutto i più giovani.

È questo il passo decisivo che si chiede oggi all'Unione europea, dove l'operatività dei media pubblici in Rete non è mai stata data per scontata, e anzi è vista come un tentativo di insidiare i legittimi profitti delle piattaforme private. Ciò non desta meraviglia, se si ricorda come l'Unione europea abbia sostanzialmente mutuato la destinazione della Rete ai soli privati quale derivava dalla disciplina statunitense, salvo poi gravare questi ultimi di crescenti compiti censori.

Il servizio pubblico potrebbe apparire quasi come un'ancora di salvataggio nel mare tempestoso e infido della Rete[78]: purché cerchi di emendarsi dai vizi dei quali è vittima, più che altrove, nel nostro Paese.

---

[75] Cfr. Corte cost., 30 maggio 1977, n. 94.

[76] Cfr. Corte cost., 25 luglio 2019, n. 206, annotata criticamente da A. Vaccari, *Sul finanziamento pubblico all'editoria: un'occasione mancata per la Corte?* in *Giurisprudenza Costituzionale*, 4, 2019, 2307 ss. Sull'imperativo di carattere costituzionale che richiede di contrastare l'inaridimento delle fonti della stampa v. Corte costituzionale, sentt. 225/1974, 202/1976, 231/1985, 826/1988, 420/1994.

[77] Così L.C. Bollinger, *Epilogue*, ivi, 297 ss., dove si accolgono i suggerimenti già elaborati con riguardo ad altri mezzi da O. Fiss, *The Irony of Free Speech,* Cambridge (MA), 1996 e C.R. Sunstein, *Television and the Public Interest,* in *California L. Rev.*, 2000, 396 ss.

[78] Cfr. ora in tal senso G.E. Vigevani, *I media di servizio pubblico nell'età della rete,* Torino, 2018.

Lo spazio digitale dei lavori parlamentari e l'emergenza sanitaria Covid-19*

Paola Marsocci

Abstract

Il saggio tratta dell'uso delle tecnologie digitali al servizio della funzionalità del Parlamento italiano, a partire dalla circostanza di fatto del contrasto alla pandemia scatenata dal virus Covid-19. Attraverso la ricostruzione degli eventi, delle decisioni adottate dalle Camere per garantire la prosecuzione dei lavori e del vivace dibattito dottrinale, si propone di evidenziare e discutere tali questioni, nella prospettiva di proporre le necessarie distinzioni e le possibili soluzioni nel rispetto pieno del costituzionalismo democratico, a prescindere dalle sollecitazioni stringenti di urgenza e necessità, quando non dalla mera opportunità pratica.

This paper deals with the use of digital technologies allowing the functionality of the Italian Parliament, starting from the factual circumstance of the fight against the pandemic triggered by the Covid-19 virus. For this purpose, current events are reconstructed together with the decisions taken by the Chambers to guarantee the continuation of their work and the lively doctrinal debate concerning them. These issues are considered and discussed with a view to proposing some necessary distinctions and possible solutions, in full respect of democratic constitutionalism, regardless of the pressing demands of urgency and necessity, or even of mere practical opportunity.

Sommario

1. Le circostanze di fatto e la loro (al momento) incessante evoluzione. Gli obiettivi del contributo. – 2. La riduzione del numero dei votanti e le altre decisioni assunte da Camera e Senato. – 3. Quali sono le questioni sul tappeto. Primo: mantenere le Camere aperte e funzionanti. Secondo: capire come, senza contrastare la Costituzione. – 4. (*segue*) Terzo: decidere (come?) con quali modalità procedurali e strumenti. Quarto: valutare se ciò valga solo nella contingenza presente o anche per il futuro. – 5. La riunione e le altre libertà praticate tramite le tecnologie digitali. – 6. Perché è (ormai) indispensabile che si scelga, distinguendo, quali sono le tecnologie digitali idonee all'esercizio della funzione parlamentare. – 7. Come non cadere nel dilemma dello "Stato soluzionista", alcune considerazioni conclusive.

*Questo saggio è anche destinato al *Liber Amicorum* per Pasquale Costanzo.
L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a doppio cieco

Keywords

parlamentarismo - emergenza sanitaria - libertà di riunione - presenza digitale - piattaforme pubbliche online

1. Le circostanze di fatto e la loro (al momento) incessante evoluzione. Gli obiettivi del contributo

L'indagine ha ad oggetto la funzionalità del Parlamento italiano in periodi di emergenza sanitaria, un tema che si è imposto all'attenzione dell'opinione pubblica a partire dalla circostanza di fatto del contrasto alla pandemia scatenata dal virus Covid-19[1]. Uno dei tanti, in verità, solo che questo nuovo ceppo di Corona virus a molti appare peggiore quanto agli effetti che ha provocato e provocherà, in termini di minaccia ad alcuni beni collettivi, quali salute, sicurezza, pacifica convivenza. Porre l'attenzione anche su quest'ultimo punto[2]

[1] L'Organizzazione mondiale della sanità ci informa che i Coronavirus sono stati identificati a metà degli anni '60, sono noti per infettare l'uomo ed alcuni animali (inclusi uccelli e mammiferi) e che le cellule bersaglio primarie sono quelle epiteliali del tratto respiratorio e gastrointestinale. Sulle cause delle epidemie, sul nesso probabile o per alcuni accertato con l'attuale modello di urbanizzazione e produzione negli allevamenti di carne, cfr. la ricostruzione di A. L. Lara, *El principal peligro que enfrentamos es considerar al nuevo coronavirus como un fenómeno aislado, sin historia, sin contexto social, económico, cultural*, *El Pais*, 29 marzo 2020; Sul tema cfr. le riflessioni di M. Carducci, *Il corpo "malato" del Sovrano*, in *LaCostituzione.info* (19 marzo 2020).

[2] Come ha fatto G. Silvestri, *Covid-19 e Costituzione*, intervento pubblicato sul sito di *Unicost. Unità per la costituzione*, 10 aprile 2020. L'A. richiama anche, ma per allontanare dalle suggestioni di impropri accostamenti, le previsioni dell'art. 78 Cost.
Non è infatti a mio avviso l'uso della similitudine con la Guerra (ricorrente nel linguaggio sia mediatico sia, in alcuni casi, politico) che ci può aiutare in questo frangente. Quando incautamente si utilizzano espressioni come "siamo in guerra" o simili, occorre almeno, nell'usare il paragone, separare il fatto dai suoi effetti. La guerra coinvolge le nazioni per via di un conflitto dichiarato o subito da chi ha il potere in quei territori e su quei popoli; a norma dell'art. 11 della Costituzione italiana essa è uno «strumento di offesa alla libertà degli altri popoli», che l'Italia ripudia; i conflitti bellici hanno a che fare con la volontà umana, spesso sono determinati da quella di pochi individui, che imprimono la direzione ai destini altrui, e sono da scongiurare con la stessa forza della volontà umana. Rimane preferibile parlare di 'emergenza sanitaria', per contribuire a sottolineare invece che il portatore dall'aggressione è un virus, pur sempre esterno o estraneo e pur sempre introdottosi a forza nelle nostre vite, non potendo qui entrare nel merito della delicata questione del ruolo attivo dell'umanità nell'alterazione degli equilibri ambientali, sopra accennato. Anche se torna comoda la metafora del nemico, il rischio è far scivolare questa qualifica addosso a chi è vittima, perché in prima persona colpito dalla malattia e potenzialmente infettivo, quando non a interi popoli che per primi hanno vissuto l'epidemia. Così pure, non di soldati e eroi in prima linea si deve parlare, perché la retorica offusca la questione della necessità e urgenza della piena e immediata tutela della salute psico-fisica di chi svolge determinate funzioni o attività. Non siamo testimoni di nessun "super potere", ma solo di una aumentata fragilità individuale e collettiva. Sottovalutare gli effetti delle parole di chi invoca lo Stato di guerra comporta l'ulteriore rischio di mal interpretare la conseguente riallocazione dei poteri pubblici, in particolare di quelli normativi. Tutt'altro valore ha invece la similitudine quando trattiamo del tema degli effetti dell'emergenza; dovremo da subito osservare, valutare, discutere e contrastare conseguenze e danni paragonabile a quelli di un post conflitto bellico, nelle prospettive economico-sociale, psicologico-comportamentale, etica e, non da ultimo, normativa e giuridica.
Sul punto, cfr. P. Armaroli, *Intervista a Sabino Cassese: "La pandemia non è una guerra. I pieni poteri al governo non sono legittimi"*, in *Il Dubbio*, 13 aprile 2020; per un punto di vista non solo giuridico, cfr. le riflessioni di A. Testa, *Smettiamo di dire che è una guerra*, in Internazionale, 30 marzo 2020 e di S. Milesi, *La viralità del linguaggio bellico*, intervista a Massimo Vedovelli, in *Vita*, 26 marzo 2020.

ha a mio avviso il pregio di rendere necessarie le riflessioni sulle ripercussioni future della fase attuale, sollecitando alle azioni volte a prevenire e calmierare il loro impatto sulla tenuta della coesione sociale.

Questo è "il" dato da cui partire, che – oltre a non consentire previsioni sulla durata dello stato di emergenza – ci pone di fronte ad una apparentemente incessante mutevolezza, di eventi, di opinioni, di sperimentazioni. Così anche, direi persino, la catena normativa che è entrata in vigore a partire dal 31 gennaio 2020[3] si iscrive 'a buon diritto' tra i fatti esemplifcativi di questo scenario e la sua interpretazione permette di puntare i riflettori sullo stato di salute (anche) della forma di governo italiana, tra indirizzo politico nazionale e rapporto tra i diversi livelli territoriali coinvolti.

Tra le circostanze di fatto che è utile porre a premessa delle considerazioni che seguono, occorre poi includere la fisicità dell'attività dei parlamentari (intesa propriamente come presenza e uso del corpo), negli spazi materiali messi a disposizione dai Palazzi della rappresentanza nazionale. La notevole e repentina diffusione della malattia non ha risparmiato infatti i membri delle Camere – come anche del Governo, Presidenti di Regione, Sindaci e consiglieri degli enti locali e regionali[4], alcuni dei quali direttamente preposti alla gestione della salute pubblica –; in molti altri casi, le misure via via più restrittive rispetto al controllo sulla libertà di circolazione nel territorio nazionale hanno concretamente reso più complessi e *delicati* i loro spostamenti, in particolare per i parlamentari provenienti delle "zone rosse".

Infine, tra le evidenze va ricordato l'uso massivo e pervasivo delle tecnologie digitali, al servizio di *ogni* libertà costituzionalmente riconosciuta e garantita (su questo specifico punto tornerò più avanti)[5].

---

[3] Delibera del Consiglio dei Ministri del 31 gennaio 2020, *Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*, (GU n.26 del 1-2-2020). Per una prima disamina della catena normativa, a partire da questa iniziale delibera, cfr. I. Massa Pinto, *La tremendissima lezione del Covid-19 (anche) ai giuristi*, in *Questione giustizia*, 18 marzo 2020; M. Luciani, *Il sistema delle fonti del diritto alla prova dell'emergenza*, *Liber Amicorum per Pasquale Costanzo*, in *Consulta online*, 11 aprile 2020.

[4] Sulla malattia, come impedimento temporaneo o permanente, allo svolgimento in presenza fisica delle funzioni pubbliche, qualche riflessione ultimamente, G. Santini, *Funzionalità delle istituzioni e impedimento dei titolari. Note sulla supplenza in tempo di epidemia*, in *BioDiritto*, 2, 2020, che giunge alla fine della sua disanima condivisibilmente a ritenere che «il sistema istituzionale italiano, per le numerose norme in materia di supplenza, non vada soggetto a particolari disfunzioni nel caso di improvvisa vacanza del titolare di un organo; piuttosto, si porrebbero dei problemi qualora più soggetti risultassero impediti nello stesso momento: talora, non si riesce a rinvenire un supplente "di secondo livello", se non a prezzo di qualche forzatura. Dovrebbero pertanto essere attentamente valutati, per il presente e per il futuro, strumenti telematici che permettano ai titolari di cariche pubbliche, confinati a domicilio o in un luogo di cura, di esercitare a distanza il maggior numero possibile di attribuzioni, fatte salve le esigenze di riserbo tipiche delle posizioni di maggiore responsabilità», 6; cfr. anche, S. Curreri, *L'attività parlamentare ai tempi del Covid-19: fiat iustitia et pereat mundus?*, *LaCostituzione.info*, 11 marzo 2020.

[5] Impiegata in modo diffuso nei contesti sociali, commerciali ed economici di tutto il mondo, la tecnologia dell'informazione, in acronimo TI (in inglese *information technology*, in acronimo IT), è l'insieme dei metodi e delle tecnologie che vengono utilizzate in ambito pubblico, privato o aziendale per l'archiviazione, la trasmissione e l'elaborazione di dati e informazioni attraverso l'uso di reti (reti aziendali, internet ecc.), elaboratori (*PC*, *server*, *mainframe* ecc.) e attrezzature di telecomunicazione (*datacenter*, *router*, *smartphone*, *tablet*, *GPS,* ecc.). Il termine si usa comunemente come sinonimo di computer e reti di computer, ma ricomprende anche altre tecnologie di distribuzione dell'informazione come la televisione, i telefoni e internet, cfr. la definizione disponibile a *it.wikipedia.org*.

Non nuove, al contrario, risultano alcune considerazioni di fondo che possono guidare il ragionamento giuridico e l'azione politico-istituzionale di questi mesi.
In gran parte delle riflessioni sino ad oggi pubblicate sono poste almeno due questioni. La prima riguarda la possibilità che le Camere continuino a svolgere compiutamente ciascuna delle proprie attribuzioni, o almeno quella parte di attività improcrastinabili e/o essenziali per la piena tenuta del sistema democratico; tale dibattito – con al centro il rifiuto di qualsiasi forzatura al principio di non sospensione delle funzioni parlamentari in democrazia – si è fatto più acceso appena arrivata la notizia delle decisioni assunte in Ungheria e della conseguente reazione dell'UE[6] ed ha aggiunto importanti spunti sul nodo del ruolo della comunicazione (istituzionale e mediatica) nella formazione dell'opinione pubblica, per il mantenimento della coesione sociale.
La seconda questione è, conseguentemente, incentrata su quali siano eventualmente i mezzi, normativi e tecnologici, sui quali si possa e occorra fare affidamento. Ci si chiede in sostanza come, riducendosi o addirittura venendo meno la possibilità per i parlamentari di essere fisicamente nei luoghi della rappresentanza nazionale, il Parlamento possa "lavorare"[7], avvalendosi di strumenti e conseguentemente procedimenti che permettano di assolvere alle proprie funzioni da luoghi *altri* rispetto a quelli messi a disposizione dai palazzi di Montecitorio e Madama.
E' noto che le restrizioni all'esercizio dei diritti (giustificate, in via generale, da situazioni attuali e concrete – come nel caso dell'epidemia – di pregiudizio per la sanità, sicurezza o incolumità pubblica) introdotte dalle norme vigenti alle libertà di circolazione e di riunione valgano per tutti i cittadini e i residenti sul territorio italiano; così come è valida per tutti la deroga in caso di "comprovate esigenze lavorative" [8]. Tra

[6] Cfr., la nota redazionale, *Stato di pericolo e poteri straordinari al governo ungherese*, in *Questione giustizia*, 1° aprile 2020. Più recentemente anche in Slovenia si paventano rischi alti per la democrazia, considerato che anche lì il Presidente ha accentrato nel governo i pieni poteri, cfr. S. Benazzo, *Janez Janša ha ottenuto pieni poteri come Orbán. La Slovenia si scopre sovranista*, in *Linkiesta*, 17 aprile 2020.

[7] L'uso della parola lavoro in questo scenario è scelto anche per evocare il dibattito (connotato anche da toni polemici) sulla opportunità di equiparare chi svolge funzioni pubbliche di gestione e rappresentanza con i dipendenti dei comparti chiamati ad assicurare le prestazioni e i servizi essenziali, sia pubblici sia privati, rispetto alla necessaria presenza sul luogo di lavoro. Pone opportunamente l'accento sulla distinzione tra lavoro "comune" e svolgimento delle funzioni di rappresentanza di deputati e senatori, M. Zampini, *Camere riunite, trattiamo bene le nostre vituperate Camere*, in *Alto Adige*, 30 marzo 2020, 1, «a far considerare che quello dei parlamentari sia un lavoro come quello delle professioni comuni ha contribuito in modo decisivo la recisione del legame tra i parlamentari e gli eletti». Le attività dei parlamentari che non si esauriscono (non dovrebbero) nelle attività all'interno delle sedi parlamentari, ma si prolungano sui territori dal collegio elettorale, passando per i partiti, e ritorno; ciò almeno è quanto avveniva prima della serie di riforme elettorali che hanno prodotto un allontanamento dal circuito appena descritto e un accentramento dell'influenza in capo ai soli vertici delle formazioni politiche; quegli stessi vertici che hanno usato e abusato delle tecnologie digitali anche per l'assolvimento di funzioni pubbliche, oggi, in tempi di emergenza, reclamano con forza la presenza fisica nelle aule della rappresentanza. Altro è, ovviamente, sostenere come fa G. Azzariti, *Editoriale. Il diritto costituzionale d'eccezione*, in *Costituzionalismo.it*, 1, 2020, 4, che sia «difficile da accettare l'idea che rimangano aperti i servizi pubblici essenziali (ospedali, farmacie, alimentari, imprese produttive necessarie, persino le tabaccherie) e non si riesca a garantire un modo per assicurare, nel rispetto delle norme di sicurezza e di quelle politiche, la continuità dell'organo vitale della democrazia rappresentativa».

[8] Rimane essenziale ricordare il significato specifico di *sospensione* dell'esercizio dei diritti e la necessaria distinzione da fare rispetto al concetto della loro restrizione, in osservanza dei limiti prescritti costituzionalmente e considerate le garanzie della riserva di legge e della riserva di giurisdizione; cfr., specialmente A. Pace, *Problematica delle libertà fondamentali, Lezioni. Parte generale*, Padova, 1990, 157 ss.,

le quattro citate nei modelli di autocertificazione messi a disposizione dal Ministero dell'interno (in attuazione del d.l. 25 marzo 2020, n. 19, che all'art. 1, c. 2, lett. *a*), consente espressamente «spostamenti individuali limitati nel tempo e nello spazio o motivati da esigenze lavorative, da situazioni di necessità o urgenza, da motivi di salute o da altre specifiche ragioni»), immaginiamo che sia questa, da interpretare insieme a "altre specifiche ragioni", a riguardare la circolazione dei parlamentari.

Per quel che riguarda più in generale lo svolgimento delle attività e funzioni parlamentari, è almeno opportuno ricordare, poi, che le Camere, come qualsiasi altra istituzione pubblica, si avvalgono di un numero elevato di personale (1.139 al 2017 quella dei Deputati – ultimo dato disponibile in Relazione all'Ufficio di presidenza sullo stato dell'amministrazione – e 610 il Senato – dato pubblicato sul portale istituzionale, a cui bisogna aggiungere i dipendenti dei gruppi ecc.) e che, per ciascuno di questi dipendenti, il diritto alla salute ed alla sicurezza sul posto di lavoro deve essere garantito[9]. Inoltre, i Palazzi della rappresentanza sono aperti ordinariamente ad un pubblico ampio, che va dai cittadini che intendano essere presenti ai lavori delle Assemblee, ai partecipanti ad incontri e convegni, ai giornalisti parlamentari, agli ospiti di parlamentari e gruppi[10].

Nella prospettiva di chi studia lo spazio di Internet nel costituzionalismo, con le considerazioni che seguono si tenterà, dunque, di contribuire al dibattito sulle garanzie da apprestare ai diversi diritti coinvolti, nel caso di esercizio delle prerogative dei parlamentari tramite piattaforme digitali: (a partire da) quello di riunione, di espressione, di voto etc., fino al diritto alla riservatezza e intimità familiare e al domicilio dei parlamentari e di chi vive con loro e, in definitiva, si tratterà di tentare di considerare un

«la locuzione 'sospensione dei diritti costituzionali' è una formula ellittica con la quale comunemente si allude alla privazione (temporanea) dell'efficacia di una o più norme costituzionali ricognitive dei diritti, da parte di un atto-fonte diverso dalla Costituzione»; si ricorderà che l'A. individua nella legge ordinaria del Parlamento lo strumento idoneo, aggiungendo che «sembra privo di senso storico, e perciò giuridicamente scorretto, dedurre […] la conseguenza […] che nel nostro ordinamento, tranne l'ipotesi di 'poteri necessari' al Governo in conseguenza della delibera parlamentare dello Stato di guerra (art. 78 Cost), non esisterebbe la possibilità di dichiarare lo stato di emergenza e, conseguentemente, non esisterebbe il potere governativo di sospendere in via generale, anche se per un periodo essenzialmente limitato di tempo (C. cost., sent. 16/1982), l'efficacia delle norme costituzionali attributive di diritti»; scartata l'ipotesi di considerare la *necessità* come fonte autonoma del diritto, l'A. indica il decreto-legge come strumento idoneo a tal fine.

A questo riguardo, G. Silvestri, *Covid-19 e Costituzione*, cit., propone gli argomenti utili a valutare in concreto se gli interventi istituzionali adottati siano appropriati, per negare così la necessità che «una situazione di emergenza richieda la sospensione, ancorché temporanea, delle garanzie, personali e istituzionali, previste dalla Costituzione» ed evidenzia «il punto capitale della problematica costituzionalistica della gestione dello stato di necessità: il rispetto del principio di legalità e della riserva di legge».

[9] Sul punto, A. Maresca, *Il diritto del lavoro al tempo del COVID-19*, *Editoriale* in *Federalismi.it*, 1° aprile 2020.

[10] A partire dal 25 febbraio 2020, i collegi dei Questori della Camera e del Senato hanno adottato una serie di misure progressive (disponibili nelle pagine degli archivi notizie dei rispettivi portali) volte a limitare l'ingresso nelle sedi della Camera a coloro che si trovassero nelle condizioni previste dalle disposizioni adottate dalle autorità sanitarie competenti, sospendendo eventi e iniziative di qualsiasi natura aperti al pubblico esterno e limitando il numero degli "ospiti" necessari (compresi i collaboratori dei membri del Governo). Le conferenze stampa sono state sospese dal 26 marzo. I lavori parlamentari, in attuazione del principio costituzionale della loro pubblicità, potranno essere seguiti, come sempre, attraverso il canale satellitare e la web-tv di Camera e Senato.

tema enorme che ha interessato e interessa la storia della filosofia occidentale: «che cosa significa presenza, esser presente? Non sembra che vi sia nulla di più chiaro: possiamo avere dubbi sulla presenza di questo o di quello, ma non su ciò che significhi esser presente»[11].

La mediazione dello strumento tecnologico contraddice (necessariamente) la presenza? E, chiedendo scusa per il gioco di parole, diviene più urgente sciogliere questo nodo nei luoghi della mediazione per eccellenza, quelli della decisione parlamentare?

2. La riduzione del numero dei votanti e le altre decisioni assunte da Camera e Senato

Il ragionamento di tutti coloro che hanno commentato cosa sta accadendo alla vita del Parlamento in questa fase ha poi, ovviamente, tenuto conto delle decisioni assunte da entrambe le Camere[12]. Sembra utile riepilogarle, di seguito, anche per arrivare ad analizzare le posizioni della dottrina a riguardo.

Al Senato, la Presidente Casellati ha comunicato il 9 marzo 2020 che «la Conferenza dei Capigruppo all'unanimità ha stabilito che le Commissioni permanenti si riuniranno esclusivamente per la trattazione di provvedimenti riguardanti l'emergenza sanitaria ed economica connessa al Coronavirus. Sono sospese le attività di tutte le altre Commissioni. Nella giornata di mercoledì 11, la votazione sullo scostamento di Bilancio avverrà per scaglioni e attraverso appello nominale e vedrà la presenza nel dibattito di 6 senatori per gruppo onde osservare la distanza di sicurezza raccomandata per tutti i cittadini»[13].

Il 31 marzo 2020, il Presidente della Camera, Roberto Fico, ha prospettato in Giunta per il regolamento i nodi relativi alle modalità di svolgimento dei lavori delle Commissioni, che tenga conto della possibilità di dibattiti e votazioni a distanza per i parlamentari impossibilitati a prendervi parte, a causa delle limitazioni della libertà di circolazione disposte per contenere l'emergenza Covid-19, in particolare quelle che

[11] Ce lo ricorda M. Adinolfi, *Voto a distanza e modalità di presenza: una questione di principio*, in *PER, progresso europa riforme*, Quaderno 5, 11 marzo 2020, 1: «Anche se non fosse possibile tracciare quella linea ed escludere categoricamente la presenza in remoto, a distanza, online, dal novero delle presenze vere e reali, non per questo non sarebbe possibile distinguere queste diverse modalità di presenza, e assegnare a ciascuna regimi determinati di esercizio, e specifiche modalità di accertamento».

[12] Si ricorda anche che il 14 marzo, alcuni senatori e deputati di "Movimenta", prima firmataria l'On. Quartapelle (Pd), hanno lanciato un appello per mettere in sicurezza personale e parlamentari ed adottare modalità di lavoro a distanza e riattiviamo l'attività di Palazzo Madama e Montecitorio.

[13] Decise le posizioni critiche sul punto della "autoriduzione" del numero dei votanti decisa da entrambi i rami del Parlamento, soprattutto riguardo alla delibera sullo sforamento di bilancio, espresse da M. Villone, *Il parlamento nella spirale di due crisi*, in *Il Manifesto*, 15 marzo 2020 e di M. Ainis, *Parlamento, meglio distante che latitante*, in *La Repubblica*, 18 marzo 2020; C. Melzi d'Eril - G. E. Vigevani, *Il Parlamento non sia assente*, in *Il Sole24Ore*, 17 marzo 2020; F. Lanchester, *Emergenza coronavirus: il dibattito sul voto a distanza*. Intervista a L. Palazzolo, 12 marzo 2020, in *radioradicale.it*: «occorre evitare l'antiparlamentarismo, non si può pensare di delegare ai soli capigruppo, ma bisogna preservare l'esistenza di tutta l'assemblea». Cfr. anche S. Ceccanti, *Intervento* in diretta Facebook, organizzata dal Presidente della Commissione affari costituzionali della Camera, on. Brescia, su *Parlamento aperto: a distanza o in presenza?* del 27 marzo 2020, disponibile su *radioradicale.it.,* che segnala come la soluzione della autoriduzione pro quota sacrifichi comunque il voto personale e l'immagine stessa del Parlamento, che lavora ad 1/6 delle presenze.

impediscono gli spostamenti dalle cd. zone e poi tra comuni[14]. Già in una precedente riunione (4 marzo), l'orientamento concorde era stato che fosse necessaria una previsione «di rango legislativo o, nell'immediato, anche con fonte di natura secondaria – finalizzata a consentire ai parlamentari, a determinate condizioni, tali da non mettere a rischio l'efficacia dell'azione di contenimento della diffusione del virus, di circolare sul territorio nazionale per esigenze connesse all'esercizio delle loro funzioni». Il riferimento (ad oggi) non è intervenuto esplicitamente, ma resta desumibile dalle specifiche deroghe previste dal d.l. n. 19 del 25 marzo scorso, art. 1, c. 2, lett. *a*). Il quadro di incertezza si è, peraltro, complicato con le ordinanze adottate da alcuni Presidenti di Regioni che hanno imposto l'obbligo di quarantena per quattordici giorni per tutti coloro che fanno ingresso nei territori delle relative regioni[15].

Tuttavia, dovendo contemperare tale possibilità con le prescrizioni e raccomandazioni delle autorità sanitarie, unanimemente la Conferenza dei Presidenti di Gruppo ha deciso di concentrare le attività parlamentari all'esame di atti indifferibili e urgenti, connessi all'emergenza Covid-19 e, per altro verso, di limitare la presenza dei deputati in seduta per periodi prolungati. In Assemblea, dunque, andrà solo l'«esame di progetti di legge indifferibili e urgenti – in primo luogo i disegni di legge di conversione di decreti-legge – e svolgimento di interrogazioni a risposta immediata e di interpellanze urgenti, ai fini del mantenimento di una costante interlocuzione con il Governo». Nelle Commissioni e altri organi parlamentari, avverrà solo l'esame degli atti indifferibili e urgenti, le audizioni dei Ministri di settore (o anche di altri soggetti) in relazione alle diverse tematiche connesse all'emergenza stessa, nonché sedute di sindacato ispettivo e l'espressione di pareri su atti del Governo in scadenza e non differibili.

A fronte di tale notevole riduzione e concentrazione dei lavori parlamentari (pienamente validità sotto il profilo ordinamentale e in linea, si sottolinea nel resoconto, con le drastiche misure prese dai Parlamenti di altri Paesi europei)[16], la Camera ha perseguì-

[14] Documento consultabile online in *camera.it*.

[15] Quando non anche il divieto di entrata e uscita dai territori regionali, frattura grave dell'ordine costituzionale, stigmatizzata anche da G. Silvestri, *Covid-19 e Costituzione,* cit., «nessuna legge autorizzativa potrà mai consentire ad una Regione (a fortiori ad un ente locale) di emanare norme che impediscano o ostacolino la libera circolazione delle persone e delle cose tra le Regioni, in palese dispregio del primo comma del citato art. 120 della Cost., come purtroppo in qualche caso si sta verificando. Un blocco di transito da una Regione ad un'altra ha una rilevanza nazionale per diretto dettato costituzionale. Sempre e comunque è necessario un provvedimento statale. La Repubblica «una e indivisibile» (art. 5 Cost.) non può tollerare che parti del territorio e della popolazione nazionali si pongano in contrapposizione tra loro. Vi osta, oltre che il principio di unità nazionale, anche il principio di solidarietà (art. 2 Cost.), inconciliabile con qualunque chiusura egoistica o particolaristica». Sul punto specifico dell'impossibilità di impedire ai parlamentari il diritto-dovere di raggiungere le Camere di appartenenza, cfr. R. Dickmann, *Alcune questioni di costituzionalità in tema di voto parlamentare a distanza*, in *Federalismi.it*, 1° aprile 2020, 15.

[16] Per un raffronto, v. gli spunti di F. Clementi, *Proteggere la democrazia rappresentativa tramite il voto elettronico: problemi, esperienze e prospettive (anche nel tempo del coronavirus)*, in *Federalismi.it*, 6, 2020, 221 ss. e *Intervento* in diretta Facebook, 27 marzo, cit., dove si ricorda che «Germania, Irlanda e Polonia non hanno il vincolo della presenza fisica, la Francia ammette il voto per delega, così come Svezia e Danimarca. In Lettonia, Canada e Inghilterra i Parlamenti hanno fatto la scelta di ridurre le loro attività. Altri, come la Svizzera hanno ridotto gli spazi fisici. Il Brasile e la Spagna e Ue hanno adottato modalità a distanza».
Diversamente, M. Luciani, *Intervento* in diretta Facebook, organizzato dall'On. G. Brescia, Presidente Camera Deputati 3 aprile 2020, in *radioradicale.it*, sottolinea l'attenzione che si deve nella comparazione con altri ordinamenti nazionali, alle peculiarità di quanto stabilito nelle relative Costituzioni e nei Regolamenti parlamenti. Anche l'esempio del Parlamento europeo è considerato, con la grande differenza

to l'obiettivo di spostare le persone coinvolte in spazi ampliati, riprogrammando l'uso di determinate aule e sale, a garanzia della distanza di sicurezza. In particolare, per i lavori dell'Assemblea, sono state adottate idonee modalità di votazione, come quella per appello nominale. Con l'obiettivo di agevolare ulteriormente l'organizzazione pratica, l'atteggiamento che trapela è quello di apertura a forme di partecipazione a distanza ai lavori, in particolare delle Commissioni (videoconferenze e trasmissione via *webtv*, con particolare riferimento allo svolgimento di sedute nelle quali non sono previste votazioni, quali quelle dedicate alle attività conoscitive e al sindacato ispettivo).
Attraverso queste comunicazioni, il Presidente, ha avuto la possibilità sia di ribadire che «tutti i parlamentari – con eccezione di coloro che per motivi sanitari di natura personale non possono allontanarsi dal luogo di domicilio – possono effettuare spostamenti» e raggiungere le sedi della Camera, sia di sollecitare la ricerca di «ulteriori strumenti e procedure già previsti nel nostro ordinamento da attivare nel contesto attuale e, dall'altro, le innovazioni che possono essere eventualmente introdotte, anche attraverso una applicazione in via analogica di istituti vigenti[17], in termini compatibili con le norme ed i principi del Regolamento e con la Carta costituzionale».
Altrettanto chiaramente, è prospettato il tema della possibile interpretazione evolutiva dell'art. 64 Cost. che consenta (in situazioni emergenziali, però) di considerare presenti ai lavori deputati che partecipino agli stessi da remoto, per il tramite di videoconferenze o altri strumenti tecnologici, senza pregiudizio per le prerogative dei parlamentari (discussione, voto, immunità di sede, divieto di accesso alle aule parlamentari da parte di estranei, poteri presidenziali di controllo della regolarità dei lavori). In ogni modo, ciò che – evidentemente con la fretta richiesta – viene sollecitata è «un'ampia adesione

che a limitare gli spostamenti dei membri sono le nuove barriere a confine dei Paesi dell'Unione, causa della impossibilità di fatto per i parlamentari europei di recarsi a Bruxelles. Quest'ultima esperienza è stata descritta dal suo Presidente, David Sassoli, nell'*Intervento* in diretta Facebook, 27 marzo 2020, cit. Da ultimo, a fine aprile è arrivata la decisione della Camera dei Comuni del Regno Unito di consentire una procedura ibrida con la presenza di parlamentari sia in aula sia da remoto. Lo stesso Presidente della Commissione che ha proposto la modifica, Sir Lindsay, ha dichiarato di immaginare questa situazione come un passo verso un Parlamento completamente virtuale, utile a consentire ai parlamentari di rimanere vicini alle loro comunità, pur continuando il loro importante lavoro di supervisione del governo (cfr. *Coronavirus: deputati intervistano i ministri tramite videoconferenza*, in *DicoNews*, 16 aprile 2020). Decisone assunta non senza conflittualità, come riporta la cronaca, tra le posizioni del *Leader of the House,* Jacob Rees-Mogg, il quale ha osservato che «oggi, invece grazie alla tecnologia il Parlamento può riunirsi, seppur in condizioni straordinarie, e non potrei essere più d'accordo con questa soluzione» e quelle di altra parte del partito conservatore, che ritiene la decisione scioccante e antidemocratica. Il piano per portare avanti i lavori parlamentare con un format ibrido, ovvero 50 deputati in aula a Westminster debitamente distanziati e altri 120 a rotazione (su 650) – che non prevede per il momento l'espressione del voto da remoto –, collegati in remoto tramite la piattaforma Zoom, è stato approvato senza che fosse necessario un voto formale e sarà utilizzato inizialmente fino al 12 maggio, ma potrebbe essere prorogato a seconda delle esigenze, cfr. A. Guerrera, *Gb, Il coronavirus trasforma la Camera dei Comuni in un "Parlamento virtuale"*, in *la Repubblica*, 21 aprile 2020.

[17] Così, sono state prospettate dalla dottrina la possibilità di istituire una Commissione speciale, ai sensi dell'art. 22 del Regolamento, cui affidare, in sede referente, i progetti di legge indifferibili e urgenti (in realtà già scartata); le disposizioni sull'istituto delle sostituzioni dei deputati impediti a partecipare ai lavori della rispettiva Commissione; il ricorso ampliato alle sedi redigente e legislativa, difficilmente praticabile visti i contenuti dei d.l. in conversione, l'accordo tra i Gruppi (dunque non vincolante per i singoli parlamentari) di non procedere alla fase di esame degli emendamenti in Assemblea, realizzando, in via di fatto, un effetto in parte analogo a quello proprio della sede redigente, che riserva alla fase di Commissione l'esame delle proposte emendative.

da parte delle forze politiche».
Accordo che può essere facilmente raggiunto per quanto concerne le "attività informali", anche delle Commissioni permanenti[18]. Mentre, per le sedi formali di riunione delle Commissioni, la Presidenza si è pronunciata nel senso che debba rimanere ferma la partecipazione diretta ai lavori, con il massimo accesso possibile anche dei deputati assenti all'informazione sui lavori parlamentari tramite il circuito chiuso o, in via sperimentale e eccezionale tramite la rete Intranet della Camera.

3. Quali sono le questioni sul tappeto. Primo: mantenere le Camere aperte e funzionanti; secondo: capire come, senza contrastare la Costituzione

Tutti i costituzionalisti intervenuti sul tema del mantenimento della funzionalità delle Camere, ad oggi, manifestano (anche negli interventi diretti all'opinione pubblica, comparsi sui media) l'esigenza di ribadire, in questa temperie, la centralità del Parlamento[19]. Si tratta di un bel segnale di compattezza e di un salutare contributo che è intervenuto immediatamente, con le prime evidenze di un rallentamento dell'esercizio sia della funzione legislativa sia di quella di indirizzo e controllo sul Governo.
Nessun dubbio che, «dal punto di vista costituzionale, il Parlamento non chiude mai»[20], «organo costituzionalmente necessario, da garantire senza eccezioni, come da lungo tempo insegna la Corte costituzionale, nella continuità operativa»[21], non può fermarsi o rischiare di fermarsi[22]; affermazioni da ribadire con forza quando si tratta di disciplinare limiti eccezionali ai diritti costituzionalmente garantiti[23]. In gioco sarebbe anche

[18] Ricorda il Presidente che «si svolgono in sede informale quelle attività che, pur riconducibili all'attività istituzionale dell'organo, non sono soggette a resocontazione (salva l'indicazione, negli atti della Camera, dell'orario di svolgimento e salva, per le sole audizioni informali, la trasmissione via webtv) … [sebbene] rilevanti sul piano procedurale e regolamentare, svolte con la presidenza del Presidente, in sede plenaria o di collegi minori, previo invio ai componenti della convocazione ufficiale, oggetto anche di pubblicazione sul sito della Camera e nell'apposito bollettino». In sostanza, si tratta delle riunioni degli Uffici di presidenza, sia in sede di programmazione dei lavori sia in sede di svolgimento di audizioni, modalità quest'ultima ampiamente conosciuta in via di prassi. Da queste vanno tenute distinte le attività non propriamente istituzionali, ma funzionali alla loro organizzazione (come riunioni, contatti per le vie brevi), svolte dai membri della Commissione o da una parte di essi, con o senza la partecipazione di soggetti esterni.

[19] Si vedano, almeno, M. Ainis, *Parlamento, meglio distante che latitante*, cit. e B. Caravita, *L'Italia ai tempi del coronavirus: rileggendo la Costituzione italiana*, in *Federalismi.it*, 6, 2020, editoriale del 18 marzo 2020.

[20] G. Azzariti, *Editoriale. Il diritto costituzionale d'eccezione*, cit, iv, descrive un Parlamento che «in questo momento appare paralizzato, avendo stabilito di sospendere tutte le sedute ordinarie, non riuscendo neppure più a votare in fretta e furia i provvedimenti necessari per far fronte alla pandemia».

[21] M. Villone, *Il parlamento nella spirale di due crisi*, cit.; A. Pertici, *Coronavirus, le Camere dimezzate votano il bilancio*, in *La Stampa*, 11 marzo 2020.

[22] Per A. Malaschini, *Procedure parlamentari e legislazione d'emergenza*, in *Working Paper Series*, LUISS School of Government, marzo 2020, «qualsiasi suggestione di sospensione dell'attività parlamentare non può essere accettata», 1; così anche B. Caravita, *L'Italia ai tempi del coronavirus*, cit., vii.

[23] Così P. Armaroli, *Ma Churchill qui da noi non è di casa. Il parlamento che chiude i battenti è uno spot contro la democrazia rappresentativa*, in *Il Dubbio*, 13 marzo 2020; C. Fusaro, *Le camere nell'emergenza della pandemia*, in *PER, Progresso, Europa, riforme*, 18 marzo 2020; G. Azzariti, *I pieni e solitari poteri del capo del*

la legittimazione delle Assemblee legislative nazionali, in termini di visibilità di fronte all'opinione pubblica e dunque di credibilità e fiducia[24].

Come anche, prosegue l'esercizio delle funzioni del Presidente della Repubblica, della Corte costituzionale[25], del Governo anche se sono variate sensibilmente – e con effetti che sarà importante valutare con attenzione – le relative modalità di rappresentazione

governo extraordinem, in *Il Manifesto*, 19 marzo 2020; L. Mazzarolli, *Riserva di legge» e «principio di legalità» in tempo di emergenza nazionale*, in *Federalismi.it*, 1, 2020, 23 marzo 2020; R. Dickmann, *Alcune questioni di costituzionalità*, cit., 7.

[24] Quest'ultimo è tra gli altri argomenti della contrarietà alle attività a distanza dei parlamentari, con eccezione per lo svolgimento di audizioni in commissione tramite videoconferenze o l'utilizzo di strumenti telematici per sedi informali e non deliberative; come accennato, questa modalità è stata utilizzata da entrambi i rami dl Parlamento, a titolo di esempio, cfr. l'audizione informale, in videoconferenza, del Ministro dell'Economia e delle finanze, Roberto Gualtieri, sulle *recenti misure economiche adottate dal Governo per fronteggiare l'emergenza epidemiologica da Covid-19*, di martedì 24 marzo, svolta presso la Nuova Aula dei Gruppi parlamentari e la Sala Koch, con le Commissioni riunite Bilancio di Camera e Senato. Sul punto, cfr. A. Pertici, *Coronavirus*, cit., quando osserva che «l'attività delle commissioni è importante, ma non può essere sostitutiva e poi l'istituzione deve farsi vedere e sentire, in momenti come questo»; V. Lippolis, *Parlamento a distanza? Meglio di no*, in *Il Dubbio*, 1° aprile 2020, pone quello a sostegno della strada imboccata finora da Camera e Senato, ossia che sia «ragionevole ridurre all'essenziale i lavori, ma dare al Paese l'immagine della loro presenza sia pure con gli accorgimenti che la pandemia impone». Cfr. anche M. Villone, *Camere a eletti contingentati, è incostituzionale*, in *Il Manifesto*, 11 marzo 2020, quando «osserva che quel che accade è uno spot per chi vuole rottamare la democrazia rappresentativa». Così anche R. Calvano, intervento in *Parlamento aperto: a distanza o in presenza? (II appuntamento)*, dibattito su Facebook, 3 aprile 2020, cit. Si vedano anche le osservazioni di M. Bozzaotre, *Alcune considerazioni su voto parlamentare a distanza, corpi del sovrano e metafisica della presenza*, in *Forum di Quaderni costituzionali*, 11 aprile 2020, 39 ss., sulla necessità di mostrare le sembianze fisiche ("corpo") del Parlamento non meno del corpo fisico (di cui salvaguardare l'incolumità) dei parlamentari.

[25] Si vedano le disposizioni della Presidente della Corte costituzionale (assunte «su conforme avviso espresso dal collegio»), del 24 marzo 2020, *Ulteriori misure per garantire la continuità dei giudizi costituzionali durante l'emergenza covid-19* e del 20 aprile 2020, *Ulteriori misure per lo svolgimento dei giudizi davanti alla Corte, anche da remoto, durante l'emergenza epidemiologica covid-19*. In questo secondo documento si legge, in particolare, «1.- Durante il periodo dell'emergenza epidemiologica, fino al 30 giugno 2020 e comunque sino a nuovo provvedimento, i lavori della Corte costituzionale proseguono secondo le seguenti modalità: a) la partecipazione dei giudici alle camere di consiglio e alle udienze pubbliche può avvenire anche mediante collegamenti da remoto e in luogo da cui essi si collegano e considerato camera di consiglio o aula di udienza a tutti gli effetti di legge; b) le modalità di cui alla lettera precedente possono essere adottate per ogni altra riunione della Corte, dei suoi giudici e organi interni, incluse le adunanze per deliberazioni amministrative, nonché quelle dell'Ufficio di presidenza, delle commissioni e dei gruppi di lavoro». Cfr. P. Costanzo, *Con l'emergenza, decolla la Corte 2.0*, in *Consulta online*, 1, 2020, 158 ss., che evidenzia l'attenzione che la Consulta ha mostrato già da prima della emergenza riguardo all'uso dello strumento telematico, ricostruisce e commenta l'attuale regolamentazione, spinta fino ad interessare rilevanti fasi processuali.

Ricorda G. Santini, *Funzionalità delle istituzioni e impedimento dei titolari*, cit., 5: «tra gli organi collegiali, occorre distinguere quelli che possono sospendere, per un certo periodo, la propria attività da quelli cui spettano, comunque, adempimenti urgenti e indifferibili. Tra i primi, si può menzionare la Corte costituzionale, che ha deciso, per il mese di marzo, di sospendere le udienze pubbliche e l'audizione di esperti, «esaminando la possibilità di predisporre nuove modalità di trattazione delle udienze, sfruttando le opportunità offerte dalla tecnologia» (c.s., 9 mar. 2020). Tra i secondi, il Consiglio dei ministri, fortunatamente, può funzionare a ranghi ridotti, in quanto il d.P.C.m. 10 nov. 1993, che ne regola i lavori, prevede, per i componenti, un obbligo di partecipazione, ma fa salvi gli impedimenti motivati e comunque non fissa un numero legale (art. 1.4). Peraltro, le deleghe di eventuali Ministri deceduti o divenuti incapaci potranno essere riassegnate ad interim con decreto del Presidente della Repubblica (art. 9.4 l. 400/88); in caso di impedimento temporaneo, il Consiglio potrebbe, con la loro intesa, invitare a partecipare, senza diritto di voto, eventuali Viceministri (art. 10.4, l. 400); il supplente del Segretario del Consiglio è individuato nel Ministro più giovane (art. 1.3 d.P.C.m. 10 nov. 1993)».

pubblica, con una notevole accentuazione della visibilità dei soli vertici di taluni organi (ovviamente, anche a livello territoriale e locale). Tuttavia, se da una parte è ammissibile e comprensibile una sovraesposizione del Governo – con modalità che permettono di arrivare direttamente all'opinione pubblica e non solo a quella nazionale –, non è auspicabile una sua contestuale sottoesposizione 'in' Parlamento[26]. Non è infatti da trascurare la preoccupazione di coloro che hanno lamentato la riduzione dell'uso del *question time*, strumento che ha appunto il pregio di rendere visibile il legame tra legislativo e l'esecutivo e di farlo 'nelle' sedi della rappresentanza nazionale.

Altra preoccupazione comune dei costituzionalisti è stata quella di ribadire che in Parlamento, al fine di decidere, non solo si vota, ma ci si confronta (anche all'interno di ciascun gruppo e fuori dalle aule delle Assemblee e delle commissioni), dialogando e ricercando soluzioni tra le diverse proposte politiche[27]. Nell'ammonire che il Parlamento non si deve ridurre ad un "votificio", alcuni hanno anche ricordano, quasi già con una punta di nostalgia, il contatto fisico e lo scontro materiale del quale non infrequentemente viene data notizia nei resoconti dei lavori parlamentari[28].

Quando però si è aperto il confronto sul *come* sarebbe e sarà possibile garantire la funzionalità delle Camere, per un tempo che ancora oggi non riusciamo a quantificare, le divergenze sono emerse ed il confronto si è avviato anche sollecitato da personalità politiche e organi di stampa.

Premesse le circostanze di fatto che ho sopra richiamato, il dibattito ha preso avvio dalla questione dell'interpretazione delle disposizioni costituzionali che riguardano il voto dei parlamentari, contenute nell'art. 64, in particolare, nei comma terzo e quarto: «Le deliberazioni di ciascuna Camera e del Parlamento non sono valide se non è presente la maggioranza dei loro componenti, e se non sono adottate a maggioranza dei presenti, salvo che la Costituzione prescriva una maggioranza speciale. I membri del Governo, anche se non fanno parte delle Camere, hanno diritto, e se richiesti obbligo, di assistere alle sedute. Devono essere sentiti ogni volta che lo richiedono». La presenza è dunque il presupposto della validità delle deliberazioni[29].

Come ho già ricordato, lo stesso Presidente della Camera ha richiamato l'attenzione sulla possibilità di interpretare evolutivamente il concetto di presenza contenuto nelle

[26] Non è in questo contributo possibile un approfondimento su quanto sia mutata la comunicazione istituzionale nella fase dell'emergenza, rinvio però a precedenti mie considerazioni sul tema della nozione, delle attività e degli strumenti della pubblicità dell'agire degli organi costituzionali, delle altre istituzioni e degli enti pubblici, cfr. *Poteri e pubblicità. Per una teoria giuridica della comunicazione istituzionale*, Padova, 2002 e *Indirizzo politico, comunicazione, responsabilità giuridica. Il programma di governo alla prova dell'opinione pubblica,* in P. Marsocci (a cura di), "*Esporre" la democrazia. Profili giuridici della comunicazione del Governo*, collana Diritto e società, Roma, 2007. Sul tema, recenti ed interessanti i lavori di A. I. Arena, *L'esternazione del pubblico potere*, Napoli, 2019 e D. Chinni, *Potere e opinione pubblica. Gli organi costituzionali dinanzi alle sfide del web*, Napoli, 2019.

[27] M. Villone, *La rappresentanza non si pratica a distanza*, in *Il Manifesto*, 31 marzo 2020. N. Lupo, *Perché non è l'art. 64 Cost. a impedire il voto "a distanza" dei parlamentari. E perché ammettere tale voto richiede una "re-ingegnerizzazione" dei procedimenti parlamentari*, in *Osservatorio costituzionale,* 3, 2020, 31 marzo 2020, 8.

[28] C. Sbailò, *Parlamento on line? Garantiamo la possibilità di violare il regolamento*, in *Formiche.net*, 31 marzo 2020.

[29] Su voto deliberativo e specificità del deliberato, «come forma ineludibile di formazione e di rilevazione della volontà degli organi costituzionali a struttura collegiale», cfr. G. Ferrara, *Gli atti costituzionali*, Torino, 2000, 43 ss.

disposizioni dell'art. 64 Cost., intendendolo non solo come vicinanza fisica delle persone[30]. Se si intraprendesse questa strada, si aprirebbe un ventaglio di opportunità riferite alle funzioni parlamentari nel loro complesso che, tuttavia, se ritenute ammissibili per logica varrebbero per il presente come per il futuro[31]. Inoltre, in astratto, potrebbero valere non solo per analoghe circostanze eccezionali riferite ad un numero consistente di parlamentari assenti per cause di necessità. Tutto ciò, a meno che non si decida espressamente (con puntuali modifiche regolamentari) in questo specifico senso.

Anticipando in sintesi le mie personali considerazioni, credo che questa ultima sia la strada da percorre.

Perché, è il concetto di *presenza* che deve essere indagato, per riflettere, come ci insegna Gianni Ferrara, «sul primo degli atti che viene a compiersi spontaneamente appena emerge un dato dell'esperienza giuridica, quello di nominarlo. E il nome della cosa è la cosa, la descrive, la identifica, ne scopre l'essenza […] Sono *topoi* da rivisitare per scoprire poi le modulazioni, le impronte, le conversioni che le varie fasi del processo storico hanno impresso agli istituti giuridici per consegnarceli nella forma che ne definiscono la contemporaneità»[32].

Dunque, è possibile chiedersi da un lato cosa significhi presenza del parlamentare, dall'altro come *oggi* debba essere intesa, nella interpretazione costituzionale.

Ferrara si riferisce prima al termine rappresentanza «il nome della rappresentanza è quanto mai rivelatore della essenza della rappresentanza» – per poi esaltarne il nesso con il termine presenza, «far sì che sia presente in qualche sede quel che presente non vi è, e non può esservi o non si vuole che vi sia o non deve». Aggiunge però ciò che sarà reso presente nella rappresentanza politica (diversamente in quella civilistica) è «un'entità non singola. Potrà, di certo, questa cosa essere anche un'entità composta da persone, ma, appunto, alla condizione che sia multipla questa entità, che si tratti cioè di una pluralità di persone». Deve essere una entità plurale a rappresentare un'altra entità

[30] N. Lupo, *Intervento* nel confronto in diretta Facebook, cit., nel sostenere che l'art. 64 terzo comma non costituisce un ostacolo al voto in differita, non ricorre alla interpretazione evolutiva, ma richiama la consolidata interpretazione del Parlamento stesso, che può tornare utile per il presente, come dimostrano l'esempio della richiesta di numero legale e alcune altre prassi sempre relative alla presenza (di veda la sent. 379/1996 della Corte costituzionale). Analogamente, anche se per arrivare alla soluzione opposta di non ritenere preferibile il "televoto" dei parlamentari, S. Silvestri, *Covid-19 e Costituzione,* cit., «non tanto per una interpretazione letterale delle parole 'presente' o 'presenti' contenute nell'art. 64 Cost., quanto piuttosto perché appare problematico poter garantire nella votazione da remoto la sussistenza delle condizioni della sua genuinità ai sensi dell'art. 48 Cost.; il che vale per tutte le forme di "democrazia digitale", che prescindono dalle condizioni ambientali in cui si trova chi esprime la sua volontà democratica». Ad auspicare esplicitamente un'interpretazione evolutiva sono stati S. Curreri, M. Ainis e L. Trucco; a respingerla M. Luciani, tutti in *Interventi* nel confronto in diretta Facebook, cit. Così, favorevole, B. Caravita, *L'Italia ai tempi del coronavirus,* cit., viii; contrario A. Malaschini, *Procedure parlamentari,* cit., 1, che ricorda come né i costituenti né gli estensori dei Regolamenti presero in considerazione ipotesi di voto espresso attraverso una comunicazione cartacea, lettera o telegramma, oppure telefonica, integrando così le possibilità di esprimerlo in presenza fisica, pur essendo disponibili tali strumenti.

[31] R. Dickmann, *Alcune questioni di costituzionalità*, cit., 6, «non pare legittima ai fini dello svolgimento delle funzioni costituzionali delle Camere una mera evoluzione 'materiale' dei regolamenti parlamentari, che sarebbe *contra Constitutionem*, e tanto meno sembrano legittime soluzioni interpretative transitorie di tali regolamenti elusive dei citati vincoli costituzionali».

[32] G. Ferrara, *Democrazia e rappresentanza politica*, in *Costituzionalismo.it*, 1, 2005.

altrettanto plurale, per essere strutturalmente credibile e funzionalmente efficace, in entrambi i casi non una mera sommatoria di individui, ma un gruppo disomogeneo quanto a idee, culture ecc., anche configgenti tra loro. Inoltre, «solo questa grande entità plurale potrebbe essere considerata capace di essere rappresentata, sia perché lo sarebbe direttamente, sia, soprattutto, perché eleggerebbe una proiezione adeguatamente plurima di se stessa»[33].

Da queste riflessioni, è possibile trarre la conseguenza, per analogia, che sia possibile ammettere l'assenza di uno o più componenti del gruppo dei rappresentanti, pur mantenendo la validità della presenza di quella che è appunto una entità plurale, ossia ciascuna delle Assemblee? Ovviamente si, ed è quanto prevede e disciplina il terzo comma dell'art. 64.

Qualora invece le eventuali assenze, a causa di impedimenti extra-ordinari, non potessero più essere computate in modo da consentire i lavori parlamentari, arrivando a metterli a rischio in modo prolungato e ripetuto, sarebbe possibile considerare le presenze da remoto? Con quali differenze circa l'espressione del voto al fine di deliberare e, invece, l'espletamento delle altre funzioni parlamentari?

Per queste ultime, sembra sussistere un sostanziale accordo da parte della dottrina, anzi per alcuni permettere la presenza da remoto potrebbe essere un'opportunità aggiuntiva offerta dall'uso delle tecnologie digitali, da cogliere anche a conclusione della fase di emergenza. In particolare, ciò sarebbe possibile per le procedure o le sedi informali, in cui non si deve deliberare (ad esempio le audizioni)[34], così come, a parere di alcuni, anche il confronto in Commissione potrebbe essere consentito in videoconferenza, visti il numero più ristretto di membri[35].

Riguardo alle modalità con cui l'organo collegiale assume le proprie decisioni, netta è invece la divisione tra chi ritiene che «non mancano precedenti né pronunce giurisprudenziali che consentono di interpretare la disposizione costituzionale in modi compatibili con l'attivazione, in tempi senz'altro eccezionali quali quelli che stiamo vivendo, di forme di attività e di deliberazione parlamentare anche "a distanza"»[36] e chi esclude tale possibilità, perché se anche «è probabile che il voto a distanza sia in concreto praticabile con le moderne tecnologie, è dubbia la piena conformità alla Costituzione e ai regolamenti»[37].

---

[33] Corsivo mio, ad evidenziare quanto le circostanze e le posizioni politiche odierne potranno avere un impatto sul dibattito in occasione del futuro voto referendario sulla riduzione del numero dei parlamentari, al quale si accennerà oltre.

[34] Tra marzo e aprile 2020, si sono svolte in videoconferenza molte delle audizioni. Sul punto, cfr. gli interventi di R. Calvano, V. Lippolis, N. Lupo e L. Trucco, nel confronto in diretta Facebook organizzata dal Presidente della Commissione affari costituzionali della Camera, on. Brescia, su *Parlamento aperto: a distanza o in presenza? (II appuntamento)*, del 3 aprile 2020, disponibile in *radioradicale.it*.

[35] S. Ceccanti, *Intervento* in diretta Facebook, cit.

[36] N. Lupo, *La rappresentanza,* cit., 2. Nello stesso senso, B. Caravita, *L'Italia ai tempi del coronavirus*, cit., viii, laddove, specifica, «che al di là di ogni ragionevole dubbio – (sia garantita) sia la possibilità di esercitare con pienezza la funzione rappresentativa, sia la libertà e, ove prevista, la segretezza del voto». Favorevole anche E. Catelani, *La tecnologia può aiutare a far funzionare il Parlamento e i prefetti ascoltino le Regioni*, in *Il Dubbio*, 26 marzo 2020.

[37] M. Villone, *La rappresentanza non si pratica a distanza*, cit. Analogamente, A. Malaschini, *Procedure parlamentari,* cit., spec. 5. In ogni caso, a parere di G. Azzariti, *Editoriale. Il diritto costituzionale d'eccezione*,

In particolare, considerato che, per dottrina consolidata, risultano assolutamente possibili le riunioni dell'Assemblea, con qualunque numero di presenti, in quanto le presenze necessarie a verificare il quorum strutturale e il quorum funzionale saranno determinanti – e dunque sono richieste – solo al momento dell'adozione di deliberazioni (di qualunque tipo)[38], in questa direzione, chi si schiera a favore ricorda anche il principio della presunzione del numero legale «che, da un lato, conferma gli ampi margini a disposizione dei regolamenti parlamentari nell'attuare la prescrizione costituzionale e, dall'altro, mostra quanti spazi vi siano oggi, pure a norme invariate, per lavorare anche con numeri assai esigui in Assemblea, e a maggior ragione nelle commissioni (a patto che vi sia una seppur minima concordia tra le forze politiche nel non fare ricorso a strumenti, come la richiesta di verifica del numero legale o di ricorso a votazioni qualificate)»[39].

Gli argomenti di chi si schiera contro, in sintesi, hanno come principiale riferimento la necessità di coniugare la praticabilità della presenza in remoto con la piena garanzia delle prerogative parlamentari disciplinate dalla Costituzione. Innanzitutto quelle che spettano a ciascun rappresentante: l'espressione della propria opinione, il diritto di proposta e quello di voto, tutelato quest'ultimo quanto a personalità, uguaglianza, libertà e (in caso sia prevista) segretezza. I dubbi più forti riguardano la effettiva possibilità di esprimersi e confrontarsi da remoto e il rischio che non sia affatto facile accertare la personalità e fugare ogni dubbio sulla regolarità del voto segreto, tanto da aumentare i contenziosi davanti alla Corte costituzionale, per conflitto di attribuzione tra poteri dello Stato (ordinanza n. 17/2019)[40].

4. (*segue*) Terzo: decidere (come?) con quali modalità procedurali e strumenti. Quarto: valutare se ciò valga solo nella contingenza presente o anche per il futuro

A chi spetta disciplinare le modalità di espressione del voto, eventualmente da remoto? Con quale strumento normativo?

Come ricordato in precedenza, la Carta contiene pochi riferimenti, lasciando spazio

cit., iv, si tratterebbe «di una deroga legittimata dallo stato di necessità, non certo una regola da introdurre per migliorare l'efficienza dei lavori del Parlamento».

[38] A questo argomento viene collegato quello del computo delle astensioni, in quanto rilevanti ai fini del calcolo del quorum funzionale, anche in riferimento alla lettura della sentenza della Corte costituzionale n. 78/1984, «che appunto ha la sua *ratio* nella valorizzazione dell'autonomia regolamentare delle Camere nell'interpretare e applicare quella disposizione costituzionale, fino al punto di attribuire significati diversi alla parola "presente" e a quella "presenti", nell'ambito del medesimo periodo», secondo N. Lupo, *La rappresentanza,* cit., 6, mentre per V. Lippolis, *intervento,* cit., la Corte nel dare ai regolamenti parlamentari la discrezionalità nell'attuare la Costituzione in tema di astensioni, si era riferita al computo della maggioranza non a quella della discussione o del voto, cioè alla maggioranza e non ai presenti.

[39] N. Lupo, ivi, 7.

[40] In verità, tale argomento è sollevato sia dai contrari (A. Malaschini*, Procedure parlamentari,* cit., 4), sia dai favorevoli (S. Curreri, *L'attività parlamentare ai tempi del Covid-19*, cit.), al voto a distanza. Cfr. anche M. Bozzaotre, *Alcune considerazioni su voto parlamentare a distanza,* cit., 36 ss.

ampio all'esercizio dell'autonomia costituzionalmente attribuita alle Camere[41]. In caso si dovesse procedere fino a spingersi nel consentire il voto da remoto per i parlamentari assenti, l'opinione prevalente non giudica idonea una mera decisione delle Giunte per il regolamento ed indica – come unica strada percorribile – la modifica dei regolamenti parlamentari, da approvarsi a maggioranza assoluta e con il voto favorevole in Aula della metà più uno dei componenti[42]. Chi avanza queste tesi, insomma, pone pragmaticamente il problema della attuazione delle modifiche proposte e si basa sulla constatazione che bisogna fare i conti con la scarsità del fattore tempo. Accanto alla provvisorietà delle misure da adottare, in questa situazione dovrebbe essere questo l'unico punto fermo[43].

Altri prospettano la soluzione di deroghe puntuali e temporanee ai Regolamenti parlamentari, unanimemente condivise nell'ufficio di presidenza e in conferenza dei capigruppo[44] ed è questa parte della dottrina che, difatti, pone l'accento su quanto le soluzioni adottate in risposta alla situazione di fatto potrebbero influenzare la vita e il funzionamento del Parlamento, oltre lo stato di necessità attuale. Altri ancora chiedono modifiche dei Regolamenti che prevedano specifiche semplificate procedure – che, seppure temporanee, aprano a interpretazioni che appaiono in verità troppo vicine al limite della "rottura" costituzionale – in presenza di comprovate situazioni di emergenza, come quella attuale[45].

---

41 Lo ribadisce, A. Malaschini, ivi, 2.

42 Cfr. B. Caravita, *L'Italia ai tempi del coronavirus,* cit., viii; A. Malaschini, *Procedure parlamentari,* cit., 3; V. Lippolis, *Intervento* in diretta Facebook, cit. S. Ceccanti, *Intervento* in diretta Facebook, cit., la ritiene solo una delle possibili soluzioni. Mentre, proprio al fine di evitare la tentazione di ricorrere al voto da remoto, G. Silvestri, *Covid-19 e Costituzione,* cit., immagina, nel caso della conversione in legge dei decreti, una modifica dei regolamenti perché sia prevista «l'ipotesi di una decisione all'unanimità della Conferenza dei capigruppo, che autorizzi la scelta del procedimento decentrato, le cui modalità non solo renderebbero più agili e veloci i lavori, ma consentirebbero pure l'adozione di tutte le cautele (numero dei presenti, distanze, scelta dei locali più adatti etc.) necessarie per l'incolumità dei partecipanti ed il contenimento del contagio. Maggioranza e opposizione sarebbero comunque garantite, giacché sarebbe sempre possibile la transizione al procedimento ordinario, su richiesta del Governo, di un quinto dei membri della commissione competente e di un decimo dell'assemblea».

43 Anche chi è più possibilista sulla compatibilità costituzionale del voto da remoto, pone però gli stessi fattori come condizione di realizzabilità, cfr. B. Caravita, *L'Italia ai tempi del coronavirus,* cit., viii, «in primo luogo, è necessaria una adeguata strumentazione e una sufficiente fase di sperimentazione».

44 G. Azzariti, *Editoriale. Il diritto costituzionale d'eccezione,* cit., iii ss., e S. Prisco - F. Abbondante, *I diritti al tempo del coronavirus. Un dialogo*, in *Federalismi.it*, 24 marzo 2020, 7; N. Lupo, *La rappresentanza,* cit., 10. Anche se con il diverso intento di auspicare il voto da remoto, anche S. Curreri, *Intervento* in diretta Facebook, cit., stigmatizza la soluzione compromissoria di lavorare a ranghi ridotti, autoriducendo la rappresentanza, in quanto altera l'equilibrio tra maggioranza e opposizione, verticalizza il dibattito parlamentare e non può essere imposta ai singoli parlamentari, che sempre potrebbero rivendicarlo, sollevando conflitto di attribuzione alla Corte.

45 S. Ceccanti, *Verso una regolamentazione degli stati di emergenza per il parlamento: proposte a regime e possibili anticipazioni immediate*, in *BioDiritto*, 2, 2020, 2 ss., auspica che per i soli parlamentari che non possono essere presenti, sia consentito oggi il voto a distanza o la presenza in videoconferenza e propone una disciplina che tenga conto di una graduazione della gravità dello stato di emergenza e permetta nel caso peggiore l'istituzione di «una Commissione bicamerale unica con poteri legislativi composta ovviamente in modo proporzionale con la presenza di tutti i gruppi, senza componenti del Governo, composte in tutto da alcune decine di parlamentari (diciamo da trenta a cinquanta)», da far lavorare in videoconferenza, su un elenco di materie, conforme alle garanzie costituzionali, e nel caso meno grave con «compiti redigenti, riservando il voto sugli articoli e il voto finale all'Aula. Anche in quel caso andrebbe consentito

Trasversalmente rispetto a questi diversi orientamenti, si sollecita infine a fare quello che si può, utilizzando (dichiaratamente) in modo non convenzionale le risorse già disponibili e adattando le procedure regolamentari, fino al limite della loro massima interpretazione in deroga, piuttosto che rischiare di implementare nuove prassi o introdurre nuovi istituti non pienamente sostenibili nella prospettiva delle garanzie costituzionali[46]. Si propone, con questo spirito, così: di ridurre di una percentuale fissa la presenza di ciascun parlamentare e, nel rapporto maggioranza e opposizione, di semplificare riducendo pro quota i membri delle commissioni[47]; di estendere l'applicazione delle procedure per le «autorizzazioni a procedere *ex* articolo 96 Cost., la possibilità per i parlamentari di esprimere il voto per tutta l'intera giornata, evitando quindi il lamentato rischio di affollamento (art. 135-*bis*, c. 8-*bis*, del Regolamento del Senato)»[48]; di usare il procedimento decentrato deliberante, e derogare con l'accordo di tutti i gruppi alla riserva di assemblea nei regolamenti parlamentari, rinviando all'aula per le sole dichiarazioni di voto con un sistema bilanciato misto[49]; di riunirsi usando le Aule con modalità particolari, a prescindere dalla appartenenza ad esse dei parlamentari[50].
In effetti, quella di adottare particolari modalità logistiche e di lavoro è stata, ad oggi, anche la scelta compiuta da Camera e Senato, attraverso la scelta della riduzione dei giorni di convocazione dei lavori; della autoriduzione dei parlamentari; del contingentamento degli emendamenti; del voto unico, quello finale[51].
A meno di non voler cedere alla tentazione di dover concludere che quello che ne viene fuori sia una sorta di rompicapo – considerato che si tratta di soluzioni che molta parte della dottrina aveva criticato – a me sembra sia utile innanzitutto prendere atto invece che le Camere (nel momento attuale di questa loro esperienza): non hanno tentato la

l'esame in videoconferenza in Commissione e potrebbe essere introdotto il voto a distanza per l'Aula anche con possibilità di delega, con modalità tali da evitare la concentrazione eccessiva di potere. In altri termini un'unica possibilità di delega da un parlamentare ad un altro parlamentare, non al capogruppo», Anche in questo caso dovrebbero valere i limiti di materia descritti in precedenza. In senso analogo, F. Clementi, *Il Parlamento deve poter funzionare sempre, ancor più dopo l'emergenza*, in *Il Sole 24 Ore*, 17 marzo 2020, per il quale «si tratterebbe di costituire una o due commissioni speciali, istituto già previsto per la trattazione di temi plurisettoriali. E di consentire i voti delle assemblee a distanza, sugli articoli e sul testo nel suo insieme. Non stupirà nessuno che si tratti di soluzioni al giorno d'oggi non rigettabili, alle semplici condizioni che si rispetti la relazione tra maggioranza ed opposizione e i rapporti all'interno di entrambe, almeno tendenzialmente».

[46] Ciò è compatibile con l'ordinamento a parere di R. Dickmann, *Alcune questioni di costituzionalità,* cit., 7, stante «il carattere "duttile" dei regolamenti parlamentari ne favorisce l'evoluzione e l'adattamento alle circostanze, per agevolare il dibattito politico e le decisioni degli organi parlamentari, purché nel presupposto che ogni sperimentazione si svolga nell'interesse del Parlamento e nella direzione tracciata dalla Costituzione».

[47] L. Violante, *Intervento* in diretta Facebook, cit.

[48] A. Malaschini, *Procedure parlamentari,* cit., 3.

[49] Sia M. Ainis, sia S. Curreri, *Intervento* in diretta Facebook, cit.; seguendo questa ipotesi, resterebbero però dubbi su come garantire a pieno il principio della pubblicità dei lavori parlamentari.

[50] Così, S. Curreri e M. Luciani, *Intervento*, cit.

[51] Cfr. il calendario dei lavori della Camera dei deputati comunicato all'assemblea il 25 marzo 2020 (resoc. sten., 62 ss.) e l'organizzazione dei lavori del Senato comunicata all'assemblea il 26 marzo 2020 (resoc. sten., 43 ss.). Sarebbe opportuno, ma non nello spazio di questo contributo, ragionare su come tale circostanza potrà influenzare il dibattito sul (posticipato) voto referendario per la modifica costituzionale del numero dei parlamentari.

strada – a Regolamenti invariati – del voto da remoto; hanno ampliato al massimo la possibilità di ricorso alle tecnologie digitali per le attività formali e informali e 'non' per le deliberazioni; si sono auto-organizzate in presenza di condizioni critiche, autolimitandosi con scelte al (ma entro il) limite della sostenibilità costituzionale. Tutto questo senza mettere *del tutto* in gioco una interpretazione evolutiva del concetto di presenza ex art. 64 Cost.
Se tali soluzioni sono, e forse saranno, sufficienti a tamponare la situazione, mi chiedo però quale sia l'utilità *pro futuro* di queste scelte.
Credo, invece, debba essere colta oggi l'opportunità almeno di riflettere su quale si possa scegliere che sia lo spazio delle tecnologie digitali nello svolgimento delle funzioni proprie degli organi costituzionali e, ovviamente, primo tra tutti del Parlamento. Per farlo, occorre "scomodare" l'interpretazione evolutiva del testo della Carta.

5. La riunione e le altre libertà praticate tramite le tecnologie digitali

Non credo sia oggi più il tempo di avere incertezze sulla qualificazione delle tecnologie digitali come "spazio" a disposizione di ogni libertà costituzionalmente tutelata, così come è possibile osservare che le autorità pubbliche possono avvalersi di questi stessi strumenti per le legittime misure a limitazione del loro esercizio, così come – certamente – se ne possono servire coloro che violino i diritti altrui.
Ha ribadito recentemente il Presidente Mattarella, proprio con riferimento alla pervasività sin qui sconosciuta che sta assumendo l'egemonia di pochi colossi dell'impresa digitale:
«Gli strumenti per guidare in modo positivo l'evoluzione digitale, a servizio delle persone, consistono nell'applicazione puntuale dei principi sui quali si basa l'esperienza liberal-democratica, costruita a caro prezzo da tanti popoli. Non esistono 'non luoghi': si tratta comunque di spazi, sia pure virtuali, in cui interagiscono persone e si registrano attività umane; e anche la dimensione digitale deve rispettare principi e regole frutto delle conquiste democratiche. I principi sono sempre quelli contenuti ed espressi nella Carte costituzionali delle democrazie»[52].
L'evoluzione delle potenzialità della Rete verso un spiccato livello di interazione tra utente e suo 'ambiente' di vita – di cui il Web 2.0, i *social networks* ed ora il cd. Internet delle cose sono i portati più significativi –, come tra i primi ci ha insegnato Stefano Rodotà[53], continua progressivamente a ridisegnare sia lo spazio pubblico sia lo spazio privato, marcando quella che per molti è una discontinuità radicale con il passato per altri è una opportunità per reinterpretare istituti giuridici che, proprio di fronte alla

[52] Intervento del Presidente della Repubblica, in occasione dell'incontro con i componenti dell'Associazione Stampa Parlamentare, i Direttori dei quotidiani e delle agenzie giornalistiche e i giornalisti accreditati presso il Quirinale per la consegna del "Ventaglio" da parte dell'Associazione Stampa Parlamentare, Palazzo del Quirinale, 25 luglio 2019, disponibile sul portale *Quirinale.it*.

[53] In molti contributi, cfr. in particolare, *Il mondo della Rete, quali diritti, quali vincoli*, Roma-Bari, 2014, spec. 13 ss.

prova di questa *realtà*[54], dimostrano la loro insostituibilità concettuale.
In particolare, proprio nella odierna situazione di emergenza, la questione della qualificazione del diritto di accesso alla infrastruttura digitale della Rete, come diritto sociale di cui il bilancio pubblico si deve fare carico, torna prepotentemente in evidenza[55]. Si tratta del nodo inclusione/esclusione – ossia, quello legato alla cd. cittadinanza digitale –, da considerare non come scelta individuale, ma come precondizione di pieno inserimento nella comunità statuale, con effetti questi in parte sì inusitati, quanto a forza e pervasività, che prendono le mosse dal processo di dematerializzazione delle merci, della loro produzione e del loro consumo.
Nessun ordinamento giuridico può permettersi di "subire" tali processi, senza l'ambizione di indirizzarli, prescriverne modalità e limiti, organizzare il sistema dei controlli e delle garanzie.
Considerati gli obiettivi di questo contributo, viene innanzitutto in evidenza la questione della struttura della libertà di riunione, con riferimento specifico alla idoneità degli strumenti messi a diposizione dell'esercizio delle relative facoltà[56].
L'art. 17 della Carta garantisce il diritto dei singoli a stare (interagendo volontariamente) insieme ad altri, in uno stesso luogo, per un certo tempo e con finalità relative alle molteplici necessità di vita; assicura anche, in tal modo la protezione costituzionale "della riunione", in sé, ossia «l'esercizio collettivo di un diritto individuale»[57].
È noto che, ancora oggi, la dottrina a questi requisiti aggiunge quella della fisicità della compresenza, benché non ne sia fatta menzione nella disposizione costituzionale, spesso ed opportunamente sottolineando che la locuzione riferita ai limiti, «pacificamente e senz'armi», non avrebbe senso con una diversa interpretazione[58].
A livello internazionale, esistono però provvedimenti in cui si fa riferimento all'uso del

[54] La Rete internet è una infrastruttura materiale ed a fruirne sono le persone, che certo non ne percorrono le "strade" con i propri corpi, ma che impegnano comunque molto concretamente i propri sensi. Ad essere virtuale (ossia ad esistere solo in potenza) è piuttosto la definizione, virtuale appunto, che ci si ostina a dare al Cyberspazio.

[55] Tesi sostenuta da tempo da molti studiosi, cfr. in particolare G. De Minico, *Diritti Regole Internet*, in *Costituzionalismo.it*, 2, 2011, spec. 2 ss.; P. Marsocci, *Lo spazio di Internet nel costituzionalismo*, in *Costituzionalismo.it*, 2, 2011, spec. 5; A. Valastro, *Internet e strumenti partecipativi nel rapporto tra privati e amministrazioni*, in M. Nisticò - P. Passaglia (a cura di), *Internet e Costituzione*, Torino, 2014; M. Pietrangelo, *Accesso ad Internet, diritto ancora diseguale? Aggiornamenti e ripensamenti*, in M. R. Allegri - G. d'Ippolito, *Accesso ad Internet e neutralità della Rete fra principi costituzionali e regole europee*, Roma, 2017, 25 ss. Ora, con riferimento all'emergenza pandemia, A. Valastro, *Internet e social media prima e dopo il coronavirus: fraintendimenti e deviazioni che tradiscono la democrazia sociale*, *Liber amico rum per Pasquale Costanzo*, in *Consulta online*, 30 aprile 2020, spec. 4 ss. Non è mancata l'attenzione alle parole scandite dal Presidente del Consiglio Conte nella conferenze stampa del 6 aprile 2020: «Internet dovrebbe essere un diritto costituzionale, garantito a tutti, nessuno escluso», cfr. il commento di G. Scorza, *Internet diritto fondamentale, meglio tardi che mai!*, in *Il Fatto quotidiano*, 7 aprile 2020.

[56] Riprendo le note categorizzazioni sulla diversità strutturale dei diritti di libertà e sulla conseguente diversità dei possibili modi di tutela, di A. Pace, *Problematica delle libertà fondamentali,* cit., 25 ss.

[57] P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 41.

[58] Per tutti, R. Borrello, voce *Riunione (Diritto di)*, in *Enc, dir.,* vo. XI, Roma, 1989, 1401; A. Pace, *Problematica delle libertà fondamentali*, Parte speciale, Padova, 1992, 299, che indica come «oggetto della tutela dell'art. 17 il diritto di ciascuno di stare fisicamente insieme». E, anche in tempi di utilizzo già pienamente consolidato del *Web*, M. Ruotolo, *La libertà di riunione e di associazione*, in R. Nania - P. Ridola (a cura di), *I diritti costituzionali*, II, seconda ed. riveduta ed ampliata, Torino, 2006, 683. M. Betzu, *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in *Rivista AIC*, 4, 2012, 4 ss.

Web come idoneo all'esercizio della libertà di riunione[59]. Il Consiglio per i diritti umani delle Nazioni Unite, prendendo posizione sulla necessità che occorra estendere le tradizionali garanzie dei diritti anche quando vengono esercitati tramite le tecnologie digitali (risoluzione del 5 luglio 2012), in una risoluzione del 2013, sottolinea l'obbligo che grava sugli Stati membri «di rispettare e tutelare pienamente i diritti di tutti gli individui di riunirsi pacificamente e di associarsi liberamente, sia online che offline» (A/HRC/RES/24/5, 8 ottobre 2013) Così anche il Comitato dei Ministri del Consiglio d'Europa si è espresso nella Raccomandazione diretta agli Stati membri ed avente ad oggetto "Guida dei diritti umani su internet" (CM/Rec(2014)6)[60], dedicando una parte specifica alle situazioni giuridiche connesse a "Riunione, associazione e partecipazione"[61].
È vero che in questi documenti non sono chiariti i termini della assimilazione tra luogo territoriale e luogo digitale e dunque tra compresenza fisico-corporea e compresenza da remoto, ma – come è già da tempo stato notato –, i servizi fruibili tramite la Rete, si associano e favoriscono comunque le tradizionali modalità di riunione[62].
E' poi il caso di ricordare che proprio la contingenza presente ha ampliato numericamente e reso, in alcuni casi, necessarie forme di presenza aggregata in Rete per lo svolgimento di attività, legate non solo al lavoro, pubbliche e private. L'esercizio del diritto ad essere compresenti in uno stesso periodo temporale consentita dalle tecnologie digitali, unitamente alla possibilità di entrare in comunicazione, consente e diviene prerequisito per lo svolgimento di tali attività. Con questa osservazione non si vogliono trascurare o sottovalutare i numerosi problemi legati, in primo luogo, alla equiparazione delle riunioni da remoto in termini di "efficacia" quanto agli obiettivi da perseguire attraverso l'aggregazione di persone, che in alcuni casi non è assoluta. Soprattutto non si intende sminuire o svilire il valore della compresenza fisica, nell'interpretazione costituzionale dei diritti.
Si può fare, per tutti, l'esempio alla didattica *on line*, svolta ad ogni livello, o anche, in questo stesso ambito, alle riunioni telematiche che permettano le deliberazioni degli organi collegiali di rappresentanza negli istituti scolastici e negli Atenei, circostanze che presuppongono e "richiedono" lo scambio ed il confronto tra le opinioni, che solo in parte si riesce a sviluppare in videoconferenza. Si tratta di esperienze di aggregazione, comunque particolari[63], che si può (e non solo per necessità assoluta) utilizzare affiancandole a quelle proprie ed ineliminabili in presenza fisica (si pensi alle riunioni

[59] Cfr., anche per la giurisprudenza richiamata, in particolare Cass. pen., sez. I, 12 settembre 2014, n. 375961, che ha definito Facebook un "luogo aperto al pubblico", M. Mezzanotte, *Facebook come "luogo aperto al pubblico"*, in *Federalismi.it*, 2, 2016, spec. 11.

[60] Adottata dal Comitato dei Ministri il 16 aprile 2014, in occasione della 1197ª riunione dei Delegati dei Ministri.

[61] «Avete il diritto di riunirvi e di associarvi con altri in modo pacifico utilizzando Internet. In pratica, significa che: 1. siete liberi di scegliere qualsiasi sito Internet, qualsiasi applicazione o altro servizio per costituire, aderire, mobilitarvi o partecipare a un gruppo sociale, o un'associazione, che siano o meno ufficialmente riconosciuti dalle autorità pubbliche».

[62] Così in riferimento alla necessità di tenere in conto le peculiarità dei nuovi strumenti tecnologico al servizio dei diritti, M. Pedrazza Gorlero, *La libertà di stampa nella postmodernità*, in Aa.Vv., *Studi in onore di Leopoldo Elia*, vol. II, Milano, 1999, 1197 e 1215 s.; Ritiene estensibile la tutela costituzionale alle riunioni in Rete, A. Pirozzoli, *La libertà di riunione in Internet*, in *Dir. Inf.*, 4-5, 2004, 595 ss., spec. 623.

[63] In questa direzione, ovviamente esiste l'esempio delle università telematiche.

telematiche consentite solo in alcune fasi delle procedure concorsuali pubbliche).
A queste vanno poi aggiunte le questioni legate al pieno rispetto della "legalità": sempre usando l'esempio del mondo della formazione, la garanzia della presenza costante e controllabile dei soggetti coinvolti, durante il tempo della riunione (a volte ostacolata da meri motivi tecnici); la necessità di un diverso contingentamento della durata degli incontri e dei singoli interventi (anche a tutela dall'uso prolungato della stessa tecnologia digitale); le garanzie connesse alla libera – dalla ingerenza di estranei alla riunione – espressione delle opinioni e dei voti ecc.
Differenti in definitiva possono essere gli "effetti" dell'esercizio delle facoltà connesse alla riunione da remoto, effetti che è pur sempre possibile ritenere non conformi sia in termini di soddisfazione delle esigenze di chi vi partecipa, sia in termini di tutela delle posizioni giuridiche coinvolte.
D'altronde, il luogo pubblico, aperto al pubblico o privato dove una riunione si svolge è sempre – offline o online – uno spazio organizzato, in questo senso utile o non utile allo scopo. Ne consegue, a mio avviso, un'altra domanda importante a cui dare una risposta: a chi appartiene e, dunque, chi ha il potere di architettare e gestire lo specifico servizio messo a disposizione della tecnologia digitale, che diviene lo spazio di esercizio della riunione?

6. Perché è (ormai) indispensabile che si scelga, distinguendo, quali sono le tecnologie digitali idonee all'esercizio della funzione parlamentare

Tenterò di fare qualche ipotesi tornando all'oggetto specifico del contributo. Nel caso dai parlamentari l'esercizio della libertà di riunione – in quei luoghi aperti al pubblico che sono le aule, le commissioni e le altre sale o spazi interni ai Palazzi della rappresentanza – è precondizione essenziale per lo svolgimento delle funzioni loro attribuite e, dunque, per l'esercizio dei diritti di libera espressione del proprio e altrui pensiero, nel confronto politico (cronaca, critica, pluralismo delle idee); di comunicazione riservata interpersonale; di associazione (organizzazione e funzionamento dei gruppi); di proposta e di voto.
Il Parlamento da anni ha intrapreso un processo di digitalizzazione e dematerializzazione. Prendendo ad esempio l'esperienza della Camera dei Deputati, nell'ultima Relazione disponibile sullo stato della Amministrazione (2017) si legge che l'impatto della tecnologia digitale si è sviluppato sia per i processi di lavoro gestiti dell'Amministrazione, «in questa direzione ha svolto un determinante ruolo propulsivo il Portale intranet, inteso quale punto di accesso unificato alla documentazione amministrativa sia di carattere personale, sia di interesse generale, nonché quale punto di accesso alle applicazioni e ai servizi necessari per lo svolgimento delle attività d'ufficio, sia per le modalità di esercizio delle prerogative parlamentari, finalizzata ad agevolarne lo svolgimento e a conseguire, allo stesso tempo, un'ottimizzazione delle attività strumentali di competenza degli uffici [...] in coerenza con il consolidato indirizzo definito in tal

senso dagli organi di direzione politica»[64].

Dunque, negli anni sono stati implementati servizi digitali non solo per migliorare la conoscibilità dell'attività parlamentare, rendendo disponibili testi e dati ufficiali custoditi in formati aperti e scaricabili da chiunque all'esterno (presupposto della attività di comunicazione istituzionale) e implementando e promuovendo progressivamente la interazione diretta e attiva con i cittadini (dalla posta elettronica, fino alla piattaforma per la partecipazione cd. civica e le consultazioni pubbliche *on line*[65]), ma anche per lo svolgimento delle attività parlamentari. In particolare, sono state sviluppate sia piattaforme digitali dedicate, sia app specifiche, progettate per rispondere alle principali esigenze nei diversi ambiti (documentazione del Servizio studi, preparazione dei lavori in Commissione, presentazione degli atti di sindacato ispettivo e delle proposte di legge, attraverso il ricorso della sottoscrizione degli atti di iniziativa parlamentare mediante firma elettronica).

E' noto che le piattaforme digitali possono essere di diverso tipo: nel caso delle piattaforme proprietarie il codice della piattaforma è di proprietà esclusiva dell'organizzazione promotrice[66], nel caso di quelle *open source* vi si potrà accedere al link di riferimento che porterà al codice aperto. Sta alle Amministrazioni delle Camere (servizi informatici interni) assicurare servizi certificati di partecipazione, tali da gestire adeguatamente l'identità dei partecipanti, la libertà di espressione, la sicurezza dei sistemi, la facilità di utilizzo ecc.[67]

Ne consegue una specificazione dell'interrogativo posto a conclusione del paragrafo precedente: nel caso di ulteriore implementazione dell'uso dei servizi digitali per le attività e funzioni delle Camere (in caso, incluso il voto da remoto) la piattaforma sarebbe di proprietà, organizzata e gestita, della istituzione parlamentare? Con quali modalità potrà ciascuno dei parlamentari entrare nei diversi tipi di riunione telematica che sono il presupposto per esercitare le proprie prerogative?

Bisogna ricordare che le più usate piattaforme che consentono oggi le videoconferenze in diretta (e la loro registrazione e archiviazione) non solo necessitano dei servizi degli , ma della gestione dai principali *Internet content providers*. Tali operatori privati diventerebbero anche loro in qualche misura "padroni di casa" degli spazi (luoghi) delle riunioni digitali.

Inoltre, gli spazi materiali in cui si trovano i parlamentari o le altre persone che partecipano fisicamente alla riunione online sono spazi privati (spesso i domicili) che fungono da luoghi di lavoro occasionalmente e momentaneamente; occorre dunque garantire

---

64 Consultabile online al link *storia.camera.it.,* 8.

65 Sulle piattaforme al servizio della partecipazione civica, cfr. Fondazione <ahref (a cura di), *I Media Civici in ambito parlamentare. Strumenti disponibili e possibili scenari d'uso*. Rapporto per il Senato della Repubblica, 25 maggio 2013. Sul tema cfr. P. Marsocci, *Consultazioni pubbliche e partecipazione popolare*, in *Rassegna parlamentare*, 1, 2016.

66 «Questo, comunque, non esclude il potenziale riutilizzo del codice stesso, previo pagamento di una quota monetaria, che varia da caso a caso, o accordo specifico», Fondazione <ahref (a cura di), *I Media Civici*, cit., 66.

67 Tuttavia, si legge sui siti delle Camere che i Servizi informatici curano la progettazione e lo sviluppo dei sistemi informativi automatizzati *anche affidati a soggetti terzi* (corsivo mio); in tal caso cura i rapporti con l'ente esterno, definisce le specifiche tecniche del progetto in *outsourcing* e ne verifica i risultati. Si pensi all'uso del canale YouTube dedicato o al canale televisivo trasmesso tramite Rai Way.

con regole comuni ed omogenee il rispetto della riservatezza e della intimità della vita domestica, nonché il diritto all'immagine di eventuali terzi.

A questo stesso riguardo, è stato infatti sottolineato che «l'immunità della sede a garanzia del libero spiegarsi delle funzioni degli eletti, fisicamente riuniti in un luogo deputato dal quale è esclusa non solo la forza pubblica, ma qualsiasi persona senza una espressa autorizzazione del Parlamento o dei suoi organi. Immunità con difficoltà estensibile a tutti i luoghi, non necessariamente coincidenti con la residenza, dai quali deputati e senatori potrebbero potenzialmente collegarsi per procedere al voto da remoto»[68], inoltre, nel caso si pensasse a consentire il voto da remoto, «se, financo con le garanzie di cui sopra, si sono verificate, dentro e fuori le Camere, violazioni scandalose dell'art. 48 Cost., possiamo figurarci cosa potrebbe accadere se il voto fosse espresso in luoghi privati, alla presenza eventuale di terzi estranei o con modalità – volute o non – tali da non garantirne la segretezza, quando richiesta»[69]. Questioni non meno delicate rispetto a quelle connesse alla personalità ed uguaglianza del voto.

Ancora, una volta accertato che la riunione digitale sia pienamente assimilabile a quella in presenza corporea (come detto in precedenza, non in assoluto, ma relativamente alle specifiche finalità dell'incontro), ci si deve chiedere se le modalità del suo svolgimento, che necessariamente saranno variate rispetto all'ordinario, rendano possibile seguire le procedure con le relative garanzie di piena attuazione delle norme regolamentari. Posti i requisiti della effettiva compresenza volontaria per il periodo di tempo definito, come attestare la presenza alla riunione? Se ci sono problemi tecnici di disconnessione involontaria momentanea di singoli, che si fa? E se invece il singolo di assenta volontariamente?[70]

Si tratta in sintesi di riflettere sui problemi applicativi e trovare (io credo comunque possibili) alcune puntuali soluzioni.

Una volta curato che questi particolari spazi (luoghi) di riunione apprestino tutte le dovute garanzie costituzionali, si deve passare a capire se il presupposto fondamentale per le deliberazioni assunte dalle Camere sia *completamente* garantito.

Mi riferisco alla esistenza ed alle modalità di dibattito/discussione. Più difficile, a mio avviso, è trovare soluzioni soddisfacenti. Non si tratta solo di organizzare il sistema che permette di prendere la parola e di ascoltare, nel contesto di direzione di chi presiede la

---

[68] A. Malaschini, *Procedure parlamentari,* cit., 6.

[69] G. Silvestri, *Covid-19 e Costituzione,* cit.

[70] A. Malaschini, *Procedure parlamentari,* cit., 4, ricorda il «controllo della regolarità delle votazioni, che i Regolamenti attribuiscono ai Presidenti coadiuvati dai Segretari e, ove necessario, dai Questori. Un controllo che presuppone oggi la contestuale presenza fisica dei "controllori" e dei "controllati" […] non sembra sussistano al giorno d'oggi modelli tali da potersi considerare assolutamente inattaccabili nella trasmissione e nella verifica dei dati: il che rende assai difficile se non impossibile, nel caso di votazioni da remoto, l'esercizio della funzione di controllo anche sotto un profilo tecnico da parte dei soggetti sopra ricordati […] verifica, ove richiesta, del numero legale. Andrebbero eventualmente sommati i parlamentari fisicamente presenti in Aula a quelli presenti on line (o nel caso più drastico contati tutti quelli on line), ampliando però così l'applicazione del nuovo modello dalla fase della votazione a quella preliminare alla votazione stessa […] il problema delle votazioni nominali con appello nel caso di apposizione della questione di fiducia (art. 94, comma 2, Cost.): non si vede in questo caso come evitare la presenza fisica, seppur scaglionata, dei parlamentari […]). I problemi che incontrerebbero le Presidenze delle due Camere ove in sede di votazione da remoto fossero sollevate questioni relative alla regolarità delle votazioni stesse».

seduta, ma anche che permetta il costante e informale dialogo tra parlamentari dentro e fuori i propri gruppi che fa parte della quotidianità del loro lavoro[71]. Inevitabilmente, anche queste attività (di cui comunque si potrebbero far carico le tecnologie digitali) sarebbero parcellizzate e differite nel tempo, con modalità ed effetti nuovi e da valutare. Sicuramente si produrrebbe l'allungamento dei tempi e la loro dilatazione nei nuovi "spazi" di decisione e di voto. Un paradosso in tempi di urgenza, che reclamano risposte rapide e "convincenti" dalle istituzioni.

7. Come non cadere nel dilemma dello "Stato soluzionista", alcune considerazioni conclusive

Come ho osservato in precedenza, appare problematico sostenere in assoluto che quella che si avvale del *Web,* nel caso di incontro e compresenza volontaria, in un determinato lasso temporale e con obiettivi da perseguire attraverso l'aggregazione di persone, non sia una riunione. Né sarebbe sufficiente, a mio avviso, ricondurre al solo esercizio dell'art. 21 o dell'art. 15 e alle relative garanzie costituzionalmente apprestate – certamente a meno che non si intenda esercitare proprio solo quei diritti di libertà – ciò che si può determinare, ad esempio, con una videoconferenza web. La manifestazione del pensiero, come la comunicazione interpersonale, non hanno il connotato essenziale di comportare necessariamente la presenza nello stesso momento di più persone che intendono entrare in relazione, elemento invece che caratterizza la libertà di riunione. Dunque, se si sceglie tale particolare modalità, l'intenzione è quella di riprodurre, nel comunicare e nell'esercitare gli altri eventuali diritti, l'esperienza di una riunione, ossia dello specifico oggetto tutelato dall'art. 17 Cost., e con riferimento alle relative garanzie. Non credo che questo possa far dimenticare l'intento fondamentale dei costituenti, quello di garantire le persone da misure arbitrarie che arrivino a impedire l'aggregazione fisica, se non per comprovati motivi di sicurezza e sanità pubblica.

Piuttosto pare necessario argomentare il perché, in riferimento ad uno specifico organo collegiale, lo svolgimento da remoto di quella determinata modalità di riunione non sia auspicabile in termini di efficacia (nel caso di studio, quanto agli obiettivi costituzionali della funzione di rappresentanza) e/o, in caso, legalmente sostenibile.

Con queste modalità si esercitano (ordinariamente) attività legate ad assolvimento di funzioni pubbliche e private, come già in precedenza accennato.

Dovute invece alla emergenza epidemiologica sono le particolari modalità di svolgimento da remoto, oltre che delle funzioni degli organi già richiamati (specie Governo e Corte costituzionale) [72], anche delle attività processuali. Qualche cenno aggiuntivo a quest'ultimo esempio sembra utile, a fronte dell'interessante dibattito avviato tra magi-

[71] Al tema del riserbo delle trattative parlamentari, fa anche riferimento R. Calvano, *Intervento*, cit.

[72] Nell'odierno dibattito, infatti sono stati avanzati esempi delle disposizioni che hanno riconosciuto la facoltà di riunirsi non in compresenza fisica, ma in videoconferenza, ai Consigli e alle Giunte comunali e delle Città metropolitane (ai sensi dall'art. 73 del d.l. 17 marzo 2020. n. 18), alle autorità indipendenti. Così, Ainis, Curreri, Trucco, *Intervento*, cit. Sostengono che l'analogia con i lavori delle assemblee parlamentari non sia in questo senso sostenibile, considerati il livello diverso di rappresentanza e la natura delle funzioni, R. Calvano, V. Lippolis e M. Luciani, *Intervento*, cit.

strati, avvocati, CSM e organi di rappresentanza, proprio a scongiurare un eccessivo – e dunque potenzialmente lesivo delle garanzie costituzionali – ricorso al processo penale smaterializzato.[73].

Anche in questo ambito, il Governo ha adottato ampie misure di contenimento dello svolgimento della funzione giurisdizionale[74]. L'art. 83 del d.l. 18/2020 – ora convertito nella legge 24 aprile 2020, n. 27 – ha introdotto importanti innovazioni, per lo svolgimento dell'udienza, relative alle attività non sospese, prevedendo che – in una serie consistente di casi – possa essere celebrata «mediante videoconferenze o con collegamenti da remoto»[75].

Se tali modalità prima potevano essere utilizzate solo con riferimento a specifici casi (detenuti non trasportabili)[76] e con l'ausilio della piattaforma interattiva proprietaria del Ministero, l'urgenza determinata dalla emergenza ha reso necessario individuare (ulteriori) piattaforme utilizzabili (ad esempio Skype o Teams di Microsoft). A farlo è il Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia (il DGSIA), con provvedimenti tali da assicurare (nel rispetto di molte delle norme di procedura penale) la reciproca visibilità tra tutte le persone coinvolte nella videoconferenza; la possibilità per il difensore di scegliere se partecipare alla videoconferenza presso l'ufficio giudiziario o presso il luogo ove è custodito l'indagato/imputato e – in ogni caso – assicurare la possibilità di comunicazioni riservate tra difensore e assistito.

---

[73] Diffusamente, G. Santalucia, *La tecnica al servizio della giustizia penale. Attività giudiziaria a distanza nella conversione del decreto "cura Italia"*, in *Giustizia insieme*, n. 993 del 10 aprile 2020; L. Fidelio - A. Natale, *Emergenza COVID-19 e giudizio penale di merito: un catalogo (incompleto) dei problemi*, in *Questione giustizia*, 16 aprile 2020.

[74] Per primo il d.l. 11/2020, in vigore dall'8 marzo 2020, ha disciplinato le modalità di "decompressione" dell'attività giudiziaria, successivamente tali disposizioni sono state stati abrogate dall'art. 83, c. 22, del d.l. 18/2020, c.d. decreto "Cura-Italia", intervenuto a graduare i previsti rinvii, le sospensioni e i differimento dei termini, in due distinti periodi: dal 9 marzo 2020 al 15 aprile 2020, sono sospese pressoché tutte le attività processuali (fatte salve alcune eccezioni) e il decorso di quasi tutti i termini processuali; dal 16 aprile 2020 al 30 giugno 2020, la decisione è affidata – un catalogo delle misure adottabili - dai dirigenti degli uffici giudiziari che «adottano le misure organizzative, anche relative alla trattazione degli affari giudiziari, necessarie per consentire il rispetto delle indicazioni igienico sanitarie […] al fine di evitare assembramenti all'interno dell'ufficio giudiziario e contatti ravvicinati tra le persone».

[75] L. Fidelio - A. Natale, *Emergenza COVID-19 e giudizio penale di merito,* cit., par. 6, «la possibilità di avvalersi di collegamenti da remoto era inizialmente prevista per la celebrazione delle attività processuali "non sospese" che coinvolgessero persone detenute, internate o in stato di custodia cautelare (art. 83, c. 12). In sede di esame parlamentare, il maxi-emendamento del governo ha introdotto una serie di ulteriori ipotesi in cui l'attività procedimentale e processuale può essere celebrata con collegamenti da remoto (art. 83, cc. 12-*bis*, 12-*ter*, 12-*quater*, 12-*quinquies*): limitando i riferimenti agli aspetti di interesse per il giudice di merito, si può dare conto del fatto che è prevista la possibilità di procedere con modalità di partecipazione a distanza». In particolare: per celebrare le «udienze penali che non richiedono la partecipazione di soggetti diversi dal pubblico ministero, dalle parti private e dai rispettivi difensori, dagli ausiliari del giudice, da ufficiali o agenti di polizia giudiziaria, da interpreti, consulenti o periti» (c. 12-*bis*); durante le indagini preliminari «per compiere atti che richiedono la partecipazione della persona sottoposta alle indagini, della persona offesa, del difensore, di consulenti, di esperti o di altre persone, nei casi in cui la presenza fisica di costoro non può essere assicurata senza mettere a rischio le esigenze di contenimento della diffusione del virus COVID-19» (c. 12-*quater*); per la celebrazione delle camere di consiglio.

[76] Così anche occorre ricordare che da molto tempo a livello di Ue esistono varie iniziative riguardanti l'utilizzo della videoconferenza nei procedimenti giudiziari, cfr. Segretariato generale del Consiglio, *La videoconferenza nel contesto della giustizia elettronica europea*, 2009.

L'art. 83, c. 12-*bis*, d.l. 18/2020 – introdotto in sede di conversione dal maxi-emendamento – ha imposto che l'udienza celebrata con videoconferenza sia condotta con modalità idonee a salvaguardare il contraddittorio e l'effettiva partecipazione delle parti. «La normativa dell'emergenza non distingue tra udienza dibattimentali e udienze camerali e tra tipologie di reati per i quali si procede o, ancora, per veste processuale della persona della cui partecipazione a distanza si discuta»[77], mentre alla trasformazione del rito non seguirebbe obbligatoriamente l'adozione anche del modulo decisorio da remoto (come stabilisce infatti il testo della conversione del d.l., licenziato dal Senato), perché la modalità di decisione da remoto sarà eventuale, sostanzialmente rimessa a una decisione preliminare della Corte medesima[78].

Da ultimo, è intervenuto d.l. del 30 aprile 2020, n. 28 (artt. 3,4 e 5), in parte tornando a restringere le ipotesi previste dal precedente d.l. e comunque spostando in avanti il termine finale del secondo periodo di emergenza, prima fissato al 30 giugno e ora al 31 luglio 2020[79].

Come è immaginabile, anche con rispetto a questa delicatissima esperienza, i commenti e gli interventi sono stati indirizzati ad analizzare il concetto e natura dei "luoghi" dai quali possono connettersi alla videoconferenza gli attori processuali, al fine di verificarne la piena idoneità nel rispetto della legalità[80]. Si va, nel caso del detenuto, dal luogo di detenzione, all'ufficio di polizia giudiziaria, alla medesima postazione da cui si collega il difensore (se l'imputato non è soggetto a misure cautelari o è libero), nel caso dei

[77] G. Santalucia, *La tecnica*, cit., par. 1. Anche durante il corso delle indagini preliminari, il pubblico ministero e il giudice potranno avvalersi di collegamenti da remoto, ancora una volta individuati e regolati con provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia. Così si è appreso dalla stampa che in videoconferenza sono stati ascoltati ad aprile i primi testimoni delle inchieste sulle morti sospette nelle RSA.

[78] Per l'intero periodo emergenziale (9 marzo - 30 giugno 2020), le deliberazioni collegiali in camera di consiglio, per la definizione dei procedimenti che non patiscono la sospensione, siano essi civili che penali, «possono essere assunte mediante collegamenti da remoto individuati e regolati con provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia».

[79] «Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19». Osserva G. Santalucia, *Un altro decreto legge – n. 28 del 30 aprile 2020 – in materia di giustizia penale per l'emergenza sanitaria e non solo*, in *Giustizia insieme*, 1 maggio 2020, che «La successione tra le previsioni dei due decreti non subisce per il vero l'interferenza dell'approvazione della legge di conversione – legge n. 27 del 24 aprile 2020, pubblicata sulla G.U. del 29 aprile successivo – che, come è noto, ha apportato importanti modifiche al decreto-legge n. 18 e che è successiva al decreto-legge n. 23, per il semplice fatto che in nessuna parte le innovazioni della legge di conversione contengono disposizioni in punto di confini temporali del periodo di emergenza».

[80] Il Csm è intervenuto dettando apposite linee guida, con delibera del 26 marzo 2020, con cui si invitano i dirigenti a favorire forme di lavoro "da remoto"; a prevedere forme di comunicazione tra uffici essenzialmente telematiche; ad adottare misure utili a contenere il numero di persone che hanno accesso agli uffici giudiziari; a coinvolgere i consigli dell'Ordine degli avvocati, stipulando con essi protocolli per «individuare modalità condivise di partecipazione da remoto dei soggetti del processo»; a predisporre turni di servizio dei magistrati – anche in deroga alle destinazioni tabellari vigenti – per "coprire" i servizi urgenti, suddividendo il carico di lavoro (e il rischio di esposizione al contagio) tra i magistrati in servizio; ad adottare le misure organizzative all'esito di procedure partecipate. Forti perplessità sono state sollevate dell'avvocatura (con alcune prese di posizione dell'Unione Camere Penali Italiane), dalla dottrina (v. quanto rilevato dall'Associazione tra gli studiosi del processo penale) e in parte della magistratura associata (v. il comunicato di Magistratura democratica su *I rischi dell'udienza telematica*).

magistrati (requirente e giudicante, e nelle camere di consiglio), la connessione avviene sia presso l'ufficio giudiziario, sia da remoto presso le loro abitazioni, così anche nel caso degli ausiliari. Evidente che tutto ciò debba essere valutato alla luce dei principi di oralità e immediatezza nel processo penale e alla possibilità di contatto tra accusato e giudice[81], considerata la particolarità della "scena pubblica", in cui consiste il dibattimento processuale[82].

Con riferimento all'esempio del mondo giudiziario[83], così come al tema di questo contributo, le preoccupazioni espresse riguardano poi e in conclusione i dubbi sul tempo a venire: l'accelerazione in chiave tecnologica dei percorsi innovativi (sebbene oggi indispensabili), non ha al momento fatto concentrare l'attenzione su quali specifiche attività potrebbero anche a regime avvenire da remoto, senza alcuna lesione dei diritti coinvolti, ma solo a segnalare il generale rischio che la tendenza innescata oggi potrebbe spingere ad impoverire e non a valorizzare le funzioni pubbliche. Lo stato emergenziale attuale «non è il paradigma fondativo delle nostre comunità politiche, non è la regola, non può neppure essere legittimato come strumento di governo, deve invece nei limiti del possibile essere circoscritto… non si deve accettare che terminato lo "stato di necessità" la rottura delle regole prosegua».[84]

E' difficile non essere d'accordo, tuttavia a mio avviso, da ora in poi, dovremo cogliere l'occasione che stiamo vivendo tutti, ma con una diversa sensibilità e consapevolezza (anche collettiva e di costruzione del senso comune), per ragionare profondamente sulla sostenibilità costituzionale delle pratiche e procedure di "lavoro" a distanza ammesse o da ammettere, a partire da quelle già in atto prima della emergenza.

Sono molte, infatti, le decisioni ormai ordinariamente di fatto operanti rispetto all'uso delle tecnologie digitali nell'assolvimento di attività e funzioni pubbliche. Non sempre sono state il frutto di opzioni discusse e condivise, non necessariamente sono né garantiste in termini di legalità, né pienamente soddisfacenti in termini di efficacia rispetto agli obiettivi da realizzare.

Una delle tante derive del capitalismo (digitale) contemporaneo è quella che è stata definita da Evgeny Morozov, proprio con riferimento al momento attuale, "dello Stato

---

[81] Sottolineano, L. Fidelio - A. Natale, *Emergenza COVID-19 e giudizio penale di merito,* cit., che «non è indifferente che una persona arrestata partecipi all'udienza di convalida in un'aula di udienza o nell'ufficio della polizia giudiziaria che lo ha appena tratto in arresto; né è indifferente che – come la recente storia giudiziaria tragicamente insegna – un giudice possa avere un contatto diretto e attento con l'arrestato; né è indifferente che tutti i protagonisti dell'udienza abbiano una possibilità di agile interlocuzione, che non si può nutrire delle sole frasi veicolate dalla telematica».

[82] F. Cordero, *Procedura penale*, Milano, 2006, 931, «hanno un costo emotivo, i dibattimenti: e il luogo conta molto nell'economia psichica; non è lo stesso stare nell'aula o in piazza. Sono rilievi antropologicamente ovvi: i processi implicano tempo e spazio separati, ossia sacri».

[83] L. Fidelio - A. Natale, *Emergenza COVID-19 e giudizio penale di merito,* cit., F. Donati, *Giustizia online al tempo del Coronavirus e dopo*, *Liber Amicorum per Pasquale Costanzo*, in *Consulta online*, 17 aprile 2020, spec. 6 ss., si pone invece il tema delle prospettive per il dopo emergenza della partecipazione processuale da remoto.

[84] G. Azzariti, *Editoriale. Il diritto costituzionale d'eccezione*, cit. 3. Nello stesso senso, S. Prisco - F. Abbondante, *I diritti al tempo del coronavirus,* cit., 7, «Ogni discussione quanto alla possibile stabilizzazione di ammodernamenti che talune soluzioni recherebbero alle istituzioni è legittima, ma va rinviata a tempi tranquilli, nei quali la riflessione può non essere concitata e può soppesare con ponderazione i pro e i contra».

soluzionista", al cui cuore starebbe:

«una serie di misure, in teoria pragmatiche, in grado di mantenere in funzione la macchina del capitalismo globale risolvendo le contraddizioni che emergono nel corso del suo funzionamento: il tutto, sorprendentemente, con notevoli profitti […] sull'idea che si possa evitare di affrontare le cause di un problema, concentrandosi invece sull'"adeguare" i comportamenti individuali alla crudele, ma immutabile, realtà […] una versione più umana ma anche più sofisticata dello stato di sorveglianza che lo ha preceduto […] Mi aspetto quindi che i governi riversino miliardi in quella che, un anno fa, ho definito la "tecnologia della sopravvivenza": tecnologie digitali che permetteranno al capitalismo di andare avanti, alleviando nel frattempo alcuni dei suoi problemi. Questo rafforzerà anche la legittimità dello stato soluzionista, che potrà vantarsi di aver respinto "l'opzione cinese" […] L'idea di costruire questo nuovo ordine sulle fondamenta digitali offerte da Amazon, Facebook o dall'operatore di telefonia mobile del vostro paese può sembrare allettante, ma non ne verrà niente di buono»[85].

Come non cadere o continuare a cadere nel dilemma dello Stato soluzionista descritto e analizzato, condivisibilmente, dal sociologo bielorusso? È sempre del tutto necessario porre la questione nei termini di resistenza alle tentazioni della tecnica?
Si tratta di evidenziare e discutere questioni – che, per il fatto di essere legate all'uso di strumenti continuamente in evoluzione, ancora oggi, appaiono nuove – per proporre le necessarie distinzioni e soluzioni, possibilmente a prescindere e non sollecitati dalla sola stringente urgenza o necessità, quando non dalla mera opportunità pratica. E' una questione di scelte, che a monte ha (o dovrebbe avere) una attenta valutazione dello specifico servizio tecnologico digitale, individuato come idoneo per quella particolare funzione o attività.
La attuale emergenza sanitaria è stata già da tanti e su molti fronti (primo tra tutti quello della tutela dell'ambiente e della sostenibilità della produzione a tutti i livelli) interpretato come un tragico e 'scomodissimo', ma prezioso ammonimento per cambiare rotta.
Tornando a volgere l'attenzione solo all'oggetto delle presenti riflessioni, sono d'accordo con chi osserva, immagino auspicandolo, che fare entrare i servizi che la fase attuale del *Web* mette a disposizione significhi reingegnerizzazione i lavori parlamentari[86].
E' a partire da questa consapevolezza che si potrebbe meglio indirizzare una possibile futura scelta (che ad oggi appare improbabile), volta a implementare – facendone oggetto di disciplina regolamentare – l'uso del digitale nelle deliberazioni parlamentari, con forme idonee a garantire a pieno il rispetto della Costituzione, nei soli casi accertati in cui uno stato di emergenza renda impossibile la presenza fisica nei Palazzi della rappresentanza di un numero consistente dei membri delle Camere e tale da mettere a rischio la funzionalità stessa del'organo; ipotesi che non è a mio avviso da respingere.
Si tratta di una sfida notevole e delicata, ma se il risultato si realizzasse in questi termini (altrimenti sarebbe, da scongiurare) sarebbe un esempio eccellente e il Parlamento riacquisterebbe anche centralità nel dibattito pubblico sullo spazio delle tecnologie digitali

[85] E. Morozov, *L'emergenza sanitaria e il rischio del totalitarismo*, in *Internazionale*, 4 aprile 2020.

[86] N. Lupo, *Intervento* in diretta Facebook, cit.

al servizio del costituzionalismo, anche – o piuttosto solo a condizione che – tali considerazioni mettano al centro la necessità di garantire l'uso istituzionale di piattaforme e app (e relativi server) dedicate, di tipo proprietario[87], con codici identificativi protetti e puntuale rispetto dei più alti standard di sicurezza informatica, contro la perdita dei dati o l'intrusione.

I servizi *web* non sono servizi come altri. Affittare una sala riunioni privata in un centro congressi o in un teatro, avvalendosi dello spazio e delle attrezzature da altri lì predisposte, non è equivalente e non solo per il diverso livello di modernità tecnologica.

Senza qui voler scomodare le ricerche sulle modificazioni profonde degli stati mentali di attenzione dettati dall'esposizione al *Web* – quasi permanente nei tempi di vita che si fondono e confondono con quelli di lavoro, fino ad ostacolare il pieno e libero sviluppo della stessa progettualità individuale e collettiva[88]–, è appena il caso di ricordare che chi struttura, se si preferisce 'architetta'[89], questi spazi dispone di un potere decisamente più pervasivo sulle stesse modalità di svolgimento delle attività e dei comportamenti che lì si esprimono.

E' necessario distinguere i 'fatti' tecnici, dalle 'tendenze' tecniche, sollecitate e precostituite a monte; il fine è di valutarne non solo astrattamente l'efficienza pratica, ma la capacità di soddisfazione del volere e delle necessità (soprattutto se istituzionali) di chi sceglie di servirsene. Le pratiche degli automatismi tecnologici sono, in definitiva, strutturanti[90]. Un ragionamento che già Michel Foucault fece, sostenendo che le scelte

[87] Del resto, potendo ciascuna Camere avvalersi di eccellenti Servizi informatici. Non è ad esempio questa la scelta fatta oggi dagli Atenei italiani, dove le attività presenti e future si avvalgono delle piattaforme architettate e messe a disposizione di Google e Microsoft. Cfr., l'esperienza del server messo a disposizione dal CNR (*jitsi.cedrc.cnr.it*). Interessante anche la mappa virtuale, che mostra le strategie nazionali adottate in materia di sicurezza dell'Italia predisposta dall'ENISA (*European Network Information and Security Agency*) e il documento *Good practices in innovation on Cybersecurity under the NCSS,* pubblicato a novembre 2019, sulle strategie nazionali volte a garantire la cyber sicurezza, al fine di disegnare una visione d'insieme di ciò che accade all'interno dell'Ue.

[88] Alla base delle ricerche sulla cd. governamentalità algoritmica, condotte da A. Rouvroy - T. Berns, *Gouvernementalité algorithmique et perspectives d'émancipation*, *in Politique des algorithmes, Metriques du Web*, Réseaux 2013/1 (No 177), ampiamente riutilizzate, ad esempio, più recentemente da B. Stiegler, *La società automatica. L'avvenire del lavoro*, Milano, 2019 (traduzione italiana del lavoro edito nel 2015), per porre le basi del suo concetto di ritenzione (il divenire passato di ciò che è stato presente) terziaria dei nuovi circuiti digitale di transindividuazione e della sua proposta di usare la stessa tecnologia digitale come *pharmakon* (nel senso etimologico dell'essere contemporaneamente tossicità e rimedio) e contrastare il presunto 'destino' di questa società dell'iper-controllo.

[89] Insieme di regole dell'hardware e del software, che L. Lessig, *Code and Others Laws of Cyberspace*, Basic Books, New York 1999, ora in versione interattiva ("wiki"), *Code version 2.0*, Basic Books, New York 2006, 128 ss. ha chiamato *Code* o architettura digitale, riferendosi al cyberspazio.

[90] Su questo come realtà effettiva e sulla migliore opportunità che il concetto di *habitus* offre per la sua qualificazione, avevo già proposto (*Lo spazio di internet*, cit. 6) di avvalersi della analogia con la nozione elaborata da Pierre Bourdieu: «sistema di disposizioni durevoli e trasponibili, strutture strutturate che funzionano come strutture strutturanti, cioè come principio organizzatore di pratiche e di rappresentazioni che possono essere oggettivamente accordate con il loro scopo, senza supporre il cosciente perseguimento dei fini e la padronanza espressa delle operazioni necessarie per realizzarli, oggettivamente 'regolate' e 'regolari', senza essere per nulla il prodotto dell'obbedienza a regole, e per di più orchestrate collettivamente, senza essere il prodotto dell'azione organizzatrice di un direttore di orchestra». Sulla apparente neutralità della tecnologia, cfr. le considerazioni approfondite di recente da E. Stradella, *Stereotipi e discriminazioni: dall'intelligenza umana all'intelligenza artificiale*, *Liber Amicorum per*

di infrastruttura software incidono profondamente sulla maniera in cui gli internauti "vedono" le informazioni e si rappresentano il mondo digitale[91], assumendo un valore di sfondo comune e dunque contribuendo a strutturare la realtà.
La strada da seguire è dunque la più tradizionale: la costruzione di un pensiero politico che indirizzi la produzione di norme e permetta di gestire (non di adeguarsi a) tali *tendenze* e i relativi effetti, indirizzando, nel rispetto pieno del costituzionalismo democratico, il saper vivere nella attuale economia digitale.

Pasquale Costanzo, cit., 30 marzo 2020, spec. 4.

[91] Riportato da D. Cardon, *La Démocratie Internet*, Promesses et limites, Seuil, Paris 2010, cit. 95. Cfr. anche F. Colombo, *Controllo, identità, parresia. Un approccio foucaultiano al web 2.0*, in *Comunicazioni sociali*, Milano, 2, 2012, 197 ss.

La libertà di espressione dei partiti politici nello spazio pubblico digitale: alcuni spunti di attualità*

Paolo Zicchittu

Abstract

Partendo da due recenti vicende giurisprudenziali, che hanno visto contrapporsi taluni movimenti di estrema destra a Facebook, in ordine alla violazione di alcuni c.d. "standard della community", a seguito dell'esposizione di contenuti discriminatori, il saggio, da un lato, si interroga sul ruolo progressivamente assunto dalle reti sociali, con riguardo all'attuazione delle garanzie offerte dall'art. 21 Cost., dall'altro, riflette sul valore e sul significato da riconoscere alla libertà di manifestazione del pensiero di quei partiti, che esprimano posizioni estremiste, eversive o antisistema. L'analisi viene condotta ricostruendo la portata normativa e la *ratio* profonda delle relative previsioni costituzionali, con specifico riguardo al diritto di esprimere liberamente il proprio pensiero, alla libertà di associazione, al diritto di costituire un movimento politico e al divieto di ricostituzione del disciolto partito fascista, anche al fine di valutare il disegno antropologico complessivo prefigurato dal Costituente di fronte ai "nemici della libertà". In questa prospettiva, ampio spazio viene assegnato all'attuazione pratica e casistica del dettato costituzionale con particolare riferimento alla posizione assunta dai giudici nazionali e dalle grandi multinazionali che gestiscono le singole piattaforme digitali, per poi giungere ad esaminare la giurisprudenza della Corte europea dei diritti dell'uomo. Il contributo avanza infine una proposta procedurale tesa a salvaguardare il più possibile tanto l'autonomia privata dei social network tanto i diritti costituzionali dei singoli e delle formazioni politiche.

Taking the cue from two recent judicial cases, which have seen some extreme right-wing movements against Facebook, in relation to the infringement of certain "community standards", after the publication of discriminatory content, the essay questions, on the one side, the role increasingly played by social networks as regards the implementation of the guarantees provided for under art. 21 of the Constitution and reflects, on the other side, on the value and the meaning to be recognized to freedom of thought for those parties expressing extremist, subversive or anti-system positions. The analysis retraces the normative scope and the rationale behind the relevant constitutional provisions, with specific regard to freedom of expression, freedom

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

of association, the right to freely associate in parties and the prohibition to reorganise, under any form whatsoever, the dissolved Fascist party, also in order to assess the overall anthropological design the Constituent laid down in front of the "*ennemis de la liberté*". From this point view, the study focuses extensively on the practical and case-by-case enforcement of the constitutional provisions, with particular emphasis on the stance taken by national judges and multinational corporations managing individual digital platforms, to then get to examine the case law of the European Court of Human Rights. Finally, the paper makes a procedural proposal aimed to ensure the highest protection to both private autonomy of social networks and constitutional rights of individuals as well as political groups.

Sommario

1. La crisi di un modello? – 2. Un buon esempio: *Facebook* contro *Casa-Pound*. – 3. Lo spazio pubblico costituzionale nell'era dei *social network*. – 4. Il divieto di «riorganizzazione del disciolto partito fascista» nella teoria e nella prassi. – 5. *Quot capita, tot sententiae* … una proposta.

Keywords

social network – Internet – libertà di espressione – partiti politici – propaganda

1. La crisi di un modello?

È ancora possibile per i moderni ordinamenti costituzionali contrastare i partiti antisistema, senza abdicare a quei princìpi di libertà e pluralismo, che da sempre caratterizzano il loro retroterra ideologico e culturale?

Questo interrogativo assume connotazioni decisamente più pregnanti di fronte alla crescita esponenziale della comunicazione politica via *social*, soprattutto da parte di movimenti, che, più o meno dichiaratamente, si rifanno all'esperienza del ventennio fascista, riproponendo paradigmi, stilemi e argomentazioni, giudicati eversivi o comunque in aperto contrasto con il patto fondativo a partire dal quale si sviluppa la Costituzione repubblicana[1]. Assai spesso, le posizioni sostenute in rete appaiono scarsamente suffragate, esageratamente semplificate e – talvolta – perfino violente, tanto da incrinare quella fiducia che, come si avrà modo di approfondire, il nostro Costituente

[1] Per un primo inquadramento della problematica richiamata nel corpo del testo si rimanda, esemplarmente, ai contributi di L. Scaffardi, *Oltre i confini della libertà di espressione. L'istigazione all'odio razziale*, Padova, 2009; L. Picotti, *Diffusione di idee razziste ed incitamento a commettere atti di discriminazione razziale*, in *Giurisprudenza di merito*, 2006, 1966 ss.; C. Caruso, *Dignità degli "altri" e spazi di libertà degli "intolleranti". Una rilettura dell'art. 21 Cost.*, in *Quaderni costituzionali*, 2013, 795 ss.; M. Bonini, *La democrazia alla prova dei suoi valori: ripudiare il partito neonazista tedesco senza scioglierlo*, in *Osservatorio Costituzionale*, 2017, 471 ss.; A. Pugiotto, *Le parole sono pietre? I discorsi di odio e la libertà di espressione nel diritto costituzionale*, in *penalecontemporaneo.it*, 15 luglio 2013.

ha riposto nelle radici ideali e nei valori costitutivi del modello liberale[2].
Le modalità attraverso cui, comunemente, avvengono gli interscambi politici su *internet*, dunque, gettano più di qualche dubbio circa la possibilità che una discorsività razionale possa effettivamente emergere dal confronto indipendente e schietto tra tutte le opinioni presenti all'interno del c.d. "*free market of ideas*", anche quelle ritenute più esecrabili[3]. Di qui, la tentazione di recuperare alcune forme di protezione della democrazia, ricorrendo alla repressione – anche penale – delle condotte che diffondono idee in radicale antitesi con il dettato costituzionale[4].

2. Un buon esempio: *Facebook* contro *Casa-Pound*

In tale prospettiva, la recente vicenda processuale, che ha contrapposto Casa-Pound Italia a Facebook fornisce degli utilissimi spunti di riflessione per comprendere quale sia, in concreto, l'esatta strutturazione dello spazio pubblico e a quali limiti di ordine costituzionale esso debba eventualmente soggiacere. La fattispecie in questione origina dal giudizio promosso in sede cautelare dalla nota associazione neofascista avverso la disattivazione della propria pagina *social* operata unilateralmente dal colosso di Menlo Park. Al riguardo, il Tribunale di Roma ha accolto integralmente il ricorso, ordinando la riapertura del relativo profilo, in ragione di alcune argomentazioni davvero peculiari, che concorrono a inquadrare il servizio prestato da questo tipo di piattaforme e, al contempo, ricontestualizzano il pluralismo politico e informativo dinanzi ai discorsi d'odio.

[2] Così D. Piccione, *L'espressione del pensiero ostile alla democrazia, tra diritto penale dell'emotività e psicologia collettiva*, in *questa Rivista*, 3, 2018, 77 ss.; M. Rosenfeld – A. Sajo, *Spreading Liberal Constitutionalism: An Inquiry into the Fate of Free Speech Rights in New Democracies*, in S. Choudry (a cura di), *The Migration of Constitutional Ideas*, Cambridge, 2007, 24 ss.; M. Orofino, *La libertà di espressione tra Costituzione e Carte europee dei diritti*, Torino, 2014, 42 ss.; O. Pollicino, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in G. Pitruzzella – O. Pollicino – S. Quintarelli (a cura di), *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, 2017, 48 ss. Tra gli scritti più risalenti, si rimanda a K. Loewenstein, *Militant Democracy and Fundamental Rights*, in *American Political Science Review*, 1937, 417 ss.

[3] Sulla regolamentazione delle nuove modalità espressive presenti in rete si vedano, in primo luogo, L. Lessig, *Reading the Constitution in Cyberspace*, in *Emory Law Journal*, 3, 1996, 1 ss. O. Pollicino – M. Bassini, *Free Speech, Defamation and the Limits to Freedom of Expression in the EU: A Comparative Analysis*, in A. Savin – J. Trzaskowski (a cura di), *Research Handbook on EU Internet Law*, Northampton, 2014, 508 ss.; P. Costanzo, *Libertà di manifestazione del pensiero e "pubblicazione" su Internet*, in *Il diritto dell'informazione e dell'informatica*, 1, 1998, 370 ss.; J.R. Reidenberg, *Yahoo and Democracy on the Internet,* in *Jurimetrics*, 2, 2002, 261 ss.; *passim* C. Caruso, *La libertà di espressione in azione: contributo a una teoria costituzionale del discorso pubblico*, Bologna, 2013.

[4] Rispetto alla repressione soprattutto penale delle condotte eversive e antisistema si consultino D.J. Schaller, *From the Editors: Judges and Politicians as Historians?*, in *Journal of Genocide Research*, 9, 2007, 2 ss.; A. Di Giovine, *Il passato che non passa: "Eichmann di carta" e repressione penale*, in A. Di Giovine – S. Sicardi (a cura di), *Democrazie imperfette. Atti del convegno dell'Associazione di diritto pubblico comparato ed europeo*, Torino, 2005, vol. I, XXVII ss.; E. Fronza, *Il negazionismo come reato*, Milano, 2012; M. Caputo, *La "menzogna di Auschwitz", le "verità" del diritto penale. La criminalizzazione del c.d. negazionismo tra ordine pubblico, dignità e senso di umanità*, in *penalecontemporaneo.it*, 7 gennaio 2014; D. Bifulco, *Negare l'evidenza. Diritto e storia di fronte alla "menzogna di Auschwitz"*, Milano, 2012; D. Piccione, *L'antifascismo e i limiti alla manifestazione del pensiero tra difesa della Costituzione e diritto penale dell'emotività*, in *Giurisprudenza costituzionale*, 2017, 1941 ss.; A. Ambrosi, *Libertà di pensiero e manifestazione di opinioni razziste e xenofobe*, in *Quaderni costituzionali*, 2008, 523 ss.

Preliminarmente, il giudice monocratico riconosce la natura *iure privatorum* del rapporto che gli utenti intrattengono con la rete sociale, concentrandosi poi sugli "standard della community" diretti a censurare la manifestazione di opinioni violente o disumanizzanti[5]. Di norma, infatti, la violazione di queste vere e proprie condizioni generali di contratto autorizzerebbe la piattaforma ad escludere o a rimuovere temporaneamente dal servizio i singoli o le organizzazioni, che, in un modo o nell'altro, incitano all'odio[6]. Tuttavia, secondo il Tribunale, la relazione tra la rete e i suoi utilizzatori finali non può essere assimilata *in toto* al rapporto contrattuale, che ordinariamente si instaura tra due soggetti privati, giacché una delle parti ricopre una speciale posizione all'interno dell'agone mediatico.

In proposito, il giudice cautelare osserva come, all'interno dell'attuale sistema comunicativo, le reti occupino oramai un livello di pervasività, tale per cui un soggetto politico, che non sia anche materialmente presente sulla piattaforma, rischia di essere escluso dal dibattito pubblico[7]. I *social network* assolverebbero, cioè, ad una funzione essenziale per l'attuazione di alcuni principi cardine dell'ordinamento, tra cui spiccano proprio la libertà di manifestazione del pensiero e il pluralismo dei partiti[8]. Da questo punto di vista, la rimozione coattiva della pagina di Casa-Pound inficia la democraticità del sistema, poiché comprime la possibilità di comunicare in pubblico alcuni messaggi politici, in ragione del loro contenuto. La disattivazione ingiustificata e improvvisa di un profilo *social* integra, pertanto, una misura sproporzionata, lesiva della libertà di espressione di un soggetto collettivo, che ricoprire una funzione costituzionalmente qualificata: qualunque sia il contegno ideologico assunto da un partito, la responsabilità dei suoi aderenti non può ricadere in via automatica sul movimento, privandolo addirittura del diritto di prendere parte al dibattito pubblico[9].

Il provvedimento cautelare, insomma, ridefinisce la gestione degli spazi comunicativi, poiché sottrae il controllo di uno dei più diffusi strumenti *social* alla piena discrezionalità dei soggetti privati e alle logiche di mercato. Il giudice cioè riconosce alla libertà di manifestazione del pensiero assicurata dalla Costituzione ai partiti una sorta di *drit-*

---

[5] Cfr. Facebook community standard n. 13, Contenuti deplorevoli, Incitamento all'odio: «Definiamo discorsi di incitazione all'odio come un attacco diretto alle persone sulla base di aspetti tutelati a norma di legge, quali razza, etnia, nazionalità di origine, religione, orientamento sessuale, casta, sesso, genere o identità di genere e disabilità o malattie gravi […] Definiamo l'attacco come un discorso violento o disumanizzante, dichiarazioni di inferiorità o incitazioni all'esclusione o alla segregazione».

[6] Così, Facebook community standard, Introduzione: «Le conseguenze per la violazione degli Standard della community dipendono dalla gravità della violazione stessa e dai precedenti della persona sulla piattaforma. Ad esempio, nel caso della prima violazione, potremmo solo avvertire la persona, ma se continua a violare le nostre normative, potremmo limitare la sua capacità di pubblicare su Facebook o disabilitare il suo profilo. Potremmo anche informare le forze dell'ordine quando, a nostro avviso, sussiste la possibilità reale di seri rischi di danno fisico o minacce dirette alla sicurezza pubblica».

[7] Trib. Roma, sez. specializzata in materia di impresa, ord. 12 dicembre 2019, § 3, p. 4.

[8] Sulla peculiare posizione ricoperta dai *social network* nell'ambito della comunicazione politica si vedano P. Costanzo, *La "democrazia digitale" (precauzioni per l'uso)*, in *Diritto pubblico*, 1, 2019, 71 ss.; F. Pira, *La net comunicazione. Partiti, movimenti e cittadini-elettori nell'era dei social networks*, Milano, 2012, 57 ss.; G. Giansante, *La comunicazione politica online. Come usare il web per costruire consenso e stimolare la partecipazione*, Roma, 2014, 106 ss.; S. Bentivenga, *Politica e nuove tecnologie della comunicazione*, Roma-Bari, 2002, 66 ss.; A. Palmieri, *Internet e comunicazione politica. Strategie, tattiche, esperienze e prospettive*, Milano, 2016, 84 ss.

[9] Trib. Roma, ord. 12 dicembre 2019, cit., § 3, p. 5.

twirkung, in grado non solo di generare obblighi a carico dei pubblici poteri, ma anche di sprigionare effetti vincolanti nei rapporti interprivati, a maggior ragione quando ci si trovi al cospetto di un potere – quello dei *social network* – capace di penalizzare notevolmente le associazioni che non si uniformano a determinati contenuti[10]. Non diversamente da quanto accade per le Istituzioni statali, quindi, anche le tecnostrutture che disciplinano concretamente l'accesso al discorso pubblico in rete sono tenute a garantire la massima apertura del dibattito politico, anche astenendosi da pervasive valutazioni di merito sui messaggi trasmessi dagli utenti[11].

Di conseguenza, il riferimento alle finalità perseguite da un'associazione, di per sé, non potrà mai costituire una giustificazione sufficiente per procedere all'oscuramento della relativa pagina. Il principio pluralista, infatti, irradia l'ordinamento in tutte le sue declinazioni, per cui ogni eventuale limite alla libertà di opinione dovrà trovare esplicito fondamento in Costituzione e sottostare a uno *strict scrutiny* da parte dell'autorità giudiziaria[12]. La generica contrarietà ai precetti costituzionali degli obiettivi programmatici di Casa-Pound non legittima *ipso facto* l'esclusione di quel movimento dalla sfera pubblica, né basta la presunta pericolosità di talune proposte per espungere definitivamente quel partito dall'*agorà* digitale. In ogni caso, conclude l'ordinanza, non può essere demandato a dei soggetti privati – e in particolar modo alle corporazioni multinazionali, che gestiscono i *social network* – il compito di valutare la conformità a Costituzione degli attori politici[13].

---

[10] Ivi, § 3, p. 6. Per la dottrina sul punto si rimanda, per esempio, a E. Bufano, *I rapporti tra un partito politico, i suoi eletti, gli iscritti: un incedere spezzato tra drittwirkung, argomento costituzionale e fuga dai principi*, in Aa.Vv. *Effettività e drittwirkung nelle discipline di settore. Diritti civili, diritti sociali, diritto al cibo e alla sicurezza alimentare*, Pisa, 2017, 189 ss.; H.C. Nipperdey, *Diritti fondamentali e diritto privato*, in P. Femia (a cura di), *Drittwirkung: principi costituzionali e rapporti tra privati*, Napoli, 2018, 53 ss. In una prospettiva più specifica si leggano per tutti F. Ferraro, *Vecchi e nuovi problemi in tema di efficacia diretta orizzontale della Carta*, in *federalismi.it*, 10, 2019, 2 ss.; O. Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in V. Piccone – O. Pollicino (a cura di), *L'applicazione giudiziale della Carta dei diritti*, Napoli, 2018, 47 ss.

[11] In senso analogo, ma in una prospettiva più ampia, si rinvia a K. Ladeur, *La Drittwirkung dei diritti fondamentali nel diritto privato. "Diritto privato costituzionale" come diritto delle collisioni*, in P. Femia (a cura di), *Drittwirkung: principi costituzionali e rapporti tra privati*, Napoli, 2018, 231 ss.; M. Hunt, *The "Horizontal Effect" of the Human Rights Act*, in *Public Law*, 1, 1998, 423 ss.; S. Gardbaum, *The "Horizontal Effect" of Constitutional Rights*, in *Michigan Law Review*, 2, 2003, 388 ss.; M. Tushnet, *The Issue of State Action/Horizontal Effect in Comparative Constitutional Law*, in *International Journal of Constitutional Law*, 2003, 79 ss.; D. Gallo, *L'efficacia diretta del diritto dell'Unione europea negli ordinamenti nazionali*, Milano, 2018.

[12] R. Alexy, *Teoria dei diritti fondamentali*, Bologna, 2012, 554 ss.; A. Ianni, *L'incidenza della Costituzione sui rapporti privati. Sul divieto di accesso agli stadi il Bundesverfassungsgericht torna ad arbitrare la partita della Drittwirkung*, in *DPCE Online*, 2018, 799 ss.; M. Kumm, *Who is Afraid of the Total Constitution? Constitutional Rights as Principles and the Constitutionalization of Private Law*, in *German Law Journal*, 4, 2006, 341 ss.; S. Haberl, *Antidiscriminazione e stato liberale di diritto. Lo sviluppo della tutela antidiscriminatoria nel diritto tedesco dei contratti*, in *Rivista trimestrale di diritto e procedura civile*, 2009, 233 ss.; A. Zoppini, *Il diritto privato e le "libertà fondamentali" dell'unione europea (principi^ e problemi della drittwirkung nel mercato unico)*, in *Rivista di Diritto civile*, 2016, 712 ss.

[13] Si veda Trib. Roma, ord. 12 dicembre 2019, cit., § 3, p. 6. In proposito, tra i commentatori si è parlato di una sorta di "appropriazione della Costituzione da parte di soggetti privati o impolitici" e di "costituzionalismo civile o societario". Così esemplarmente G. Teubner, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, Roma, 2005, 105 ss. e R. Dworkin, *Foreword*, in I. Hare – J. Weinstein (a cura di), *Extreme Speech and Democracy*, Oxford, 2009, V ss.

3. Lo spazio pubblico costituzionale nell'era dei *social network*

In questo scenario, lo spazio pubblico si dilata considerevolmente fino a inglobare quegli attori privati che, in virtù di una loro posizione di fatto, incidono sull'esercizio dei diritti fondamentali. In maniera del tutto simmetrica, le garanzie costituzionali si espandono, democratizzando la regolazione privatistica della rete. Anche alle piattaforme *social* potranno così estendersi le considerazioni che hanno tradizionalmente caratterizzato il sistema democratico, riconoscendo perfino ai movimenti antisistema la facoltà di esprimersi legittimamente nel dibattito pubblico (digitale).

In effetti, il combinato disposto degli articoli 18, 21 e 49 della Costituzione – unitamente a quanto prescritto dalla XII disposizione transitoria e finale – offre una panoramica piuttosto eloquente circa i rapporti che l'Assemblea Costituente ha inteso instaurare nei confronti degli interlocutori politici, che non si riconoscono nei valori democratici e, più specificamente, nei riguardi di quei partiti che si ispirano palesemente agli ideali del Ventennio[14].

Pur nel fondato timore che la proclamazione delle libertà civili potesse condurre ad una legittimazione dei fascisti, i Padri fondatori tratteggiarono ugualmente un agone pubblico basato sulle regole di una democrazia aperta, che affermasse i propri valori caratteristici in modo tollerante, garantendo il dissenso. L'impianto complessivo della Costituzione manifesta una fiducia, quasi incondizionata, nel metodo democratico, inteso come strumento principe del dibattito politico, in grado di includere pacificamente nel confronto dialettico anche i c.d. "nemici della libertà" [15]. Più precisamente, il dettato costituzionale può ritenersi dominato dal tentativo di lungo periodo di realizzare un sistema sociale inclusivo, all'interno del quale potesse competere anche chi, avversando i contenuti valoriali del nuovo assetto normativo, ne accettasse comunque i meccanismi procedurali generali: una volta esauritasi l'emergenza storica, che imponeva di condannare, anche in termini simbolici, il regime fascista, i movimenti eversivi avrebbero dovuto essere reintegrati, senza negare loro il diritto di esistere e svilupparsi[16].

---

[14] In questa prospettiva si confrontino P. Calamandrei, *L'avvenire dei diritti di libertà*, Firenze, 1946, XII ss.; G.E. Vigevani, *Radici della Costituzione e repressione della negazione della Shoah*, in *rivistaaic.it*, 4, 2014, 14 ss.; A. Pace, *Problematica delle libertà costituzionali*, Padova, 1988, vol. II, 357 ss.; G. DeMuro, *Il dibattito sui partiti: per un diritto individuale di partecipazione politica*, in *Quaderni costituzionali*, 2008, 144 ss.; E. Rossi, *La democrazia interna nei partiti politici*, in *rivistaaic.it*, 1, 2011, 8 ss.

[15] Secondo C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958, 51 «il prezzo dell'interpretazione del dovere di fedeltà alla Repubblica quale fedeltà a una verità è quello di trasformare lo Stato stesso in una chiesa, con i suoi dommi da garantire contro gli infedeli. Questa identificazione però già inesatta in sé, è specificamente condannata proprio dalla solenne proclamazione della libertà di manifestazione del pensiero». In una prospettiva analoga, S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, 211 ss. e A. Pace, *Delimitazione della garanzia costituzionale: esclusione del "subiettivamente" falso. Ancora sul fondamento e sui limiti del c.d. diritto di mentire come aspetto del diritto di difendersi in giudizio*, in A. Pace – M. Manetti, *Commentario della Costituzione. Art. 21. Rapporti civili. La libertà di manifestazione del proprio pensiero*, Bologna, 2006, 89 ss.

[16] Commissione per la Costituzione, Prima Sottocommissione, Seduta del 26 settembre 1946. La discussione si concentrò sulla possibilità di ammettere il sequestro preventivo degli stampati e di circoscriverlo ai soli reati "non politici". Al riguardo, il Deputato liberale Lucifero d'Aprigliano manifestò

In tale logica, il rafforzamento del metodo democratico, come criterio di organizzazione della competizione elettorale, ha storicamente rappresentato una garanzia giuridica, tesa a salvaguardare le caratteristiche ideologiche del nuovo assetto repubblicano. Coerentemente con questo impianto, i contenuti espressi dai singoli partiti sono sempre stati recessivi rispetto a un'accettazione condivisa delle regole del gioco[17]. Fin dall'inizio, l'art. 49 Cost. ha concepito le associazioni politiche come ordinamenti spontanei, originari e volontari e in questo modo ha ridotto i margini di manovra del legislatore – e a maggior ragione degli operatori privati – che potrà indicare alcuni requisiti minimi di democraticità, ma non potrà mai determinare le scelte ideologiche e le opzioni organizzative, che caratterizzano l'identità profonda di un movimento[18].

Nella prospettiva del Costituente, dunque, la preoccupazione per un ritorno al più recente passato totalitario avrebbe dovuto essere scongiurata, innanzitutto, sul terreno del confronto dialettico e dell'educazione civica[19]. Ed è proprio in questa logica che la disciplina dei partiti si armonizza e si raccorda con il dettato dell'art. 21 della Costituzione. I principi di pace, tolleranza, democrazia, libertà e uguaglianza, che fondano ancora oggi il nostro ordinamento non furono codificati in limiti specifici alla manife-

la preoccupazione che un simile strumento potesse essere impiegato per reprimere arbitrariamente le condotte di «scrittori d'avanguardia, non solo nel campo culturale, considerati ribelli rivoluzionari o che invitano al disordine». La soluzione accolta in quella sede e poi confermata anche dall'Assemblea, con l'ammissibilità del sequestro solo a seguito di atto motivato da parte dell'autorità giudiziaria nel caso di delitti per i quali la legge sulla stampa espressamente lo autorizzi, fu senza dubbio influenzata dal timore che potessero ritornare nel corpo sociale i germi del Fascismo. Così, Lelio Basso affermava che la preoccupazione fondamentale dovesse essere la difesa della democrazia e della Repubblica e quindi, in presenza di giornali neofascisti, invocava una norma costituzionale che consentisse di non pubblicare tali giornali. Subito dopo, tuttavia, egli stesso riconosceva che, una volta superato il momento eccezionale, questa norma potesse presentare aspetti di pericolosità rispetto alla libertà di opinione e dunque dovesse essere abbandonata.

[17] Per una ricostruzione del concetto di "metodo democratico" nella Costituzione si vedano tra i numerosissimi contributi I. Pellizzone, *Organizzazione e funzioni dei partiti: quale democrazia interna?*, in *gruppodipisa.it,*, 2, 2019, 198 ss.; A. Barbera., *La democrazia "dei" e "nei" partiti tra rappresentanza e governabilità*, in S. Merlini (a cura di), *La democrazia dei partiti e la democrazia nei partiti*, Firenze, 2009, 231 ss.; M. Rubechi, *Meno partiti, tutti democratici*, in A. Barbera – G. Guzzetta (a cura di), *Il governo dei cittadini*, Rubbettino, 2007, 691 ss.; L. Carlassare, *Rappresentanza politica e partiti tra pubblico e privato*, in F. Mannella (a cura di), *Unità della scienza giuridica. Problemi e prospettive. Giornata di studi in onore di Margherita Raveraira*, Napoli 2016, 38 ss.; G. Amato, *Nota per una legge sui partiti in attuazione dell'art. 49 Cost.*, in *Rassegna parlamentare*, 4, 2012, 5 ss.; S. Gambino, *Una rilettura dell'art. 49 cost.: la democrazia dei partiti e la democrazia nei partiti*, in Aa.Vv., *Studi in onore di Fausto Cuocolo*, Milano, 2005, 481 ss.; C. Pinelli, *I partiti nel nuovo sistema italiano: forme della democrazia o strumenti di leader?*, in *astrid-online.it*, 1, 2009; *passim* M. Perini, *La democrazia nell'organizzazione interna dei partiti politici italiani*, Milano, 2018.

[18] Cfr. Commissione per la Costituzione, Prima Sottocommissione, Seduta del 19 novembre 1946. Togliatti preoccupato per una possibile esclusione dalla vita politica del Partito Comunista, che adottava un fermo centralismo, si oppose con successo alla proposta presentata dagli Onorevoli Merlin e Mancini, che prospettarono un controllo sull'organizzazione dei movimenti politici e sul rispetto da parte delle relative dirigenze della dignità e della personalità degli iscritti, secondo i principî costituzionali di libertà e uguaglianza.

[19] Per una prima panoramica sul punto, si leggano *ex plurimis* i contributi di A. Cardini, *I partiti e la Costituente*, in *Studi senesi*, 3, 2008, 381 ss.; G. Rizzoni, *Commento all'art. 49 Cost.*, in R. Bifulco – A. Celotto – M. Olivetti (a cura di), *Commentario alla Costituzione*, vol. I, Torino, 2006, 981 ss.; S. Bartole, voce *Partiti politici*, in *Digesto delle discipline pubblicistiche*, Aggiornamento, Torino, 2000, 398 ss.; E. Rossi, *I partiti politici*, Roma-Bari, 2007, 35 ss.; A. Ruggeri, *Note minime in tema di democrazia interna dei partiti politici*, in Aa.Vv., *Studi in onore di Aldo Loiodice*, vol. I, Bari, 2013, 121 ss.

stazione del pensiero, né portarono all'introduzione di vincoli legati alla tutela dell'ordine pubblico[20]. In altri termini, anche nella disciplina della libertà di pensiero venne rigettata qualsiasi tentazione di richiedere ai cittadini una fedeltà alla Repubblica, da intendere come obbligo per i singoli e per le associazioni di aderire in maniera acritica alle concezioni della Carta fondamentale.

Per certi versi, si può perfino ritenere che la Costituzione abbia inteso manifestare una sorta di fiducia antropologica nei cittadini che votano e si esprimono all'interno del contesto democratico: i partiti potranno organizzarsi autonomamente, proponendo ai rispettivi gruppi di riferimento le idee che ritengono più convincenti, ma gli elettori prediligeranno *naturaliter* quei movimenti realmente rappresentativi, che incarano cioè i valori democratici in linea con il nuovo assetto repubblicano. Se un partito avanza soluzioni eversive, patrocina una visione autoritaria della società oppure propone programmi in aperto contrasto con la cultura costituzionale, ricorrendo ad un linguaggio imbarbarito, violento, razzista e discriminatorio, la sanzione, prima o poi, sarà chiara e netta: la perdita di consenso politico, il deflusso degli elettori, l'indebolimento del partito stesso come organizzazione e, infine, la sua scomparsa dalla scena istituzionale[21].

Nella visione più profonda – e forse anche più aulica – del Costituente si situa, allora, la consapevolezza che perfino l'ideologia fascista si combatta con un sistema dotato di adeguati pesi e contrappesi, con un Parlamento libero di discutere e con una stampa indipendente, ma mai con la repressione del dissenso in quanto tale[22]. In tal modo, la Costituzione recupera una larga parte delle radici più moderne dell'illuminismo: crede fermamente negli uomini, nella loro capacità di perseguire un progresso morale e materiale attraverso l'utilizzo della ragione e riflette queste convinzioni nelle disposizioni che disciplinano la partecipazione dei cittadini alla vita pubblica[23].

---

[20] In questo senso si consulti P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 229, il quale non esclude neppure il falso soggettivo dalla protezione dell'art. 21. Similmente, si leggano pure P. Costanzo, *Non c'è nulla come il diffuso consenso per smuovere lo spirito di contraddizione*, in *federalismi.it*, 1, 2016, 1 ss. e M. Manetti, *I limiti oggettivi: l'ordine pubblico nelle democrazie pluralistiche*, in A. Pace – M. Manetti (a cura di), *Commentario della Costituzione. Art. 21. Rapporti civili. La libertà di manifestazione del proprio pensiero*, Bologna, 2006, 231 ss.

[21] Rispetto allo spirito che animò la stesura di questa disposizione si veda *ex multis* G. Pasquino, *Commento all'art. 49 della Costituzione*, in G. Branca – A. Pizzorusso (a cura di), *Commentario della Costituzione. Articoli 48-52. Rapporti politici*, Bologna-Roma, 1992, 7 ss.

[22] Più in generale, sul complesso rapporto tra democrazia e verità nei sistemi pluralisti, anche con riguardo alla criminalizzazione delle opinioni eversive o antisistema, si vedano, per tutti, P. Häberle, *Diritto e verità*, Torino, 2000, 93 ss.; G.E. Vigevani, *L'influenza delle leggi razziali nell'elaborazione della Costituzione repubblicana*, in *Nomos. Le attualità nel diritto*, 2009, 91 ss.; B. Pezzini, *Attualità della Resistenza: la matrice antifascista della Costituzione Repubblicana*, in B. Pezzini – S. Rossi (a cura di), *I giuristi e la Resistenza. Una biografia intellettuale del Paese*, Milano, 2016, 219 ss.; F. Blando, *Movimenti neofascisti e difesa della democrazia*, in *costituzionalismo.it*, 1, 2014, 1 ss.; D.J. Schaller, *From the Editors: Judges and Politicians as Historians?*, in *Journal of Genocide Research*, 1, 2007, 2 ss.

[23] Così *ex multis* J.S. Mill, *On liberty* (1859), trad.it. *Saggio sulla libertà*, Milano, 2002, 46, «impedire l'espressione di un'opinione è un crimine particolare, perché significa derubare la razza umana, i posteri altrettanto che i vivi, coloro che dall'opinione dissentono ancor più di chi la condivide: se l'opinione è giusta, sono privati dell'opportunità di passare dall'errore alla verità; se è sbagliata, perdono un beneficio quasi altrettanto grande, la percezione più chiara e viva della verità, fatta risaltare dal contrasto con l'errore». J. Milton, A*reopagitica, A speech of Mr John Milton for the liberty of unlicensed printing to the Parliament of England* (1644), trad. it. *Areopagitica. Discorso per la libertà di stampa*, Milano, 1998, 32; B. Constant, *De la liberté des Anciens comparée à celle des Modernes* (1819), trad. it. *La libertà degli antichi paragonata a quella dei*

4. Il divieto di «riorganizzazione del disciolto partito fascista» nella teoria e nella prassi

Non pare estranea a questo progetto complessivo neppure la stesura della XII disposizione transitoria e finale, che – come noto – vieta «la riorganizzazione, sotto qualsiasi forma, del disciolto partito fascista»[24]. Sebbene, infatti, in alcuni momenti del secondo dopoguerra abbia dominato una visione della democrazia, per così dire, più militante, tesa ad escludere dal dibattito pubblico chi si opponesse ai valori costituzionali, la tendenza prevalente si è attestata quasi sempre verso un radicale rifiuto del diritto sanzionatorio per reprimere le condotte di quei movimenti, che avversassero, anche apertamente, il nuovo sistema repubblicano[25]. Per dirla con le parole della Corte, la portata precettiva dalla XII disposizione è stata tradizionalmente stabilita con riferimento esclusivo alle precise esigenze storico-politiche, che ispirarono l'adozione di quella stessa norma[26]. Il divieto di ricostituzione del partito fascista non ha quindi per oggetto un concetto vago e indefinito, capace di portare ad una trasformazione attiva dell'ordine democratico, ma si concentra su un fatto storicamente determinato, coincidente con quel movimento politico «che prese corpo in Italia dal 1919 fino al 25 luglio 1943 e che si chiamò Fascismo»[27].

Ci si trova, pertanto, al cospetto di un principio generale, che intende segnare una netta cesura rispetto al passato piuttosto che realizzare una preclusione *pro futuro*, volta a restringere lo spazio democratico a disposizione dei movimenti considerati estremisti[28]. Detto altrimenti, non si tratta di una norma che definisce la spettanza della libertà di parola o che limita la manifestazione del pensiero in un contesto pubblico – reale o digitale – ma di una prescrizione, diretta a determinare chi possa intervenire nella competizione elettorale democratica: affinché la partecipazione attiva dei cittadini

moderni, Macerata, 2004.

[24] La falsità, l'inesattezza storica o l'aspirazione sovversiva di alcune opinioni non pare di per sé sufficiente a rendere costituzionalmente inammissibili le correlative manifestazioni pubbliche come "pensieri puri", ammessi al dibattito e auspicabilmente alla confutazione. Non deve infatti dimenticarsi che l'art. 21 Cost. copre tanto la diffusione di opinioni, quanto la pura narrazione di un fatto, vero o falso che sia. Così *passim* S. Ceccanti, *Le democrazie protette e semi-protette dopo la terza ondata: da eccezione a regola*, Torino, 2004; G.E. Vigevani, *Associazione (libertà di)*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, 481 ss.; A. Longo, *I simboli (del Fascismo) e il tempo (della Costituzione): pochi spunti suggeriti dalla sentenza della Corte di Cassazione n. 37577 del 2014*, in *osservatoriocostituzionale.it*, 10, 2014, 1 ss.

[25] Per una più attenta ricostruzione delle tendenze legislative e giurisprudenziali in materia si legga G.E. Vigevani, *Origine e attualità del dibattito sulla XII disposizione finale della Costituzione: i limiti della tutela della democrazia*, in *questa Rivista*, 1, 2019, 6 ss.

[26] Così C. cost. sent. 74/1958.

[27] Cfr. Commissione per la Costituzione, Prima Sottocommissione, Seduta del 19 novembre 1946, e, in particolare, il confronto che coinvolse gli Onorevoli Togliatti, Basso e Dossetti. Per una ricostruzione di quel dibattito si rinvia a V. Crisafulli, *I partiti nella Costituzione*, in Aa.Vv., *Studi per il XX anniversario dell'Assemblea Costituente. Le libertà civili e politiche*, vol. II, Firenze, 1969, 112 ss.

[28] In questa prospettiva, anche per una riattualizzazione della XII disposizione si rimanda a L. Picotti, *Istigazione e propaganda della discriminazione razziale fra offesa dei diritti fondamentali della persona e libertà di manifestazione del pensiero*, in Aa.Vv., *Discriminazione razziale, xenofobia, odio religioso. Diritti fondamentali e tutela penale*, Padova 2006, 117 ss.; V. Zagrebelsky, *I delitti contro l'ordine pubblico*, in F. Bricola – V. Zagrebelsky (a cura di), *Giurisprudenza sistematica di diritto penale*, Torino 1996, 537 ss.; P. Caretti, *I diritti fondamentali, Libertà e Diritti sociali*, Torino, 2011, 372 ss.

possa fattivamente concretizzarsi, è necessario che il dibattito pubblico sia libero e che tutte le idee, anche quelle infondate, astrattamente pericolose o addirittura palesemente false possano manifestarsi senza restrizioni[29].

Pur nella legittima aspirazione di difendere la democrazia contro possibili degenerazioni del pluralismo, lo scopo ultimo della XII disposizione, da leggersi in congiunzione con gli artt. 18 e 49 Cost., resta comunque quello di garantire il più ampio confronto delle idee, nel quadro di una società non omogenea. Nel complesso, quindi, emerge la ferma volontà dei Padri fondatori di dare vita – coraggiosamente, data anche la temperie storica – a un ordinamento capace di affermare i suoi valori antifascisti attraverso la dialettica politica con i propri antagonisti[30].

Verosimilmente, le ambizioni dei Costituenti sono state in parte disattese dal legislatore e, più di recente, dai gestori privati delle reti *social*, i quali hanno surrettiziamente circoscritto la libertà di manifestazione del pensiero dei partiti antisistema, eversivi o comunque non allineati. Sovente, cioè, è prevalsa quella logica congiunturale, basata sull'emergenza post-bellica, che la stessa Assemblea Costituente intendeva gradualmente abbandonare[31]. Sembra però di potere sostenere che, sebbene a fronte di alcune applicazioni ondivaghe, gli indirizzi giurisprudenziali maggioritari abbiano ridotto la portata sanzionatoria delle previsioni legislative. Da questo punto di vista, la legge di attuazione della XII disposizione non ha ostacolato l'inclusione nell'arco costituzionale del Movimento Sociale Italiano, trovando applicazione una sola volta, allorché, nel 1973, fu sciolta la formazione di estrema destra Ordine Nuovo[32]. I medesimi reati di opinione, previsti come corollario diretto al divieto di riorganizzazione del partito

[29] Al riguardo si consultino N. Bobbio, *Dal fascismo alla democrazia*, Milano, 1997, 61 ss.; A. Perduca, *Fascismo II) Disposizioni penali sul fascismo*, in *Enciclopedia giuridica Treccani*, vol. XIV, Roma 1989, 5 ss.; L. Diotallevi, *Sulla permanente "attualità" del reato di "manifestazioni fasciste" ex art. 5 "Legge Scelba*, in *Giurisprudenza costituzionale*, 2014, 4801 ss.

[30] Si pensi ad esempio alle previsioni contenute nella Legge fondamentale tedesca del 1949. In proposito si vedano anche A. Alesiani, *I reati di opinione. Una rilettura in chiave costituzionale*, Milano, 2006, 141 ss.; P. Barile – U. De Siervo, *Sanzioni contro il fascismo ed il neofascismo*, in *Novissimo digesto italiano*, vol. XVI, 1959, 541 ss.; G. De Vero, voce *Istigazione a delinquere e a disobbedire alle leggi*, in *Digesto delle discipline penalistiche*, vol. VII, Torino, 1993, 233.

[31] In particolare, questa impostazione protezionistica si è manifestata, dapprima, con la legge n. 645 del 1952 (c.d. "legge Scelba"), che ha introdotto, tra l'altro, il reato di apologia del fascismo; in seguito, con la legge n. 962 del 1967, che punisce l'apologia di genocidio; con la legge n. 654 del 1975, che criminalizza la propaganda razzista e l'istigazione a commettere atti discriminatori, e, da ultimo, con la legge n. 205 del 1993 (c.d. "legge Mancino"). Per un commento si veda nonché P. Caretti, *Manifestazione del pensiero, reati di apologia e di istigazione: un vecchio tema che torna d'attualità in una società multietnica*, in Aa.Vv., *Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile*, Padova, 2003, 121, secondo cui «qualora si decidesse di sanzionare anche la mera diffusione di idee razziste, indipendentemente dall'esigenza di ricostruire un nesso tra istigazione e azione successiva, la penalizzazione del pensiero razzista non si tradurrebbe in una limitazione alla libertà di manifestazione del pensiero, quanto in una sua totale negazione, in nome di un principio, ritenuto non mediabile con altri interessi diversi sia pure costituzionalmente tutelati».

[32] A riprova di una certa oscillazione degli indirizzi giurisprudenziali, si vedano i recenti pronunciamenti del Tribunale di Milano in merito alla sanzionabilità del "saluto romano". Così Trib. Milano, sez. III pen., 27 novembre 2018, n. 13843 e n. 2488. Per un commento si vedano rispettivamente A. Nocera, *Manifestazioni fasciste e apologia del fascismo tra attualità e nuove prospettive incriminatrici*, in *penalecontemporaneo.it*, 9 maggio 2018 e S. Galluccio, *Il saluto fascista è reato? L'attuale panorama normativo e giurisprudenziale ricostruito dal Tribunale di Milano in una sentenza di condanna*, in *penalecontemporaneo.it*, 29 aprile 2019.

fascista, sono stati puntualmente delimitati dal giudice costituzionale, che ha ritenuto punibili unicamente le condotte apologetiche realizzate con modalità tali da risultare potenzialmente in grado di ricostituire il PNF[33]. Nell'esegesi di queste disposizioni, dunque, assume rilievo dirimente il requisito della violenza come strumento di lotta politica, che arrivi a ledere i valori della dignità umana e dell'eguaglianza. *Ergo*, affinché un partito sia bandito dal sistema democratico – e di conseguenza anche da una rete *social* – non è sufficiente un'ideologia ultra-conservatrice o genericamente contraria ai valori della Costituzione[34].

Certo, anche gli ordinamenti democratici e pluralisti tendono all'unità politica della propria compagine sociale e delineano una comunità, che si struttura in modo ordinato attorno ad alcune finalità fondamentali da riaffermare e proteggere quotidianamente, il punto cruciale, però, sta nella scelta degli strumenti atti a garantire quel sistema di riferimento, senza rinunciare a un'integrazione politica diversificata: non è attraverso la criminalizzazione delle opinioni o, peggio ancora, tramite un potere censorio affidato ai nuovi "*giganti di silicio*", che lo Stato costituzionale può mantenere le promesse di libertà ed eguaglianza su cui è stato faticosamente edificato[35]. Affidare alle regole delle piattaforme *internet* il ruolo di unico "custode" delle posizioni democraticamente ortodosse e quindi accettabili significa ingerirsi in ambiti strutturalmente riservati alla politica e alla società civile, ragion per cui eventuali restrizioni alla diffusione o alla propaganda di idee antisistema dovranno provenire unicamente da norme legislative e dovranno giustificarsi solamente in ragione della necessità di salvaguardare altri valori di rango costituzionale[36].

Questo perché, come detto, la nostra Costituzione accetta con fiducia il rischio della libertà, scommettendo a favore di una democrazia aperta, che includa progressivamente anche le culture e le forze politiche ad essa ostili. La libertà di poter manifestare liberamente qualsiasi tipo di opinione attraverso la rete, infatti, non giova solamente a chi si faccia promotore di opinioni estreme, ma beneficia altresì chi si deve confrontare con quelle idee eversive, violente o antistoriche, perché induce ad approfondire, ampliare e, se il caso, a riconsiderare il proprio punto di vista, affinché prevalga dialetticamente la posizione più ragionevole. Di fronte alla pervicace negazione di valori democraticamente condivisi occorrerà, cioè, rafforzare la propria impostazione, suffragandola con dati di fatto e articolandola in maniera più convincente; solo in tal modo, si svilupperanno utilmente gli anticorpi sociali necessari per espungere dal dibattito pubblico le visioni più estreme, evidenziando la loro fallacia logica, la loro

[33] Cfr. *ex plurimis*, C. cost., sent. 1/1957; C. cost., sent. 74/1958, C. cost., sent. 15/1973.

[34] In ordine al requisito della violenza come strumento di lotta politica capace di giustificare lo scioglimento di un partito si leggano L. Basso, *Considerazioni sull'art. 49 della Costituzione*, in Aa.Vv., *Indagine sul partito politico. La regolazione legislativa*, vol. I, Milano 1966, 141 ss. e C.E. Traverso, *La genesi storico-politica della disciplina dei partiti nella Costituzione italiana*, in *Il Politico*, 2, 1968, 281 ss. Più di recente si veda anche S. Bonfiglio, *L'articolo 49 della Costituzione e la regolazione del partito politico: "rilettura" o "incompiuta" costituzionale?*, in *Nomos. Le attualità nel diritto*, 2, 2017.

[35] S. Rodota*, Una Costituzione per Internet?*, in *Politica del diritto*, 3, 2010, 337 ss.

[36] Sul punto si vedano secondo prospettive diverse C. Caruso, *La libertà di espressione presa sul serio. Casa pound c. Facebook, atto I*, in *sidiblog.org*, 20 gennaio 2020; A. Di Giovine, *I confini della libertà di manifestazione del pensiero*, Milano 1988, 96 ss.; G. Marini, voce *Ordine pubblico (delitti contro l')*, in *Novissimo digesto italiano*, Appendice V, Torino 1993, 233 ss.

pericolosità e la loro inadeguatezza.
Proprio per questo, anche i *social network* sono chiamati a garantire orizzontalmente la diffusione di tutte le idee, senza esercitare censure o reticenze di sorta, ma concorrendo a realizzare la democraticità complessiva del sistema.

5. *Quot capita, tot sententiae* ... una proposta

La decisione che definisce la controversia tra Facebook e Casa-Pound sembra dunque cogliere perfettamente le problematiche giuspubblicistiche sottese al rapporto tra associazioni politiche e piattaforme *social*, riaffermando con assoluta decisione i valori di una democrazia inclusiva, anche e soprattutto di fronte a messaggi particolarmente odiosi, che si collocano ai confini più estremi della libertà di espressione. Ciò nonostante, l'ordinanza presenta comunque alcune criticità, legate, da una parte, ad una regolamentazione giurisdizionale degli spazi comunicativi presenti in rete e, dall'altra, ai rapporti che il nostro ordinamento instaura con altri sistemi di protezione dei diritti.
E in effetti, questa soluzione è stata sostanzialmente riformata nel suo impianto di fondo dallo stesso Tribunale di Roma[37]. Di recente, infatti, la Sezione per i diritti della persona e l'immigrazione ha ritenuto pienamente legittima la cancellazione del profilo di Forza Nuova, sulla base di motivazioni tese a valorizzare tanto la natura contrattuale del rapporto che lega Facebook ai propri iscritti quanto la dimensione sovranazionale delle violazioni.
Con riguardo al primo aspetto, la nuova ordinanza valorizza la dimensione privatistica del negozio stipulato tra i *social network* e i loro utenti, precisando che le condizioni generali del servizio impegnano il sottoscrittore a non utilizzare la piattaforma per scopi «illegali, ingannevoli, malevoli o discriminatori» e a non pubblicare contenuti che non rispettino «i diritti di terzi o le leggi vigenti», pena la rimozione delle relative pagine. In tale prospettiva, sarebbero pertanto i medesimi "standard della community" – che i fruitori accettano consapevolmente prima di avvalersi di quella rete sociale – a legittimare l'eventuale oscuramento di un *post* da parte del gestore[38]. Imporre autoritativamente i contenuti che Facebook deve veicolare, specie se queste esternazioni violano delle specifiche clausole contrattuali, significa ridurre in maniera drastica l'autonomia negoziale di un soggetto, che, per quanto occupi una posizione del tutto peculiare all'interno dell'ordinamento, è e resta un ente privato: un *social network* rimane pur sempre un'azienda e, come tale, deve poter decidere liberamente cosa rimuovere e cosa ospitare negli ambiti che gestisce. Lo statuto delle società private, insomma, non deve essere confuso con quello del servizio pubblico[39].
Ma vi è di più. I reiterati riferimenti al fascismo, unitamente alla propaganda di opinioni

[37] A settembre 2019, Facebook aveva cancellato decine di profili legati ad associazioni, genericamente ritenute di estrema destra, precisando che «le organizzazioni che diffondono odio o attaccano gli altri sulla base di chi sono non trovano posto su Facebook e Instagram. Candidati e partiti politici, così come tutti gli individui e le organizzazioni presenti su Facebook e Instagram, devono rispettare queste regole, indipendentemente dalla loro ideologia».

[38] Trib. Roma, sez. diritti della persona e immigrazione civile, ord. 24 febbraio 2020, § 2, p. 15.

[39] Circa la distinzione tra gestore privato e servizio pubblico si leggano *ex multis* P. Troiano, *I principi*

discriminatorie nei confronti di rom, migranti, donne e omosessuali – che già di per sé basterebbero per ritenere che Facebook abbia il diritto di risolvere il contratto con gli utenti che amministravano le pagine facenti capo a Forza Nuova – inducono il giudice a ritenere che il *provider* sia, in realtà, gravato dal dovere giuridico di risolvere i contratti[40]. La nuova ordinanza asserisce, infatti, che il contenuto e il tono generale dell'azione politica dell'associazione e delle sue articolazioni rivestano una marcata natura negazionista e che, per questo motivo, contrastino con i valori fondamentali di pace e giustizia, espressi nel Preambolo della Convenzione europea dei diritti dell'uomo[41].
In questa prospettiva, il giudice esclude pure che le condotte assunte da Forza Nuova possano ricadere sotto la protezione dell'articolo 10 CEDU, dal momento che, nell'ampia casistica richiamata dal provvedimento, la libertà di espressione verrebbe impiegata per finalità contrarie alla lettera e allo spirito della Convenzione, frustrando così il contenuto essenziale del diritto e configurando un vero e proprio abuso[42]. I considerevoli rimandi alla giurisprudenza convenzionale e al diritto dell'Unione non solo ampliano il contesto normativo di riferimento, ma inseriscono la decisione nell'alveo di una casistica europea piuttosto consolidata, che, in nome della salvaguardia dei valori trasfusi nei Trattati, ha iniziato ad escludere con enfasi crescente i c.d. "discorsi d'odio" dalla tutela riconosciuta alla libera manifestazione del pensiero, fissando dei limiti contenutistici alle opinioni presenti in rete, a prescindere dalle circostanze del caso concreto[43]. Coerentemente, la pronuncia cerca di evitare che un giudice interno possa costringere Facebook alla pubblicazione di messaggi politici proibiti dalle proprie *policies*, in ragione dei quali sarebbe poi, quasi sicuramente, sanzionato come *provider* del servizio da

generali in materia di informazione e i compiti di servizio pubblico nel settore radiotelevisivo, in A. Frignani – E. Poddighe – V. Zeno Zencovich (a cura di), *La televisione digitale: temi e problemi*, Milano, 2006, 33 ss.; P. Caretti, *Diritto dell'informazione e della comunicazione*, Bologna, 2013, 211 ss.; P. Costanzo – C. Pinelli, *Media, poteri, diritti*, in *Rivista di diritto costituzionale*, 1998, 255 ss.; R. Zaccaria – A. Valastro – E. Albanesi, *Diritto dell'informazione e della comunicazione*, Padova, 2013, 369 ss.; M.R. Allegri, *Informazione e comunicazione nell'ordinamento giuridico italiano*, Torino, 2012, 88 ss.

[40] Cfr. Trib. Roma, ord. 24 febbraio 2020, cit., § 3.1.1, p. 24.

[41] Per una documentata rassegna dei post e dei messaggi pubblicati da Forza Nuova, dalle diverse associazioni collegate al partito e dai suoi aderenti, si rinvia a Trib. Roma, ord. 24 febbraio 2020, § 3.1.1., p. 17 ss.

[42] Con riferimento alla libertà di manifestazione del pensiero così come tutelata dalla CEDU, anche con riguardo all'abuso del diritto si leggano per tutti M. Manetti, *L'incitamento all'odio razziale tra realizzazione dell'eguaglianza e difesa dello Stato*, in AA.VV, *Scritti in onore di Gianni Ferrara*, vol. II, Torino, 2005, 526 ss.; G. Cannie – D. Voorhoof, *The Abuse Clause and Freedom of Expression in the European Human Rights Convention: an Added Value for Democracy and Human Rights Protection?*, in *Netherlands Quarterly of Human Rights*, 1, 2001, 64 ss.; M. Castellaneta, *La repressione del negazionismo e la giurisprudenza della Corte europea dei diritti umani*, in *Diritti umani e diritto internazionale*, 1, 2011, 73 ss.; A Buyse, *The limits of freedom of expression from an abuse of rights perspective. Articles 10 and 17 ECHR*, in E. Brems – J. Gerards (a cura di), *Shaping Rights in the ECHR*, Cambridge, 2014, 189 ss.; R. Post, *Constitutional Domains: Democracy, Community, Management*, Cambridge, 1995; D. Pulitanò, *Di fronte al negazionismo e al discorso d'odio*, in *Diritto penale contemporaneo*, 4, 2015, 1 ss.

[43] Per una panoramica iniziale si rinvia a P. Vidal-Naquet, *Gli assassini della memoria. Saggi sul revisionismo e la shoah*, Roma, 2008; C. Caruso, *L'hate speech a Strasburgo: il pluralismo militante del sistema convenzionale*, in *Quaderni costituzionali*, 2017, 963 ss.; C. Visconti, *Aspetti penalistici del discorso pubblico*, Torino, 2008; V. Manes, *Introduzione. La lunga marcia della Convenzione europea ed i nuovi vincoli per l'ordinamento (e per il giudice) penale interno*, in V. Manes – V. Zagrebelsky (a cura di), *La Convenzione europea dei diritti dell'uomo nell'ordinamento penale italiano*, Milano, 2011, 22 ss.; E. Stradella, *La libertà di espressione politica simbolica e i suoi limiti: tra teorie e prassi*, Torino, 2008.

una Corte sovranazionale[44].

Come è evidente, dietro a queste decisioni si situano due concezioni diametralmente opposte della democrazia e del dibattito pubblico. Da un lato, si colloca la rappresentazione offerta dai giudici europei e dal diritto dell'Unione, che mira a pacificare l'agone politico, prescindendo dallo scopo che le libertà perseguono nei singoli ordinamenti: una democrazia protetta e militante, orientata a conservare il sistema e a preservare la concordia sociale, espungendo le posizioni potenzialmente lesive, disturbanti o, più genericamente, non allineate con i valori fondativi della CEDU e dei Trattati internazionali[45]. Dall'altro, si posiziona, invece, la visione sistematicamente desumibile dalla nostra Carta costituzionale, diretta a salvaguardare al massimo la libertà di manifestazione del pensiero, integrando il dissenso politico e preservando comunque il pluralismo: una democrazia aperta, che accetta con fiducia un modello competitivo, fondato sul conflitto e sull'eterogeneità degli interessi e che scommette sulla capacità di discernimento dei cittadini.

Una volta ponderati accuratamente tutti gli interessi coinvolti, una risposta più convincente per risolvere la questione, armonizzando così anche le necessità provenienti dai diversi sistemi di tutela e riavvicinando le diverse concezioni della democrazia presenti negli ordinamenti europei, potrebbe essere allora quella di procedimentalizzare l'*iter*, che conduce all'oscuramento di una pagina *social*. La predeterminazione di una procedura certa, chiara e trasparente, infatti, salvaguarderebbe i diritti dei singoli e delle associazioni che subiscono la rimozione improvvisa del proprio profilo e ridurrebbe altresì l'attivismo dei giudici, conducendo a soluzioni tendenzialmente più univoche.

Da questo punto di vista, Facebook dovrebbe, in primo luogo, assolvere a tutta una serie di obblighi informativi nei confronti degli utenti, con riguardo precipuo ai contenuti potenzialmente vietati. Secondariamente, occorrerebbe pure garantire ai soggetti sanzionati con l'oscuramento della pagina una sorta di "diritto di difesa", assicurando loro il contraddittorio con gli amministratori della piattaforma, per illustrare le proprie ragioni. In questo modo, si eviterebbe che le reti *social* ricorrano ad una vera e propria censura privata, esercitata in assenza di qualsiasi confronto e ispirata ad una malintesa correttezza espositiva, che potrebbe colpire, indistintamente, tutte le opinioni in quanto tali, solo perché non si conformano alla visione dominante in un dato contesto storico-sociale.

---

[44] Per un esame più accurato della giurisprudenza della Corte EDU, anche con riguardo alla responsabilità del *provider* per contenuti lesivi dei diritti umani si rinvia *ex multis* ai contributi S. Parisi, *Il negazionismo dell'Olocausto e la sconfitta del diritto penale*, in *Quaderni costituzionali*, 2013, 890 ss.; D. Keane, *Attacking Hate Speech under Article 17 of the European Convention on Human Rights*, in *Netherlands Quarterly of Human Rights*, 2007, 641 ss.; 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, 80 ss.; I. Hare, *Extreme Speech under International and Regional Human Rights Standards*, in I. Hare – J. Weinstein (a cura di), *Extreme Speech and Democracy*, Oxford-New York, 2009, 67 ss.; R. Errera, *Freedom of speech in Europe and in the USA*, in G. Nolte (a cura di), *European and U.S. Constitutionalism*, Strasbourg, 2005.

[45] Per una ricostruzione del concetto di democrazia all'interno del sistema CEDU si consultino, ad esempio, C. Vercelli, *Il negazionismo. Storia di una menzogna*, Roma-Bari, 2013; V. Pisanty, *L'irritante questione delle camere a gas*, Milano, 2014, 251 ss.; di A. Ruggeri, *Salvaguardia dei diritti fondamentali ed equilibri istituzionali in un ordinamento "intercostituzionale"*, in *rivistaaic.it*, 3, 2013, 14 ss.; A. Tesauro, *Riflessioni in tema di dignità umana, bilanciamento e propaganda razzista*, Torino, 2013, 83 ss.; D. Di Cesare, *Negare la Shoah. Questioni filosofico-politiche*, in F. Recchia Luciani – L. Patruno (a cura di), *Opporsi al negazionismo. Un dibattito necessario tra filosofi, giuristi e storici*, Genova, 2013, 84 ss.

Media regulation at a distance: video-sharing platforms in AVMS Directive and the future of content regulation*

Lubos Kuklis

Abstract

This article argues that the inclusion of video-sharing platforms in the new version of Audiovisual Media Service Directive, not only extends the scope of media regulation in the EU, but also brings a fundamentally new approach to the content regulation as such. With this approach, EU recognises the inherent difference between more traditional types of media, in which the editorial rights and responsibilities lie with the media themselves, and the platformed social media, in which it is the active user, who is the originator and primary uploader of the content. Following this distinction the new regulation is systemic rather than focusing on individual pieces of content on the platforms, but also recognises the rights of the users, and legislates for more transparency. Although the latter two elements are included in the Directive in only rudimentary form, and they apply only to video content, the proper transposition of these into the national legislations of the EU member states have a real potential for improving the current state of social media governance.

Summary

1. Context. – 2. The new version of AVMSD. – 3. What is video-sharing platform? – 4. The basic principles of VSP regulation. – 5. Conclusions.

Keywords

Audiovisual Media Services Directive - video-sharing platforms - media regulation - content regulation - content moderation

*L'articolo è stato inviato su richiesta della direzione e, pertanto, in conformità all'art. 15 del regolamento della Rivista, non è stato sottoposto a referaggio

1. Context

There is a lot of attention currently paid to the question of how to adjust the current legal framework to address the problems that came with the rise of social media. From the distribution of terroristic content, through mass production and spread of hate speech and disinformation, to the proliferation of problems connected to children well-being, all of these are the cause of great concern to many. Not that these phenomena were not present in society during the analogue media era. But the production possibilities enabled by digital technology and frictionless exchange of information through social media brought these on an entirely new level. So much so, that now there is a widespread fear that the fabric of democratic societies themselves is under threat.

There are many ideas on how to approach these problems, but very few of them, so far, were actually put into practice. The notable exception is the German Network Enforcement Law (NetzDG), that introduced the liability of social media platforms over the hate speech and other illegal content on their services.

Similar initiatives are now in different stages of preparation also in other countries. A lot of interest was generated by the UK Government's Online Harms White Paper, which should serve as a basis for future comprehensive regulation of online content. Another one that is nearing the end of the legislative process, and also is closest to Germany's NetzDG, is so-called "Avia law" in France.

These initiatives, however, do not enjoy unequivocal support. The common criticism levelled against them is that they are disproportionately oriented toward the swift removal of content without creating any safeguards toward their opportunistic enforcement by platforms. This is based on the view, that, designed as they are with strict penalties for non-compliance, these laws strongly incentivise the providers to take-down the content whenever in doubt as to its legality– an outcome that will arguably further drive out marginalised views from the digital public sphere.

In the EU, these questions should be addressed by the so-called Digital Services Act (DSA). Announced by incoming President of the EU Commission von der Leyen, and currently officially existing only as an 8 pages long idea paper, the DSA should replace the current E-Commerce Directive,[1] and presumably alter its liability regime for intermediaries and broaden its scope. Now, both of these changes are a matter of a lot of debating and, given the state of the preparations for this legislation, also a lot of fantastical projections from all sides.

Whatever the final result, DSA will very probably present a fundamental shift in the legal approach to online platforms regulation. The fact is, however, that it still lies in rather distant future.

But there is EU legislation currently in force, Audiovisual Media Service Directive (AVMSD), that addresses some of these problems already, and this legislation is due to be transposed into national legal systems of all EU member states very soon. It

[1] Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

is a new version of the Directive which origins date back to 1989, when it dealt with TV broadcasting only. In 2010 its scope was extended to video-on-demand services, and at the end of 2018, it was widened yet again to so called video-sharing platforms (VSPs).

And it is the Directive's approach toward VSPs that may prove to be part of the regulatory solution for online content more broadly. True, this particular legislation concerns only audiovisual content, and therefore, does not cover all content on social media. With this model, however, as this article tries to explain, we are witnessing a new approach to content regulation that, if successful, can later be extended to other areas. That is why it warrants close inspection. And ideally, this should be done before the transposition of the provisions in question into national legislative frameworks.

This article will focus on the basic principles of VSP regulation in AVMSD and why some of these principles are creating a new kind of content regulation. It will also try to assess the potential of this framework in addressing two prominent issues currently present in the area of digital media governance, namely that of adequate protection of the rights and interests of the users, and the problem of transparency in content moderation.

2. The new version of AVMSD

The extension of the scope of AVMSD to the regulation of video-sharing platforms, is the first time that legislation on an EU level has addressed specific content regulation on any kind of digital platform. In the context of a changing mood toward big tech, the provisions of the Directive may prove to be very influential. Either because its implementation would lead to a more satisfactory rearrangement of the current situation in the EU media environment, or because of some tough lessons learned.

From the broader perspective, the approach that the new AVMSD takes is in line with the ideas voiced by many of those thinking and writing about the potential content regulation on platforms.

Its approach to content regulation is systemic rather than focusing on individual pieces of content on the platform, it recognises the rights of the users, including explicitly mentioning the protection of freedom of expression of those that upload content, and it legislates for transparency.

And it is these three elements of VSP regulation that this article is primarily focusing on. On the systemic approach because it is an entirely new element in the EU media regulation. On the latter two elements, rights of the users and transparency, because, while fairly rudimentary in their phrasing in the Directive, these may prove to be crucial in the development of a new approach to content regulation on digital platforms. Indeed, to achieve this, it would take a certain regulatory angle to interpret the provisions of the Directive. This article is looking at the VSP regulation in AVMSD precisely from this perspective. It tries to highlight those parts that, if given priority by legislators in the member states, may help in improving the current workings of the media environment in digital space.

3. What is video-sharing platform?

The inclusion of video-sharing platforms into the scope of AVMSD has been debated. From its introduction, the Directive has laid down the regulation for audiovisual media with a clearly defined editorial control over the content they were providing. With video-sharing platforms, however, things are markedly different.

As defined by AVMSD, video-sharing platform is a service devoted to the provision of programmes and user-generated videos for which its provider does not have editorial responsibility, but which the provider is organising – automatically or otherwise. This disconnection between the provider and editorial responsibilities is a clear sign that with this type of service, we are not dealing with media in the traditional sense. The ultimate example of such a service is Google's YouTube, where the provision of videos is its primary function.[2] But AVMSD also introduces regulation for services which character may not be that clear-cut.

The Directive's definition introduces two alternative criteria on which the legal recognition of VSP hinges – that the provision of audiovisual content[3] is either the principal purpose of the service (or of its dissociable section – Facebook Watch would be a good example) or its essential functionality. While the former, as was already stated, is fairly uncontroversial and clearly points to prototypical VSPs like YouTube, it is the latter that will bear the most scrutiny in borderline cases.

From the beginning, one of the most controversial questions was whether VSP regulation in AVMSD would also cover video content on social media. Not only does the notion not appear in the first draft proposal by the Commission, but one of the (later deleted) recitals explicitly excluded it.[4]

This approach betrays a very cautious stance initially taken by the Commission towards the regulation of social media in general. Its co-legislators were not as timid, and the final version is bolder in its wording.[5]

This does not mean, however, that the extent to which social media providers fall

[2] Other examples would be Vimeo, or French service Dailymotion.

[3] This is, of course, a gross simplification for the sake of readability. The whole paragraph reads: «video-sharing platform service' means a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the video-sharing platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks within the meaning of point (a) of Article 2 of Directive 2002/21/EC and the organisation of which is determined by the video-sharing platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing».

[4] The wording of the recital 3 of the proposal: «Social media services are not included, except if they provide a service that falls under the definition of a video-sharing platform». Proposal for a Directive of the European Parliament and of the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities».

[5] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

within AVMSD has clear boundaries. The interlocutors during the legislative process understood that this is not the case,[6] and obliged the Commission in consultation with the responsible member states' authorities gathered in the Contact Committee to prepare guidelines to help to clarify the definition.[7]

4. The basic principles of VSP regulation

The main aim of this article is to examine the principles that make an AVMSD approach to VSP regulation novel. There are of course other principles, that will shape the implementation and, later on, practical application of the VSP regulation – like country of origin principle or minimum harmonisation regime – but as they do not constitute a conceptual change, but are rather a continuation of the older media regulation paradigm, we won't deal with them here.

So, the principles that are employed in media regulation on the EU level for the first time are:[8] a) a systemic approach; b) transparency; c) the active user as a regulatory actor. Now they will be discussed in turn.

4.1. A systemic approach

Content regulation on media platforms is a widely discussed topic nowadays. Until fairly recently the consensus seemed to have converged on the idea that, from a legal perspective, social media are mere communication intermediaries and, as such, do not possess any substantial editorial powers and, therefore, should not hold editorial responsibility for the content they carry. Starting with the famous Section 230 of the US Communication Decency Act, followed in the EU by the provisions of E-Commerce Directive, this notion seemed to be firmly established in the law of democratic countries.

However, the strong impact of these platforms on society and the fact that the editorial influence the platform providers exercise over the content posted by their users is not negligible, have prompted many to question the validity of these liability exemptions, mainly for potentially dangerous content like hate speech or so-called terrorist content.[9]

Still, the content on the platforms is mainly created by their users and not the platforms themselves. When it comes to editorial competences of the platform providers,

[6] Recital 3b in the General Approach of the Council of the EU, adopted May 2017 in *eur-lex.europa.eu*.

[7] See Digital Single Market – AVMSD Contact Committee, in *ec.europa.eu*.

[8] There are new also on the EU member state level. But for two of them, the systemic approach and transparency, one can argue that some elements of those already appear in German NetzDG, hence this more precise qualification.

[9] In the EU, the main attention is now aimed at announced Digital Services Act that will supposedly focus also on these matters.

those are manifested in the organisation of the content rather than its production.[10] Therefore, there is a difference between the editorial influence exercised by social media providers and the older types of media such as broadcasting, so it is only logical for regulation to follow this distinction.

The AVMSD explicitly recognises this in its recital 48 (first sentence): «In light of the nature of the providers' involvement with the content provided on video-sharing platform services, the appropriate measures to protect minors and the general public should relate to the organisation of the content and not to the content as such».

This recital is of vital importance for the interpretation of the measures laid down for VSPs in the Directive. In contrast to audiovisual media services, i.e. broadcasting and on-demand services, the protected areas enumerated in art. 28b(1), as well as measures listed in art. 28b(3), should not be aimed at the content itself, but only its distribution. Although one might have some difficulty imagining this in practice, the major consequence should be that while broadcasters are objectively responsible for every single piece of content that appears on their broadcasts, VSPs should only be responsible for its systemic treatment. This is, after all, the general approach taken by the NetzDG,[11] and also that proposed in other prominent initiatives.[12] Furthermore, this is arguably the only approach that can accommodate AVMSD provisions with those of the E-Commerce Directive. As no other part of the document mentions this, the first sentence of recital 48 may be considered an important limit on the legislation of new measures in member states during the transposition phase. This is enhanced by the fact that the provisions for VSPs are in a minimum harmonisation regime, which means that member states may choose to impose measures that are more detailed or even stricter than the ones in the Directive.

4.2. Transparency

Transparency is often cited as a key issue in the governance of digital platforms. One cannot devise any meaningful policy or legal action or assess whether such a thing is indeed even needed, when regulators, researchers, activists, users and practically all others are kept in the dark with regard to how platforms work. And although the AVMSD does not go all the way in this regard, transparency has a prominent role in the Directive and has the potential to be a crucial piece of the regulatory puzzle.

In this regard, two instances of transparency requirements in the Directive are relevant. The first is seeking to increase transparency in the decision processes within the platforms themselves; the second is connected to co-regulation.

[10] Although VSPs can have their own productions e.g YouTube Originals.

[11] See the English translation in *bmjv.de*.

[12] See: Creating a French framework to make social media platforms more accountable: Acting in France with a European vision, Interim mission report, "Regulation of social networks – Facebook experiment", 2019; Online Harms White Paper, 2019; OFCOM: Addressing harmful online content, 2018.

4.2.1. Transparency and content moderation

According to art. 28b(3)(i): «establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints to the video-sharing platform provider in relation to the implementation of the measures referred to in points (d) to (h)».

As this is the only provision directly concerned with transparency on the decision processes about the content within VSPs in AVMSD, it is crucial to put it in the proper context.

First of all, we have to note that the transparency obligation out in art. 28b (3)(i) serves both the user who complained and the user against whose content the complaint was directed. From a plain reading, it may be more straightforward to understand this provision as only to enhance the position of the complainant, but such an interpretation would not fulfil the whole scope established in this provision. The transparency aimed at tools helping users to notify the platform about potential wrongdoing is already covered by art. 28b(3)(d),[13] and art. 28b(3)(e)[14]. In contrast to that, to be transparent about 'handling and resolution' of complaints should mean ensuring that all those that are impacted by the decision have the opportunity to understand it. And as independent regulators will have to assess this measure according to art. 28b (5)[15], it follows that they should be able to obtain this information too. It may be that not all the information should be available to everyone, be it for privacy, or some other relevant reasons. In such cases, however, there should still be mechanisms in place, that would ensure that transparency is achieved without unnecessary disclosure of sensitive information. This provision is thus potentially a useful tool in protecting the rights of users. Especially in the case of users who are actively uploading content, this is something that is conspicuously missing in online platforms today. The user whose content is taken down by platform provider usually receives only a generic explanation of the reasons why it happened. Considering the prevalence of online communication via online platforms, and the impact on speech rights that these kinds of decisions have, this is woefully inadequate.

By implementing art. 28b(3)(i) in a certain focused way, the situation just outlined may change. For this, however, it is important to bear in mind both the aim and potential importance of this provision in the exercise of human rights online.

Every online platform has a more or less elaborate moderation system that aims to protect users from potential online harm. In a relatively short time, these systems have evolved from "Feel bad? Take it down" approach to an ultra-detailed set of rules on

[13] By which the provider should be responsible for «establishing and operating transparent and user-friendly mechanisms for users of a video-sharing platform to report or flag to the video-sharing platform provider concerned the content referred to in paragraph 1 provided on its platform».

[14] By which the provider should be responsible for «establishing and operating systems through which video-sharing platform providers explain to users of video-sharing platforms what effect has been given to the reporting and flagging».

[15] «Member States shall entrust the assessment of those measures to the national regulatory authorities or bodies».

a level to which no media regulatory body currently operates.[16] The reason for this is that, while analysts and ultimately decision-making personnel at a regulatory body do have at least some discretion when assessing the content in question, content moderators at platforms do not. The platforms want their rules to be applied consistently across all jurisdictions, and this is arguably not achievable, on the scale the biggest platforms currently operate, without detailed and strictly enforced rules.

This also means, however, that the decision on whether particular content is in line with the platform's rules often hinges on a distinction so minute that it might not be recognisable to anybody without proper training. Not that the user, under current circumstances, would be able to find out. The platforms are simply not making their rules available down to such details.

Typically, what a user can see in the Terms of Service are rules that go into far less depth on what behaviour and what kind of content is prohibited on the platform.[17] But the application of these general rules and their interpretations created during the process, are what counts in reality, and these are hidden from plain view.

This is not to say that these rules are entirely arbitrary. Major platforms like Facebook and YouTube have billions of users with all sorts of cultural backgrounds, so finding one set of rules that fits all circumstances is nearly impossible. The rules need to address new situations and, therefore, continuously evolve.[18] Even the processes that lead to these incremental changes may be quite elaborate.[19]

Platforms also recently increased their transparency in various content moderation statistics like the number of complaints and take-downs.[20] But here we have to state, that, although commendable, these initiatives have their limits, as there is no way to independently verify the published data.[21]

Even more importantly, all this does not change the fact that, when it comes to content moderation, there is almost no transparency in the underlying processes or their outcomes.

There are several reasons why platforms are not being open in this regard. The fact is that, until very recently,[22] the platforms have not been pushed to be transparent about their content moderation by any kind of legal obligation. Therefore, many reasons why they have not done so may fall under the umbrella of simple convenience. But

---

16 K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in *Harvard Law Review*, 131, 2018, 1631.

17 The name may differ from platform to platform, Facebook, e.g. call its rules Community Standards.

18 There are, of course, all sorts of problems with this approach, from the inconsistent application, through the lack of clarity about the motivations behind the rules, to absolute lack of accountability. But we have to bear in mind, that this is still the area of platforms' own discretion. The question of protecting users' rights online is discussed in section 3.4. of this article.

19 Facebook's "mini-legislative session" where rules on content are created is described in D. Kaye, *Speech Police, The Global Struggle to Govern the Internet*, New York, 2019, 53-58.

20 R. Gorwa – A.T. Garton, *Democratic Transparency in the Platform Society*, in N. Persily – J. Tucker (eds.), Social Media and Democracy: The State of the Field, Cambridge, forthcoming.

21 On verification of data, see section 4.2.3 of this paper.

22 "NetzDG", or so-called "Avia Law" in France have introduced substantial transparency obligations for platforms.

there is one argument, often made by platforms, that claims broader regulatory implications. This is the argument that, when shown all the details of decision-making processes in content moderation, the nefarious actors may be able to game them.[23] Researchers, however, tend to dispute this claim, contending that the risks are widely overstated. As Ben Wagner writes, there is an overriding interest in greater transparency of large private intermediaries, and, similarly to what has already been stated about privacy and other concerns in relation to art 28b(3)(i), «the information does not need to be such that it enables the manipulation of the system».[24]

In relation to AVMSD we have to distinguish the general content moderation, outlined in basic tenets above, from the handling of the complaints.

Arguably, all complaints procedures will involve content moderation at some point. However, not all aspects of content moderation are connected to complaints and certainly not all moderation is triggered by them.

As we have already seen, the AVMSD transparency requirement in art. 28b(3)(i) covers, prima facie, only content moderation attached to complaints. The two other relevant provisions in question (art. 28b (3)(d) and (e)) are also concerned, broadly speaking, only with reporting content by users and platforms' dealing with reporting potentially harmful content. Now the question is whether the procedures and decisions that deal with the similar application of platforms' content standards, but taken on the platform's own initiative, are outside of the scope of AVMSD. Moreover, practically speaking, are these two types of decisions even dissociable?

As the VSP regulation is concerned only with video content, it may be, that the providers could separate content moderation on video and other content, and then provide information only about the former. The question of whether they could legitimately, and meaningfully, separate information on content moderation exercised when handling complaints, and when acting on their own initiative, is another matter.

Of course, there are various interpretations possible, but the role of legislators in Member States during the transposition phase should be to find the one most closely aligned with the ideal of full realisation of users' rights on online platforms. For this, it is crucial that the users have certainty regarding the limits to their behaviour and behaviour of others on the platform. Because only then can they make informed decisions and take actions when they feel mistreated. With transparency, in other words, they would possess a necessary, although not by any means sufficient, tool to defend their rights online.

4.2.2. Transparency and co-regulation

The new version of the AVMSD has a strong focus on self- and co-regulatory solutions. Almost every major theme in the AVMSD has these alternative regulatory arrangements mentioned as an acceptable or even preferred solution. And the VSP

[23] N. Suzor, *Lawless: The Secret Rules that Govern our Digital Lives*, Cambridge, 2019, 16.

[24] B. Wagner, *Free Expression? – Dominant Information Intermediaries as Arbiters of Internet Speech*, in M. Moore – D. Tambini (eds.), *Digital Dominance: Implications and Risks*, Oxford, 2018, 232.

regulation is not an exception.

Before we turn to transparency requirements for co-regulatory mechanisms in VSP regulation, it is useful to briefly discuss what the co-regulation in this context might actually mean.

There are no legally binding definitions of either self- or co-regulation. Especially on the European level, however, there is a number of documents describing them, including the definitions for the purposes of the Interinstitutional Agreement on Better Law-Making from 2003,[25] and, most importantly from the perspective of this article, their characterisation in recital 14 of the Directive itself.[26]

Of course, neither self-regulation nor co-regulation can be seen as solutions to every regulatory problem. Although positive aspects are widely recognised, it also has to be stressed that what matters in the end, is the actual exercise. And there are examples when alternative approaches to regulation brought questionable outcomes.[27]

Also, the extent to which different areas of regulation are prone to either self- or co-regulation vary. In this regard, however, the regulatory model taken by the Directive seems to be a good fit for co-regulation.

As we have already seen, the regulatory model for VSPs in AVMSD constitutes only a systemic oversight of content-moderating measures, giving to VSP providers a strong regulatory role. From this perspective then, it seems that self-regulatory part of the co-regulation mechanism is already written into the Directive.

Here lies a conceptual problem, however. In the traditional sense, the self-regulatory body should have an industry-wide relevance[28], but the rules in the Directive aim at individual providers, and currently, there is no industry-wide initiative that could be considered self-regulatory in this traditional sense. True, Facebook has created an option for its Oversight Board project to become one. But this would mean that other social

[25] Interinstitutional agreement on better law-making, OJ C 321, 31.12.2003.

[26] Recital 14 of AVMSD: «Self-regulation constitutes a type of voluntary initiative which enables economic operators, social partners, non-governmental organisations and associations to adopt common guidelines amongst themselves and for themselves. They are responsible for developing, monitoring and enforcing compliance with those guidelines. Member States should, in accordance with their different legal traditions, recognise the role which effective self-regulation can play as a complement to the legislative, judicial and administrative mechanisms in place and its useful contribution to the achievement of the objectives of Directive 2010/13/EU. However, while self-regulation might be a complementary method of implementing certain provisions of Directive 2010/13/EU, it should not constitute a substitute for the obligations of the national legislator. Co-regulation provides, in its minimal form, a legal link between self-regulation and the national legislator in accordance with the legal traditions of the Member States. In co-regulation, the regulatory role is shared between stakeholders and the government or the national regulatory authorities or bodies. The role of the relevant public authorities includes recognition of the co-regulatory scheme, auditing of its processes and funding of the scheme. Co-regulation should allow for the possibility of state intervention in the event of its objectives not being met. Without prejudice to the formal obligations of the Member States regarding transposition, Directive 2010/13/EU encourages the use of self- and co-regulation. This should neither oblige Member States to set up self- or co-regulation regimes, or both, nor disrupt or jeopardise current co-regulation initiatives which are already in place in Member States and which are functioning effectively».

[27] See, e.g., the situation around UK's co-regulatory scheme for on-demand audiovisual services in *ofcom.org*

[28] This also what AVMSD states in recital 14.

platforms would join the initiative, and such a thing is not expected anytime soon.
One can argue, however, that all VSP services, and more generally social media, constitute a market, or at least a playing field, of its own. It doesn't resemble the environments that are traditionally governed by self and co-regulatory arrangements, with many players navigating the same environment. So, it may be that in this area, and arguably, there will be others like this in the near future, we should change our perspective.
Also, the statutory regulation, as opposed to self or co-regulation, typically entails a more direct exercise of regulatory powers than in those alternative regulatory arrangements. But when, for example, BAI stated in its contribution to Irish Government's consultation, that they are not foreseeing a co-regulation for the implementation of VSP rules in the Directive, they also said, that they are not foreseeing to regulate the VSPs directly. So, what kind of approach is being taken here?
The crucial criterion to distinguish between statutory, self- or co-regulatory arrangement would need to be found somewhere else. And the best solution would probably revolve around the question, who is making the rules.
The Directive calls the rulebooks for these alternative regulatory arrangements "codes of conduct". And it is the procedure for creating those that makes the most sense focusing on when trying to distinguish co-regulation from statutory one. Systems for VSP regulation where the codes of conduct are created by self-regulatory bodies (or, at least, the self-regulatory bodies have a meaningful role during their creation), and which systemic application is overseen by state regulatory bodies, can be called co-regulation. Those that are both created and overseen by state regulatory bodies, in line with BAI's ideas, would best be seen as statutory regulation.
With this somewhat longer caveat lets now focus on what are the Directive requirements for transparency in co-regulatory mechanisms.
In its art. 4a(1)(c) the Directive puts a transparency requirement into the core of co-regulatory schemes. Although it is not obligatory to apply measures laid down in the Directive via these mechanisms, as has been already noted, the call for co-regulation is very prominent throughout the Directive, and especially so in the art. 28b dealing with VSPs.
If a member state chooses to establish co-regulatory mechanisms for VSPs, its intrinsic aspect should be the «regular, transparent and independent monitoring and evaluation of the achievement of the objectives aimed at».[29]
Now, how far these requirements may go, is up for debate. They may probably range from minimalistic ones, like self-reporting obligations, to extensive requirements that would involve regulatory audits.[30]
As we already mentioned, there are no self-regulatory or co-regulatory systems in

[29] Art. 4a(1)(c).

[30] The calls for audit competencies for regulators are becoming commonplace, e.g. B. Wagner – C. Ferro, *Report on the Governance of Digitisation, Enabling Digital Rights and Governance*, forthcoming; K. Rozgonyi, *Holding digital platforms accountable: what role to public scrutiny? – A blueprint for audiovisual media policy intervention,* ICA 2019 Post-conference, Building Bridges Between Scholarship and Advocacy for Digital Media Policy, 2019; *Creating a French framework to make social media platforms more accountable: Acting in France with a European vision*, Interim mission report, "Regulation of social networks – Facebook

place in the area of VSPs, so it is difficult to say what is their potential in terms of transparency. Any legislator that is serious about making the digital space more transparent, however, should probably aim at something close to the latter end of the transparency spectrum.

4.2.3. Transparency and data verification

It is one thing to oblige the platform providers to disclose certain data to the regulator, and another to have the ability to ensure that those data fulfil certain criteria in terms of their quality and completeness. To rely solely on the platforms in this regard, as is currently the case, will not be sufficient in the future, especially with AVMSD in force, as we are now moving from pure self-regulation, or, better, non-regulation, towards legally binding rules that call for actionable accountability.

The potential models through which the data can be verified for regulatory purposes vary. It may be that the future media regulators tasked with VSP regulation will also be endowed with data verification competencies alongside those regarding transparency. But while the latter are competencies exercised by some media regulators even today, the situation is entirely different with the former ones.

Data verification is a distinct process that requires specialised expertise. While media regulators currently do have at least some experience with transparency, when dealing with transparency reports by their regulatees in various areas, they usually do not deal with data verification.

Also, data processing in whatever form carries a risk of exposure that might lead to mishandling or even outright abuses of data. And the security concerns are even greater when we consider that media regulators are not the only authorities that would need reliable data from the platforms to exercise their powers. The same would arguably apply to data protection authorities, competition authorities and quite a few others.

To mitigate both of these concerns, i.e. the lack of expertise and security risks involved, it may be worth examining the possibility of keeping transparency and data verification on the one hand, and regulation on the other, as two separate processes. The former could be exercised by a single authority, where both the expertise and security measures could concentrate on the task of gathering verified data, and the regulatory functions could stay more or less as they are now with sector-specific regulators. These authorities then would be provided with the data within their legal competence, to a legally-specified extent for a legally-specified purpose, by the newly established data transparency/verification authority.[31]

experiment", 2019; M. Vermeulen, *Online Content: to regulate or not to regulate – is that the question?,* APC Issue Paper, 2019.

[31] B. Wagner – L. Kuklis, *Disinformation, data verification and social media*, LSE Media Blog, 2020.

4.3. The active user as a regulatory actor

The exercise of traditional (i.e. pre-digital platforms era) media regulation meant finding a proper balance between two competing sets of rights and values, those of freedom of the media and informational rights of public on the one hand, and other public interests, like protection of human dignity, privacy or democratic order represented by the regulator, on the other. The media themselves were the bearers of freedom of media/expression, they had sole editorial responsibility for their content, and they alone decided who can speak on their behalf or through them.
With the advent of social media, the situation has changed. Now there is an active user who is the main creator and publisher. It is of course factually not entirely right to say that platforms have no editorial control over it but, legally, it almost stands, as both US and EU law to a large extent exempt them from liability over the content.
Up until now, however, the user has had very few enforceable protections when it came to his freedom of expression or other informational rights. True, the UN Human Rights Council declared that human rights jurisdiction also extends fully into the digital environment,[32] but without enforceable legal instruments and taking into account protections of platforms from liability, this was of little practical use.
In the EU, increasingly cases are appearing in which courts are forcing platforms to take down or even restore the content in recognition and application of user rights in the online environment. But this only highlights the need for a systemic solution. There needs to be a system that will shield platforms from liability where it will hinder their legitimate use and endanger their users' rights, but it has to have its limits where preventable harm to individuals or society occurs on a massive scale.
So, the nexus of rights and values in the media environment, that in the past had two sharply defined poles, now takes the shape of a triangle, which the new AVMSD recognises in rather unequivocal terms.

4.3.1. Active user in AVMSD

In the first sentence of art. 28b(3), the AVMSD establishes the points to consider when determining individual measures of VSP regulation: «For the purposes of paragraphs 1 and 2, appropriate measures shall be determined in light of the (1) nature of the content in question, (2) the harm it may cause, (3) the characteristics of the category of persons to be protected as well as (4) the rights and legitimate interests at stake, including (5) those of the video-sharing platform providers and the (6) users having created or uploaded the content as well as (7) the general public interest».
Several of these are sufficiently self-explanatory, but some point towards a deeper meaning that may open a new way of looking at the governance of digital space.
Numbers (5), (6), (7) all point to the interests and values that need to be taken into ac-

[32] UN Human Rights Council, Resolution: The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29 June 2012 [draft] in *undocs.org* (adopted on 5 July 2012).

count when determining individual measures for VSP platforms.[33] Interestingly, users that are to be protected by those measures are not mentioned as direct actors in this regulatory model. Their interest is included in (3), and partly in (1) and (2), and definitely in general public interest consideration (7), but they are not included as a special regulatory actor. This approach, however, is entirely warranted.

Media regulation is not, and never has been, about protecting the individual interests of the members of the audience. Of course, those interests are implicitly anticipated by media regulation and may often coincide with the regulatory ones. However, media regulation, in contrast to other legal frameworks like consumer protection or various civil law remedies, is there primarily to look after wider societal interests rather than those of an individual nature. It is therefore understandable that, when it comes to VSP regulation, the approach is systemic and not individual.[34]

With the user "having created or uploaded the content" (6) (an active user), however, the situation is different. As it is an active user whose creative force is behind the content shared on digital platforms, there is a need for redistribution of rights and responsibilities previously reserved only for media.

So far, the regulatory approach focused predominantly on taking down illegal or harmful content from the platforms via different instruments. From a soft approach like EU's Code of Conduct on Hate Speech, through a rather hard one like the proposed Regulation Combatting the Dissemination of Terrorist Content Online, to proper national legislation like NetzDG, all of these strongly push for its content removal. What they have further in common is the absence of any safeguarding mechanism for protection of freedom of expression of the users. The incentives for the platforms are thus strongly stacked on the side of removal, and it is much easier for providers to err in that direction than against it.

To recognise an active user as a regulatory actor means to rebalance those incentives. If a human rights approach to the regulation of online space is to be taken seriously,[35] the regulation also needs to pay attention to what is happening to legitimate content on the platforms, not only to the harmful one.

And AVMSD is the first legal instrument making it clear, that it is also the interests of uploading users that must be taken into account when regulating content on online platforms.

As with transparency, also here one cannot say that AVMSD provisions regarding the protection of users from infringement on their rights are sufficient. Far from it. However, the inclusion of interests of the active user as a legal condition for the implementation of the measures required of platforms by the Directive creates the way through

[33] In it not entirely clear from the wording of the Directive what "determined" in this instance means. Does it only mean "put into biding legislation", or should it cover also the actual application of those measures? But as it probably would not make sense to take listed interests into account when devising legislation but not when applying it, I would interpret it, certainly in this article, that the principles are valid in both cases.

[34] See also recital 48 of AVMSD.

[35] D. Kaye, *A Human Rights Approach to Platform Content Regulation*, Report of the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/38/35, 2018.

which the rights of users can be enforced in a much stronger way than it has been until now. Now it is up to policymakers in the member states to use it.

4.3.2. Proportionality and balancing

If the new rights of active users are fully recognised, it will have a profound impact on the way the fundamental communication rights are exercised online.

The established legal approach of courts and other institutions when resolving conflicts in media environment, is to use so called principle of proportionality to ensure that basic communication rights and freedoms, like the freedom of speech and right to information, are protected.

The principle of proportionality is one of the basic legal principles of EU law.[36] Its role is to ensure that all rights, values and interests are given due consideration and no action of the state is taken beyond what is necessary when in conflict with them.[37] It has also a strong structural dimension that, over time, became a standardised tool for courts and even regulators to resolve these conflicts, called the proportionality test.

The most common version of the test has three steps: suitability, necessity and proportionality in a strict sense.[38] During the first step, it is examined whether the measure in question is suitable to achieve its stated goal. The second step is there to examine whether or not there might be another measure available that would cause less or no damage to the rights or interests with which the measure in question conflicts.

If the answers to first and second steps are satisfactory, meaning that the measure at hand is indeed suitable and necessary to achieve its stated goal, the test moves to its third phase: proportionality in the strict sense. In this stage, the rights and interests in conflict are balanced.

The balancing exercise is based on the premise that fundamental rights are not absolute and have a different weight under different circumstances. It is through the balancing that the authorities determine what is the actual weight of the rights in conflict and which one should, under given circumstances, get precedence.

We already discussed the changing nature of the nexus of rights that comes with the inclusion of an active user into the media environment. And it is the balancing exercise, where this shift from media/regulator dichotomy to user/platform/regulator triangle will be most visibly manifested, as there will often be yet another right or interest to take into account.

In regulating traditional media, the proportionality principle has, explicitly or implicitly, been used for a long time. Now there is a new challenge ahead of policymakers, regulatory authorities, and courts, to apply it in the new "triangle-shaped" regulatory environment. In addition, the new systemic approach is based on the premise that the first line of regulation are VSPs themselves, so, by "regulatory" extension, they will

[36] P. Craig – G. de Búrca, *EU Law*, Oxford, 2015, 545.

[37] Recital 51 is specifically referring to balancing of rights in this sense.

[38] R. Alexy, *A Theory of Constitutional Rights*, New York, 2010.

have to play their role, as well.[39]

5. Conclusions

The regulation of VSPs in AVMSD is the new element of EU media regulatory framework. Not only that this is the first time that audiovisual content on the digital media will be regulated, but also the means to do so are novel.

This is caused equally by structural elements of the digital services that are subject of this regulation, and also by the limits the current legal framework, represented in the EU by E-Commerce Directive, puts on the regulation of content on the online intermediaries.

Because of this, the approach of the AVMSD is systemic, with setting out the measures for the treatment of problematic content, rather than focusing on the individual pieces of the content themselves.

This article describes this new systemic approach and the roles of VSP providers and regulators within it, while also highlights the structural changes in the regulatory environment that moves from traditional media/regulator dichotomy to media/user/regulator triangle. These changes, however, also require that the interests of the active user, who is the main source behind creating and uploading content, are fully taken into account by legally recognising his or her rights and by providing him or her with information on the functioning of the platforms through the introduction of transparency obligations.

Both of these elements are present in the new version of AVMSD, although only in a rudimentary form. However, as this chapter argues, their impact can be considerable if they are given due priority during the transposition phase by national legislators.

[39] See e.g. European Law Journal, Special Issue: Internet and human rights law, Volume 25, Issue 2, March 2019.

A legal analysis of the use of blockchain technology for the formation of smart legal contracts*

Giusella Finocchiaro - Chantal Bomprezzi

Abstract

The object of the present work is to provide a legal analysis of the formation of legally binding agreements through blockchain-based smart contracts. Smart contracts are computer codes that are capable of running automatically upon the occurrence of specific conditions and according to pre-specified functions. These codes can be stored and processed on a blockchain and any change is recorded in the blockchain. The expression "smart legal contract" refers to the use of smart contracts in the contractual domain to perform already existing contracts or to express legally binding agreements in the form of lines of computer code. Regarding the latter, researchers question whether blockchain-based smart contracts can be considered legally binding contracts. The study aims at putting in correlation contract requirements with blockchain-based smart contracts. The scope of the analysis is to verify how to interpret the rules on contract formation to make blockchain-based smart contracts fit into contract law.

Summary

1. Introduction. – 2. Blockchain-based smart contracts: a technical overview. – 3. Smart contracts in the light of contract law. – 4. Offer and acceptance. – 5. Time of conclusion of the contract. – 6. Contractual intention. – 7. The e-Commerce Directive and the Consumer Rights Directive. Information requirements. – 8. Form. – 9. Conclusions.

Keywords

blockchain - smart contract - contract law - contract formation – e-commerce

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

1. Introduction

Blockchain-based smart contracts are self-executing computer programs stored on a blockchain, which can be used in the contractual domain to perform already existing contracts or to express legally binding agreements in the form of lines of computer code. The basic idea is that impartial computers might replace corruptible humans in conducting their affairs.[1] Blockchain technology might reinforce this idea thanks to its decentralised and immutable nature.

There is an academic debate about the implications of blockchain-based smart contracts on contract law. The main question is whether they can be considered as contracts, taking into account that they are merely lines of code, that the blockchain is an emerging technology, and that there are some legal requirements to form legally binding agreements.

On this point, it has to be evidenced that blockchain-based smart contracts can fit other uses cases apart from the contractual domain, and they do not always have a legal significance. The present work aims at putting in correlation contract requirements with blockchain-based smart contracts. The scope of the analysis is to verify how to interpret the rules on contract formation to make blockchain-based smart contracts fit into contract law. It focuses on the exchange of offer and acceptance, the time of conclusion of the contract, the contractual intention, and the form of the contract.[2] Two sections deepen the topic of information requirements and acknowledgment of receipt laid down in the Directive 2000/31/CE[3] and Directive 2011/83/UE[4] because they apply before or at the moment of placing an online order, so they concern contract formation.

Since blockchain technology and its applications are a global phenomenon, to make the work both adaptable to multiple jurisdictions and to foster broader discussions, the paper refers to the three most important sets of contract law principles: The Unidroit Principles of International Commercial Contracts (PICC),[5] the Principles of European Contract Law (PECL), [6] and the Draft Common Frame of Reference of Eu-

---

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

[1] E. Mik, *Smart contracts: terminology, technical limitations and real world complexity*, in *Journal of Law, Innovation and Technology*, 9, 2017, 270.

[2] It does not investigate sufficient agreement and indicia of seriousness that do not seem to pose different issues.

[3] 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 (the so called "Directive on electronic commerce").

[4] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (the so called "Consumer Rights Directive").

[5] *Unidroit Principles of International Commercial Contracts*, Rome, 2016.

[6] O. Lando - H. Beale (eds.), *Principles of European Contract Law*, Parts I and II, The Hague - London - Boston, 2000; O. Lando - E. Clive - A. Prüm - R. Zimmermann, *Principles of European Contract Law*, Part III, The Hague - London – Boston, 2003.

ropean Private Law (DFCR).[7] In addition, as the work assesses contracts concluded by electronic means, it also refers to the Model Law on Electronic Commerce (MLEC),[8] the Model Law on Electronic Signatures,[9] and the United Nations Convention on the Use of Electronic Communications in International Contracts.[10]

2. Blockchain-based smart contracts: a technical overview

"Blockchain" is an umbrella term that includes several independent projects. To date, the two prominent blockchain implementations are Bitcoin[11] and Ethereum.[12] The former was designed to handle financial transactions and to be a core asset for a decentralised virtual market where users exchange virtual coins.[13] The latter, on the other hand, has become a flexible tool for handling secure and trustworthy exchanges of information beyond the financial field, including smart contracts.

A smart contract is a collection of code (its functions)[14] and data (its state)[15] that resides on a specific address (or account). The state of the smart contract can change according to the inputs it receives – which call the functions - and the corresponding output –which depends on the instructions provided by the code. Every change of state represents a transaction that is stored in the blockchain. The code is written in a specific computer language. For instance, the language of Ethereum is Solidity. Solidity is a Turing-complete programming language, which means that it can express any computable function. In Ethereum, every transaction is not free of charge but has a cost that depends on the complexity of the smart contract and is expressed in units called "gas".[16] This is due to the computational effort needed to run the contract.[17]

Blockchains are data structures distributed across a network of computers (or nodes).

---

[7] C. von Bar - E. Clive - H. Schulte-Nölke, *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DFCR),* Munich, 2009.

[8] UNCITRAL, *Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*, New York, 1999.

[9] UNCITRAL, *Model Law on Electronic Signatures with Guide to Enactment 2001*, New York, 2002.

[10] UNCITRAL, *United Nations Convention on the Use of Electronic Communications in International Contracts*, New York, 2007.

[11] www.bitcoin.org. The author of the Bitcoin white paper is Satoshi Nakamoto. See S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System.*

[12] www.ethereum.org. The author of the Ethereum white paper is Vitalik Buterin. See V. Buterin, *Ethereum White Paper: A next-generation smart contract and decentralized application platform.*

[13] On virtual coins, see A. G. Gambino - C. Bomprezzi, *Blockchain e criptovalute*, in G. Finocchiaro - V. Falce (eds.), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019, 267 ss.

[14] In computer science, a function is a section of a computer program that works based on inputs (requests, or calls) and produces a corresponding output (result).

[15] In computer science, a state of a computer program corresponds to its actual values or contents.

[16] Every gas unit corresponds to a certain amount of crypto-currencies.

[17] For a detailed description of the functioning of smart contracts in Ethereum, see C. Dannen, *Introducing Ethereum and Solidity – Foundations of Cryptocurrency and Blockchain Programming for Beginners*, New York, 2017.

Users can interact with the blockchain (i.e. read and write transactions) through their user profiles, also called wallets. A software infrastructure supports the blockchain data structure, ensuring that: nodes can join and leave the network, without compromising the global status of the blockchain data structure; nodes can either discard or accept every change in the blockchain.

Blockchains are made up of blocks. Each block contains: (i) a timestamp, recording its creation time, (ii) a nonce, i.e. a numeric value associated to that single block, (iii) the identifier of another block, (iv) a block status among valid, non-valid, and orphan,[18] and finally (v) a sequence of smart contract transactions. A transaction can either be the uploading of a smart contract on the blockchain or the invocation of some operation of the smart contract.

Hash functions identify each block. Hash functions detect tampering activities: by knowing the block bits and the block hash, the hash function of the block bits can be computed, and it can be checked whether the returned value is the same as the original block hash.

Wallets are software applications that hold the pair of keys used to read and write data in the blockchain. Indeed, each user has a pair of keys. The public key acts as a sort of public address. Users use it to send transactions to the owner of the key. The private key has to be kept secret because it is used to add transactions. The combination of private and public keys is called asymmetric cryptography.[19]

The peculiarity of blockchain technology, as revealed by its name, is that the records of the transactions are grouped to form a block, and the blocks are linked to form a chain. Since every block in the blockchain refers to a previously existing block through its hash, the blockchain is considered immutable. Indeed, any unauthorised change will be immediately visible, because it would cause a modification of the hash and the linked ones.[20]

Usually, blockchains can be permissionless or permissioned. Differences have regard to the different types of permission granted to network participants. Namely, there is the permission to write (i.e. to generate new transactions) and commit (i.e. to update the state of the ledger and add new blocks).[21] In permissionless blockchains, anyone can become a user and write transactions without pre-identification. Any computer can be a node in the network.[22] Furthermore, everyone can add new blocks and update the ledger. In permissioned blockchains, only pre-selected participants can trans-

[18] A block is valid when the network accepts to add it to the blockchain. In the opposite case, the block is not valid. Instead, a block is orphan when the majority of the network initially accepts it but later rejects it in case a longer blockchain does not include that specific block.

[19] In asymmetric cryptography, the key that is used to encrypt the data differs from the key used to decrypt such data. So, asymmetric cryptography is more secure than symmetric cryptography, because it is not necessary to share the same key.

[20] For an overview of the functioning of blockchain technology, see Z. Zheng - S. Xie - H. Dai - X. Chen - H. Wang, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, proceedings of the 2017 IEEE 6th International Congress on Big Data, Honolulu, 25-30 June 2017. For more details, see I. Bashir, *Mastering Blockchain*, Birmingham – Mumbai, 2018.

[21] G. Hileman - M. Rauchs, *2017 Global Blockchain Benchmarking Study*, in *Social Science Research Network (SSRN)*, 22 September 2017, 20.

[22] Permissionless ledgers usually rely on open-source software that anyone can download.

act in the network, only authorized devices can take part as nodes and add blocks. Permissionless and permissioned blockchains also differ for the permission to access the ledger and read transactions. Indeed, permissionless blockchains are usually public, so they have a high degree of openness and anyone can read the transactions. Instead, permissioned blockchains are generally private, because transactions are only visible to authorised users. The reason is that permissionless blockchains are general purpose and do not belong to anyone. In contrast, permissioned blockchains are specifically built to fit a specific purpose of a single entity or a consortium that decided to invest in setting up and maintain the entire system (hardware and software).
As concerns smart contract transactions, firstly a user has to initiate an operation of the smart contract. In doing so, the user has to connect to a node. The algorithm applies to the current state of the smart contract and then computes the next state of the smart contract. When the latter state is determined, a transaction is built. Then, several nodes (validation nodes) have to certify whether the transaction is valid. Each validation node re-executes the operation starting from the original state and checks whether it gets to the same new state. In case of a positive answer, the transaction is valid. If the transaction is valid, all nodes of the network add it to the blockchain. Consequently, all copies of the smart contract in the network change their current state.[23]

3. Smart contracts in the light of contract law

"Smart contract" is a misleading expression. It recalls legal contracts. When Nick Szabo theorised to embed contractual clauses in the hardware and software, «in such a way to make breach of contract expensive», he talked of "smart contracts".[24] With the advent of blockchain technology, this idea has become implementable.[25] Indeed, in the beginning, blockchain technology developed to exchange virtual currencies. Subsequently, it allowed the recording of every digital asset. The most advanced blockchain applications allow the uploading of deterministic computer programs that automatically execute according to predetermined conditions.[26] Therefore, blockchain technology also permits to perform contractual agreements. For this reason, when discussing this blockchain functionality it is usual to refer to it as "smart contract".[27]
Smart contracts are not necessarily contracts. A smart contract *per se* is a computer code that, upon the occurrence of a specific condition, is capable of running auto-

[23] C. Sillaber - B. Waltl, *Life Cycle of Smart Contracts in Blockchain Ecosystems*, in *Datenshutz und Datensichrheit*, 8, 2017, 497.

[24] N. Szabo, *The idea of Smart Contracts,* 1997.

[25] On notion and characteristics of smar contracts, see R. Weber, *Smart Contracts: Do we need new legal rules?*, in A. De Franceschi - R. Schulze - M. Graziadei - O. Pollicino - F. Riente - S. Sica - P. Sirena (eds.), *Digital Revolution – New Challenges for Law. Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*, München, 2019, 301-303.

[26] Melanie Swan divides blockchain development in Blockchain 1.0, 2.0, and 3.0. See M. Swan, *Blockchain. Blueprint for a new economy,* Sebastopol, 2015.

[27] E. Mik, *Smart contracts,* cit., 273.

matically. This code can be stored and processed on a blockchain and any change is recorded in the blockchain.[28] In theory, smart contracts can automate everything. For example, a smart thermostat that regulates the temperature inside a house according to predetermined settings is a smart contract. In these cases, smart contracts have no legal significance. They acquire legal connotations when they are used to automate legally relevant actions or operations. For instance, a smart contract might issue an administrative authorisation when all the requirements to obtain it are fulfilled.

When smart contracts are used in the contractual domain, someone suggested talking about "smart legal contracts". Usually, researchers distinguish between smart legal contracts as contracts or as means to perform already existing contracts. [29] The latter refers to the use of computer code to automate the performance of an agreement (totally or partially) that formed outside the blockchain, independently of how the agreement was reached.[30] In this hypothesis, the smart contract is not a contract, but it is the tool through which a contract is performed. Automated performance replaces performance of the obliged party. The former hypothesis has regard to the possibility to express an agreement in the form of lines of code. On this point, it is questioned whether smart legal contracts can be contracts.[31] To answer the question, someone rightly starts from the legal definition of contract.[32]

A contract is a legally binding agreement between two or more parties.[33] So, the agreement constitutes the very basis of the contract. The mutual consent of the parties (the agreement) is reached through the exchange of an offer and an acceptance. Another fundamental requirement is the parties' expression of their intention to be legally bound by the contract. This means that the offeror and the offeree intended to enter an agreement apt to produce legal effects within a legal system.

In order to reach the so-called "meeting of the minds", both parties must express their intent in some forms. According to the principle of informality, in the silence of law, the parties are free to choose any form to conclude contracts. [34] This principle allows the conclusion of contracts in electronic form. Another internationally recognised principle supports this statement, which is the principle of non-discrimina-

[28] This definition of smart contract appears in J. Earls *et al.*, *Smart contracts: is the law ready?*, Chamber of Digital Commerce Report, 2018, 10.

[29] E.g. see O. Rikken *et al.*, *Smart contracts as a specific application of blockchain technology*, in *dutchblockchaincoalition.org*, 2017, 22; A. Savelyev, *Contract law 2.0: "smart" contracts as the beginning of the end of classic contract law*, Higher School of Economics Research Paper no. WP BRP 71/LAW/2016, 2016, 9; Smart Contracts Alliance, *Smart contracts: 12 Use Cases for Business & Beyond*, Chamber of Digital Commerce, 2016, 40; G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, in *Rivista Trimestrale di Diritto e Procedura Civile*, 2, 2018, 443 ss.

[30] E.g. the contract could be concluded through access to a website, by e-mail, orally or in written form at the contemporary presence of two (or more) parties.

[31] E.g. see K. Werbach - N. Cornell, *Contracts Ex Machina*, in *Duke Law Journal*, 67, 2017, 338; J. G. Allen, *Wrapped and Stacked: "Smart Contracts" and the Interaction of Natural and Formal Language*, in *European Review of Contract Law,* 4, 2018, 319.

[32] K. Werbach - N. Cornell, *Contracts Ex Machina*, cit., 338.

[33] See G. Christandl, *Formation of contracts*, in N. Jansen - R. Zimmermann (eds.), *Commentaries on European contract laws*, Oxford, 2018, 236 ss. See also PECL 2:101, DFCR II.-4:101.

[34] PICC 1.2, PECL 2:101(2), DFCR II. – 1:106.

tion.[35] Consequently, contracts can also be expressed in the form of computer code. However, the creation of a smart legal contract does not automatically imply the conclusion of a contract in the lack of a legally binding agreement. Therefore, smart legal contracts can be considered contracts only in the presence of a legally binding agreement. As Sillaber and Waltl observe, «although a smart contract has been stored on the blockchain, this fact alone should not be considered as a party's agreement to enter the contract as anybody can submit any smart contract to the blockchain indicating an obligation for any random wallet owner».[36]

The meeting of the minds (exchange of offer and acceptance) may occur in various ways. Durovic and Janssen stress that smart legal contracts can be concluded either off-chain or on-chain.[37] The authors explain the process of formation of on-chain contracts by referring to the upload of a proposed contract in coding language in the Ethereum platform and its following acceptance by a participant in the Ethereum network that communicates with the uploaded smart contracts (for example by making a payment in ethers). In other terms, a smart legal contract is formed inside the blockchain when a smart contract code is uploaded to the blockchain, but there is not still an agreement on it. Here, the smart contract represents, in combination with the blockchain, the tool through which a user expresses her contractual will.[38] If the will of the user who uploaded the smart contract matches with the one of another user, a contract is formed, and the smart contract becomes a smart legal contract. The formation of smart legal contracts on-chain is more interesting because the blockchain is a new technology. Indeed, smart contracts without the blockchain have been existing for several years.[39]

The following sections put in correlation contract requirements with the formation of blockchain-based smart contracts. The scope of the analysis is to verify how to interpret the rules on contract formation to make blockchain-based smart contracts fit into contract law.

4. Offer and acceptance

The agreement between the parties required to form a valid contract normally con-

[35] Art. 5 of the MLEC and Art. 8(1) of the United Nations Convention on the Use of Electronic Communications in International Contracts. Art. 46 of the Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (e-IDAS Regulation) establishes that «an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form».

[36] C. Sillaber - B. Waltl, *Life Cycle of Smart Contracts,* cit., 498-499.

[37] M. Durovic - A. Janssen, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, in *European Review of Private Law*, 6, 2019, 760.

[38] *Ibid.*

[39] F. Di Ciommo, *Smart contracts and (non)law. The case of financial markets*, in *Law and Economics Yearly Review*, 7, 2018, 303.

sists of an offer and a corresponding acceptance.[40]

Some authors observe that when a party uploads a smart contract to the blockchain, the uploading[41] corresponds to an offer.[42] The offer must contain all the elements of a valid contract. Otherwise, there is not an offer but an invitation to the other party to enter into negotiations.[43] On this point, Durovic and Janssen consider that «as the "offeror" posts his "contract" onto the blockchain in a binary computer code which specifies precisely the terms of the transaction, it will regularly be held to constitute an offer, not an invitation to treat».[44]

An offer can be directed towards one or more specific persons. Alternatively, it can be addressed to the general audience (proposal to the public).[45] In a blockchain, this depends on the possibility of one or more participants to interact with the smart contract code.[46] More specifically, and from a technical point of view, if the operations of the smart contract are restricted to a specific address (or wallet, or user's profile) in the blockchain, the offer is directed towards a specific participant in the blockchain. In the opposite case, any participant in the blockchain can send transactions, so the offer is open to the general public.

Turning to acceptance, it does not have to meet any specific requirements apart from the offeree's agreement on all the terms of the offer. Therefore, once the offeror has uploaded the smart contract, the offeree could accept it by signing a transaction with a private key.[47]

If the declaration of the offeree does not refer to all the terms of the offer or does not consent to the precise terms of the offer, it is not an acceptance but rather a counter-offer.[48] In the latter case, the counter-offer has to be followed by an acceptance to form a contract. Here, the problem is the immutability of blockchain technology. The code of the smart contract cannot be modified in the blockchain. Consequently, there is no other option than to accept (or to not accept) it.[49] The offeree would need

---

[40] J.M. Smits, *Contract law-a comparative introduction,* Northampton, 2017, 41.

[41] The smart contract code is uploaded on a local node of the blockchain through a "deploy" transaction. Then, the smart contract is replicated in all the nodes of the blockchain.

[42] J. Earls *et al.*, *Smart contracts,* cit., 15; M. Durovic - A. Janssen, *The Formation of Blockchain-based Smart Contracts,* cit., 762.

[43] J.M. Smits, *Contract law-a comparative introduction,* cit., 43 ss. See also Arts. PICC 2.1.2, PECL 2:201, DCFR II. – 4:201 and Art. 11 of the UN Convention on the Use of Electronic Communications in International Contracts.

[44] M. Durovic - A. Janssen, *The Formation of Blockchain-based Smart Contracts,* cit., 762.

[45] J.M. Smits, *Contract law-a comparative introduction,* cit., 44 ss. See also Arts. PECL 2:201 (2) and DFCR II. – 4:201 (2).

[46] J. Earls *et al.*, *Smart contracts,* cit., 17; J. Madir, *Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks?*, in *Social Science Research Network (SSRN)*, 14 December 2018, 7.

[47] J. Earls *et al.*, *Smart contracts,* cit., 17; J. Madir, *Smart Contracts*, cit., 7.

[48] J.M. Smits, *Contract law-a comparative introduction,* cit., 54.

[49] Carron and Botteron talk about a "take it or leave it" offer. See B. Carron - V. Botteron, *How smart can a contract be*, in D. Kraus - T. Obrist - O. Hari (eds.), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law*, Northampton, 2019, 124; Werbach and Cornell argue that smart contracts are by default unilateral because only one party places them on the blockchain. See K. Werbach - N. Cornell, *Contracts Ex Machina*, cit., 343.

to upload a new smart contract and upload it to the blockchain. The upload would correspond to a new offer and the offeree would become the offeror.
The acceptance can occur also in the absence of a specific declaration when it is implied by the offeree's conduct.[50] More precisely, if the offeree starts performing the contract, her actions can be considered as a valid acceptance of the offer. Un unequivocal behavior of the offeree showing a clear acceptance is required. In a blockchain, for example, ceding control over a certain amount of money to the code can be considered acceptance.[51]

5. Time of conclusion of the contract

Establishing the exact time of contract conclusion is of huge importance. From that moment, indeed, the parties are legally bound by the contract, and the contract is in abstract apt to produce its legal effects. In addition, at the time a contract is concluded the offeror can no longer revoke her offer.[52] The time of conclusion of a contract can be determined easily if the parties are present or make use of an instantaneous means of communication. It is more problematic when the parties are absent and a certain amount of time passes between offer and acceptance.[53] If that is the case, the time of conclusion of a contract varies according to the applicable legal system. In general, there are three main rules: 1) the dispatch rule (known also as 'mailbox' or 'postal' rule), where acceptance becomes effective at the moment of sending; 2) the receipt rule, which determines that a contract is considered concluded when the offeror receives the acceptance; 3) the actual notice rule, according to which a contract is formed when the offeror acquires knowledge of the acceptance.[54] Anyway, the jurisdictions that adopt the actual notice rule mitigate it by presuming that the offeror acquires knowledge of the acceptance when it reaches her address unless the offeror proves that acquiring knowledge of the acceptance was impossible for reasons not dependent on her fault.[55]
In the field of electronic contracts, these rules apply by bearing in mind the principle of functional equivalence.[56] Proposal and acceptance are sent or received in the form

[50] J.M. Smits, *Contract law-a comparative introduction,* cit., 57-58. See Arts. PICC 2.1.6 (3), PECL 2:204 (1) and DFCR II. – 4:204(1).

[51] M. Raskin, *The Law and Legality of Smart Contracts*, in *Georgetown Law Technology Review*, 1, 2017, 322; B. Carron - V. Botteron, *How smart can a contract be,* cit., 128 take the example of the transfer of cryptocurrencies by an investor in an ICO. M. Durovic - A. Janssen, *The Formation of Blockchain-based Smart Contracts,* cit., 762-763 imagine the uploading of a smart contract for the transferring of the ownership of a car for 10 ethers, and state that the upload of the 10 ethers by an offeree is an acceptance done by conduct.

[52] G. Christandl, *Formation of contracts,* cit., 323.

[53] Ivi, 324 ss.

[54] The dispatch rule is typical of Common Law. The receipt rule applies to Austria, Germany, and France. Moreover, it is followed by the PICC, the PECL, and the DFCR. The actual notice rule is applied in Italy and Spain.

[55] Art. 1326 (1) *Codice Civile* and Art. 1262 (2) *Código civil.*

[56] The MLEC and the United Nations Convention on the Use of Electronic Communications in

of data messages by means of electronic addresses. The dispatch rule implies that a contract is concluded when the electronic communication that represents the acceptance leaves the information system under the control of the offeree,[57] while, following the receipt rule, the time of conclusion is when the electronic message that contains the acceptance reaches the offeror's information system and can be accessed by the offeror.[58] The latter is also valid with the actual notice rule unless the offeror demonstrates that she was unable (without fault) to know about the acceptance.[59]

In a white paper by R3 and Norton Rose Fulbright,[60] the conclusion of a smart legal contract on the blockchain is compared to the exchange of data messages through e-mails because in the blockchain offer and acceptance are expressed by data messages sent using public-key infrastructure through an Internet connection. Indeed, according to the MLEC and the UN Convention on the Use of Electronic Communications in International Contracts, a data message is any information generated, sent, received or stored by electronic, magnetic, optical or "similar means".[61] This definition

International Contracts established the principle of functional equivalence. The principle is based on an analysis of the purposes and functions of the traditional paper-based requirement to determine how those purposes or functions could be fulfilled through electronic-commerce techniques. H.D. Gabriel, *The United Nations Convention on the Use of Electronic Communications in International Contracts: an Overview and Analysis*, in *Uniform Law Review*, 11, 2006, 285. M. Ratti, *La Convenzione sull'uso delle comunicazioni elettroniche: le principali disposizioni,* in G. Finocchiaro - F. Delfini (eds.), *Diritto dell'informatica*, Milano, 2014, 71. About the use of metaphors to describe the world of the web in the transition from the the real space to the cyberspace, see A. Morelli - O. Pollicino, *Le metafore della rete. Linguaggio figurato, judicial frame e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto*, in *Rivista AIC*, 1, 2018, 1.

[57] Art. 15 of the MLEC establishes the time of dispatch of a data message. Art. 10(2) of the UN Convention on Electronic Communications defines the time of dispatch of electronic communication. See W. Kilian, *Time and Place of Dispatch and Receipt*, in A. H. Boss - W. Kilian (eds), *The United Nations Convention on the Use of Electronic Communications in International Contracts: An In-depth Guide and Sourcebook*, Austin - Boston - Chicago - New York - the Netherlands, 2008, 162.

[58] DFCR I. – 1:109 (4)(c) provides that a notice transmitted by electronic means reaches the address when it can be accessed by the addressee. According to Art. 10(2) of the United Nations Convention on the Use of Electronic Communications in International Contracts, electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address. See also Art. 15(2) of the MLEC. I. Schwenzer - F. Mohs, *Old Habits Die Hard: Traditional Contract Formation in a Modern World*, in *Internationales Handelsrecht*, 6, 2006, 236.

[59] As reported by M. Giancaspro, *Is a "smart contract" really a smart idea? Insights from a legal perspective*, in *Computer Law & Security Review*, 33, 2017, 825, in England, when an offer is accepted via technology, acceptance becomes effective upon receipt, as opposed to the dispatch rule for traditional contracts (regulation 11 of the Electronic Commerce Regulations 2002). The reason is that the dispatch rule was conceived as a compromise between the free revocability of the offer until conclusion and the need to protect the offeree. Indeed, with traditional ways of communication for concluding contracts at a distance, acceptance could have taken a lot of time before arriving at destination. So, the offeree should have been able to accept a contract with the certainty that it would have been binding. Now, because offer and acceptance are exchanged instantaneously, the dispatch rule has lost its function. See A. Rawls, *Contract Formation in an Internet Age*, in *Columbia Science and Technology Law Review*, X, 2009, 207 ss; E. Mik, *The Effectiveness of Acceptances Communicated by Electronic Means, or – Does the Postal Acceptance Rule Apply to Email?*, in *Journal of Contract Law*, 26, 2009, 8. The same is in Australia, while in the USA the dispatch rule applies even when acceptance occurs via the Internet. In France, French courts usually decide on a case-by-case basis.

[60] R3, Norton Rose Fulbright, Can smart contracts be legally binding contracts?, R3 and Norton Rose Fulbright White Paper, November 2016, 22.

[61] Art. 2(1)(a) of the MLEC and Art. 4(1)(c) of the United Nations Convention on the Use of Electronic Communications in International Contracts.

was intended to apply to all existing communication techniques and all types of paperless messages.[62] Moreover, as with e-mails, the offeror and the offeree do not make use of an instantaneous means of communication (such as the telephone) but they are absent and a certain time passes between offer and acceptance.

These data messages are sent and received using electronic addresses, i.e. the accounts that every user has to create to take part in the blockchain and to send transactions.[63] There is no difference with electronic commerce, where the offer and the acceptance are sent from an electronic address or received by an electronic address in the form of data messages. For this reason, the dispatch, the receipt, and the actual notice rules have to be interpreted in the same way. Namely, according to the dispatch rule, the contract is concluded when the offeree sends the acceptance (in the form of a data message) by her electronic address; according to the receipt rule, the contract is concluded when the offeror's electronic address receives the acceptance (in the form of a data message); according to the actual notice rule, similarly to the receipt rule, the contract is concluded when the offeror's electronic address receives the acceptance unless the offeror proves that she could not access her information system for reasons not dependent on her fault.

The remaining issue is to establish which acts correspond to the sending and the receipt of the acceptance in the blockchain.[64] In our opinion, the offeree sends her acceptance when she sends the transaction of acceptance from her address to the address of the smart contract after having signed it with her private key. As concerns the receipt, we think that the offeror receives the acceptance when the transaction of acceptance also reaches her node after having been validated. Indeed, valid transactions are replicated in all nodes of the blockchain network.

In summary, according to the dispatch rule, the contract is concluded when the offeree sends the transaction of acceptance after having signed it with her private key; according to the receipt and the actual notice rule, the contract is concluded when the transaction of acceptance reaches the offeror's node (under the actual notice rule, the offeror can prove that he could not acquire knowledge of it for reasons not dependent on her fault). The application of the dispatch rule, the receipt rule, or the actual notice rule depends on the applicable law.

In case of acceptance by conduct, the contract is concluded through the performance of the contract by the offeree.[65] This statement does not need further interpretations in the domain of blockchain-based smart legal contracts.

---

[62] A. Mukherjiee, *Smart Contracts – Another Feather in UNCITRAL's Cap*, in *Cornell International Law Journal Online*, 8 February 2018.

[63] See section 2.

[64] According to M. Giancaspro, *Is a "smart contract" really a smart idea?,* cit., 830 «The obvious question is whether acceptance occurs once the party seeking to purchase the goods transmits their offer, once it is received and authenticated through consensus of network users, or once it is coded and added to the blockchain».

[65] PICC 2.1.6(3), PECL 2.205 (3), DFCR II. – 4:205 (3).

6. Contractual intention

As mentioned above, in addition to the meeting of the minds, parties must have the intention to be legally bound to their agreement. When a contract is expressed with the language of the code, because the average man is not capable to understand it, it is questioned whether it can be said that the accepting party had the intention to conclude a contract and to be bound by it.[66]

According to the prevailing view, contractual intention has to be objective and not subjective, in the sense that it does not matter the inner intention of the party, her perceptions or understanding. To protect the expectations of the other party and to preserve efficiency and legal certainty of contractual relationships, the agreement must be understood from the external perspective of a reasonable observer. An objective evaluation of the party's statements or conduct has to be carried out by taking into account the circumstances of the case and the general principle of good faith.[67]

In the light of that, the law pays much attention to contractual intention when terms are drafted unilaterally and not individually negotiated between the parties, as is for contracts with standard terms and conditions. It is wondered whether the non-drafting party can be considered bound by the contract. It is today generally acknowledged that the drafting party has to take reasonable steps to bring terms to the other party's attention when the contract is made or beforehand.[68] «To take reasonable steps» means that «[…]the supplier has to take care that the other party is actually aware of those terms and may easily read them».[69] Similarly, Annex I(1)(i) of the Unfair Contract Terms Directive[70] states that the consumer should have a «[…]real opportunity of becoming acquainted» with the terms «[…]before the conclusion of the contract», otherwise the term is considered unfair and does not bind the consumer. The Directive only refers to B2C contracts. Indeed, consumers are the weakest party and need a higher level of legal protection.

The existence of contractual intention has also been discussed about "wrap contracts", which are adhesion contracts concluded online. The most common wrap contracts are "click-wrap" and "browse-wrap" agreements. They are presented and concluded in a non-traditional manner. Indeed, in a click-wrap agreement, the terms are presented in a scrollable box or at a hyperlink, and the other party has to click on an "I agree" button to accept. In a browse-wrap agreement, the terms are accessible through hyperlinks ("Terms of use" or "Legal terms") and the user accepts using a website or downloading the digital content, without having to click on the "I agree" box or take any other positive action. In both cases, courts have expressed the need to provide

[66] B. Carron - V. Botteron, *How smart can a contract be,* cit., 128 ss; Pinsent Masons, Smart insurance Contracts: A discussion paper by Pinsent Masons and Applied Blockchain, 2017, 12; R. O' Shields, *Smart Contracts: Legal Agreements for the Blockchain*, in *North Carolina Banking Institute*, 21, 2017, 186.

[67] J.M. Smits, *Contract law-a comparative introduction,* cit., 64-70. See also PECL 2:102 and DFCR II.-4:102.

[68] See N. Jansen, *Art. 2:104: Terms not Individually Negotiated*, in N. Jansen - R. Zimmermann, *Commentaries on European contract laws*, cit., 272 ss. See PICC 2.1.19, PECL 2:104, DFCR II.-9:103.

[69] Ivi, 278.

[70] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

the other party with sufficient notice of the existence of the terms before or at the time of contract conclusion.[71] In this regard, it is not sufficient to give notice of the existence of the terms, but the terms have to be conspicuously and clearly presented to the non-drafting party. Therefore, the supplier has to take care that the other party is (or should be reasonably) aware of being entering into a contract. Without these arrangements, it has been argued that in browse-wrap contracts it is unlikely that the non-drafting party is aware of the existence of a contract because she is not required to take any positive assenting action. Similarly, in click-wrap contracts, online users do not give importance to the action of clicking on a box as they do with the physical act of placing a signature. In the latter case, however, a higher level of awareness is presumed because the offeree is asked to do something to enter the agreement.

To summarise, in adhesion contracts – being them in paper or online – it is necessary to provide the other party with the terms of the contract in a clear and comprehensible version for the average man in ways that allow her to become reasonably aware of being entering a contract. Otherwise, it cannot be affirmed that the non-drafting party intended to conclude a contract.

Taking account of the above, we think that the fact alone that the contract is expressed in computer code does not suffice to exclude contractual intention. The accepting party has the duty to get informed and understand what she is doing before accepting the offer. Instead, it should be considered the circumstances that preceded the conclusion of the contract, and the qualities of the accepting party.

It has been already described[72] that in on-chain contracts there are "take it or leave it" offers, in the sense that because of the immutability of the blockchain there is not the possibility to make a counter-offer. The contract is drafted unilaterally, and the other party has no other option to accept or not accept it, as is with adhesion contracts. We also find similarities with wrap contracts because of the non-traditional way of expressing assent. Indeed, once the offeror has uploaded the smart contract code on the blockchain, the offeree can accept it by sending some data to the address of the smart contract (e.g. by signing a transaction of acceptance with a private key or by transferring a certain amount of cryptocurrencies). In this event, only one party drafts the terms of the contract, using a non-comprehensible language (at least for the average man), and those terms are accepted in a non-traditional way. For these reasons, we believe that the offeror should accompany the code with a natural language version of the terms, in a clear and comprehensible manner. Moreover, the other party should have the opportunity to understand the moment in which she is going to enter into a contract. For example, O'Shields talks of the possibility to provide an "I agree" button;[73] McKinney, Landy and Wilka propose a check-box or "execute" button.[74]

---

[71] On this topic, see R. Momberg, *Standard terms and transparency in online contracts*, in A. De Franceschi (ed.), *European Contract Law and the Digital Single Market – The Implications of the Digital Revolution,* Cambridge –Antwerp – Portland, 2016, 189 ss.

[72] Section 4.

[73] R. O' Shields, *Smart Contracts,* cit.,186.

[74] S. A. McKinney - R. Landy - R. Wilka, *Smart contracts, blockchain, and the next frontier of transnational law*, in *Washington Journal of Law, Technology & Arts*, 13, 2018, 326.

The distinction between B2B and B2C contracts is also relevant. Businesses usually have more bargaining power than consumers. For example, they may have greater economic possibilities to consult an expert that can understand the language of the code. It might also happen that the contract is concluded based on a pre-existing framework agreement that set the main object of future contracts and the modalities of their conclusion on-chain.[75]

7. The e-Commerce Directive and the Consumer Rights Directive. Information requirements

The Directive 2000/31/CE on electronic commerce and the Directive 2011/83/EU on consumer rights in distance and off-premises contracts include some rules that apply before or at the moment of placing an online order. So, it is important to verify whether these rules are also applicable to the formation of blockchain-based smart legal contracts.

The e-Commerce Directive approximates certain national provisions on information society services also relating to electronic contracts,[76] i.e. contracts concluded at a distance and by electronic means.[77] "Electronic means" refer to «[…]electronic equipment for processing (…) and storage of data».[78] We think that there are no obstacles to the application of the Directive. The offeror and the offeree do not make use of an instantaneous means of communication but they are absent and a certain time passes between offer and acceptance. Moreover, the offeror instantiates a smart contract and the offeree accepts the contract by sending a data message to the smart contract code. Both use a public-key infrastructure and an Internet connection. A distributed and decentralised electronic ledger (the blockchain) processes and stores the offeror's uploading, the offeree's data message, and the resulting change of state of the smart contract code.

Similarly, the Consumer Rights Directive apply to distance contracts, that is «any contract concluded between the trader and the consumer under an organised distance sales or service provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded».[79] Recital 20 also considers mail orders and the Internet as means of distance communication. Other provisions explicitly refer to distance contracts concluded by electronic

[75] Especially if the parties transact through a permissioned blockchain set up for specific purposes.

[76] See Art. 1(2) of the Directive.

[77] According to Art. 2(1)(a) of the Directive, «information society services[…]» are «[…]services within the meaning of Art. 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC», i.e. any services normally provided for remuneration, at a distance and by electronic means at the individual request of a recipient of services.

[78] See recital 17 of the Directive.

[79] See Art. 2(7) of the Consumer Rights Directive.

means.[80] So, we believe that the Directive is also applicable to contracts concluded on-chain for the same reasons expressed for the e-Commerce Directive about the at a distance and electronic nature of such contracts (even though the Directive 2011/83/EU only concerns B2C contracts).

That clarified, both Directives set down some information requirements that the service provider or the trader shall provide to the recipient of the service or the consumer.[81] Art. 10 of the e-Commerce Directive establishes that such information requirements are not mandatory in B2B contracts, while those laid down in the Consumer Rights Directive only refer to B2C contracts.[82] Art. 10 of the e-Commerce Directive also states that the provision shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.

It could be questioned whether the on-chain modality of conclusion of smart legal contracts can be considered an equivalent individual communication like electronic mail.

In that regard, we already explained that in blockchain the offeror can direct her offer towards one (or more) specific person(s) or to the public. In the former hypothesis, only authorised blockchain addresses can interact with the smart contract code, while in the latter any participant in the blockchain can send data messages to the smart contract code. When the offeror directs the offer towards one (or more) specific person(s) we think that the contract is concluded by a form of individual communication equivalent to electronic mail. Indeed, the fact that the offeror indicates one (or more) specific address(es) means that she has already identified the recipient(s) of the offer. In the opposite case, the recipient of the offer is indifferent to the offeror, as is when a business makes available her offer on a website. So, we assume that when the offeror addresses her offer to one (or more) determined recipient(s), the information requirements laid down in Art. 10 of the e-Commerce Directive do not apply.

Maybe, this form of individual communication is more frequent in permissioned blockchains[83] because they are closed systems with known participants.

Another question is whether these information requirements can be expressed in the language of the code. On this point, we think that there are two main obstacles, one technical and one legal.

About the former, someone has observed that not all contractual conditions are operational. There are non-operational contractual conditions, such as those that determine the applicable law or jurisdiction.[84] Similarly, information requirements need a descrip-

[80] See Art. 8(2) and Art. 11(3).

[81] Art. 5 and 10 of the e-Commerce Directive; Art. 6 of the Consumer Rights Directive.

[82] Art. 6(8) of the Consumer Rights Directive states that these information requirements are in addition to information requirements contained in the e-Commerce Directive.

[83] Section 2.

[84] E. Mik, *Smart contracts: terminology, technical limitations and real world complexity,* cit., 294. In general, there are huge difficulties to embed a contract in the form of computer code. Computer language is not flexible, while flexibility allows the adaptation of the contract to all future circumstances and to the context; it does not consider that contracts are by their nature incomplete and have to be supplemented through gap-filling. About this, see J. G. Allen, *Wrapped and Stacked,* cit.; J. M. Sklaroff, *Smart contracts and the cost of inflexibility*, in *University of Pennsylvania Law Review*, 166, 2017, 263; P. Cuccuru, *Beyond Bitcoin: an*

tive, and non-operational, language.

From a legal point of view, both Directives stress the importance of transparency of information. Art. 5(2) of the e-Commerce Directive states that «where information society services refer to prices, these are to be indicated clearly and unambiguously»; Art. 10 of the same Directive dictates that the information is given by the service provider «clearly, comprehensibly and unambiguously». Art. 6 of the Consumer Rights Directive establishes that the provider shall provide the consumer with the information «in a clear and comprehensible manner».

With the advent of the Internet and the development of electronic commerce, people started to conduct their affairs without knowing the identity of the counterparty and without the possibility to directly test the quality of desired services and products. Indeed, the Internet is an open network that permits communication between strangers. They conclude contracts by navigating on websites made available by businesses or intermediary platforms that display virtual icons and buttons that may disorient customers.[85] This led to a lack of trust in the online market. For this reason, traditional contract law needed to be accompanied by further norms to encourage electronic contracting. [86] Among them, information requirements help the other party to become aware of the conclusion of the contract and its contents. In other words, they aim to enhance trust in electronic and distance contracts. A higher level of protection is needed in B2C contracts, where the consumer is the weakest party, and in contracts concluded by access to a website because the identity of the other party is unknown and the terms of the contract are arranged unilaterally. For these reasons, according to the e-Commerce Directive, information requirements are mandatory in B2C contracts and applicable to all contracts not concluded with electronic mail or other equivalent individual forms of communication. The latter modality of contract conclusion is more suitable for parties that already know each other and that are both involved in the process of the drafting of the contract.

In the previous section, we assumed that smart legal contracts should be provided in natural language when the parties have a different bargaining power (such as in B2C contracts), the contract is drafted unilaterally and the accepting party has not the capacity to understand the language of the code. In this way, the party can become reasonably aware of the contract. Therefore, we believe that also information requirements should be given in natural language (in a clear, unambiguous and comprehensible manner) in the same cases where they are mandatory, i.e. in B2C contracts and when the on-chain modality of conclusion of smart legal contracts cannot be considered an equivalent individual communication.

early overview on smart contracts, in *International Journal of Law and Information Technology*, 25, 2017, 179.

[85] The so-called "wrap agreements". See the previous section.

[86] G. Pearce - N. Platten, *Promoting the Information Society: The EU Directive on Electronic Commerce*, in *European Law Journal*, 6, 2000, 363; G. Finocchiaro, *Il perfezionamento del contratto on line: opportunità e criticità*, in *Diritto comunitario e degli scambi internazionali*, 1-2, 2018, 187. About the impact of the Internet on law, see O. Pollicino - M. Bassini, *Internet Law in the Era of Transnational Law*, EUI Working Paper RSCAS 2011/24; O. Pollicino - M. Bassini, *The Law of the Internet between Globalization and Localization*, in M. Maduro - K. Tuori - S. Sankari (edss), *Transnational Law – Rethinking European Law and Legal Thinking*, Cambridge, 2014, 346 ss.

Lastly, because information requirements have the purpose of strengthening the offeree's confidence in the other party's, De Graaf[87] reflects on the practical need of information requirements for blockchain-based smart legal contracts. He argues that «Many commercial parties that wish to sell products or services on the Internet gave an interest in complying with those laws. Traditionally, they sell more when buyers trust them. And one way to gain trust is by providing information about yourself and by complying with internet laws. However, there is no (or less of a) need to do so with smart contracts. Because smart contracts execute themselves, trust in the code is important, not trust in the supplier».[88] In the opinion of the author, the obliged party cannot control the computer system that performs the contract on her behalf thanks to the immutable character of blockchain. By uploading the smart contract to the blockchain, the party cannot refuse to perform. There is no more need to trust in the other party – that cannot avoid execution – but in the code.

Taking apart any considerations regarding the actual capacity of blockchain technology to avoid the control of the obliged party on the performance of the contract, which should be dealt with separately, information requirements do not only contribute to the identification of the party. De Graaf rightly observes that «If the supplier feels no need to comply with these laws and (therefore) also does not provide information about himself, enforcements by courts of law becomes difficult, if not impossible. And if the supplier has no physical address and his assets are unknown, it is difficult to litigate against him and execute his assets if he is ordered by a court to pay a sum of money».[89] Information requirements do not only concern the identity of the obliged party or her geographical address of establishment – which allow the enforcement of the contract - but also the products and services offered, the prices, the technical steps to follow to conclude the contract, the places and the modalities of access to the terms of the contract, the technical means for identifying and correcting input errors prior to the placing of the order, the languages of the contract, and so on. In short, information requirements try to empower the awareness of the weaker party's actions so that to rebalance the parties' negotiating position and foster e-commerce. Therefore, even though on the one hand parties might be more confident that the contract is performed thanks to the blockchain, on the other hand, the blockchain does not remove the risk of unaware and disadvantaged parties.

7.1. The acknowledgment of receipt

Art. 11 of the e-Commerce Directive states that in case the recipient of the service places his order, the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means.[90] This duty does not introduce a

[87] T. J. De Graaf, *From old to new: from internet to smart contracts and from people to smart contracts*, in *Computer Law & Security Review*, 35, 2019, 9.

[88] *Ibid.*

[89] Ivi, 9-10.

[90] A similar provision is laid down in DFCR II. – 3:202.

new way for the exchange of offer and acceptance but is intended to give certainty about the conclusion of the contract because the recipient is distant and cannot know if the order arrived at its destination.[91] The acknowledgment of receipt is not mandatory in B2B contracts[92] and shall not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communication.[93] The reasons for these derogations are the same as those concerning information requirements. In short, in these situations, the conclusion of the contract is less risky for the recipient, and the latter can understand more easily whether and when a contract was concluded. Therefore, Art. 11 of the e-Commerce Directive is applicable and not applicable in the same cases information requirements apply or do not apply.[94]
Maybe, the distributed character of blockchain might help to fulfil the function of the acknowledgment of receipt, i.e. to detect the receipt of the order. Indeed, after the validation nodes have validated the transaction of acceptance, the latter is replicated in the nodes of the network and becomes visible.[95] Thus, the blockchain might be useful to give evidence of the receipt of the order.

8. Form

In section 3, we claimed that a contract can also be expressed in the language of the code, according to the principle of informality and the principle of non-discrimination. Smart contracts fall under the definition of electronic document laid down in the e-IDAS Regulation according to which an electronic document is «any content stored in electronic form, in particular text or sound, visual or audiovisual recording».[96] Indeed, smart contracts are computer programs stored on a decentralised ledger.[97] In its report "Blockchain and digital identity" the European Union Blockchain Observatory and Forum affirms that «as fully digital ledgers, blockchains are by definition electronic documents under eIDAS. That means, among other things, that blockchains, or more properly the data, included smart contracts, contained therein, cannot be denied legal force solely because of their electronic nature».[98]

[91] J. K. Winn - J. Haubold, *Electronic Promises: Contract Law Reform and E-Commerce in a Comparative Perspective*, in *European Law Review*, 27, 2002, 575; D. Memmo, *Il consenso nei contratti telematici*, in G. Finocchiaro - F. Delfini, *Diritto dell'informatica,* cit., 503.

[92] Art 11(1).

[93] Art. 11(3).

[94] See the previous section.

[95] This depends on the right to read transactions. As seen in section 2, in permissionless blockchains everyone can read transactions, while in permissioned blockchains this is possible only for authorised addresses.

[96] Art. 3(35).

[97] In the USA, some countries (Arizona, California, Nevada, Tennessee, Ohio) have introduced *ad hoc* rules that recognise all records in the blockchains as electronic records under the Uniform Electronic Transaction Act (UETA). See 2017 Ariz. HB 2417; 2018 Cal. AB 2658; Nev. Rev. Stat. Ann. § 719.090; 2018 Ohio. SB 220 1306.01; 2018 Tenn. SB 1662 47-10-202. See A. J. Bosco, *Blockchain and the Uniform Electronic Transactions Act*, in *The Business Lawyer*, 74, 2018/2019, 243.

[98] See page 21. The report was published on 2 May 2019 and is accessible at *eublockchainforum.eu*.

Sometimes the law requires some formalities for the validity of contracts or to prove their existence.[99] In this regard, the UNCITRAL has adopted the functional equivalence approach.[100]

When the law requires some formalities for the validity or to make evidence of a contract, the parties have usually to sign the contract. [101] When the contract is in an electronic form, it can be signed with electronic signatures. Art. 2(a) of the UNCITRAL Model Law on Electronic Signatures defines electronic signatures as «data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message». According to Art. 3(10) of the e-IDAS Regulation electronic signatures are «data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign». Electronic signatures differ from traditional signatures because the latter are the result of a human gesture, so they are based on graphics. Electronic signatures are the result of a technological procedure and are based on a technique.[102] Hence, it was wondered when electronic signatures could be considered equivalent to handwritten signatures.

On this point, Art. 7(1) of the UNCITRAL Model Law on Electronic Commerce provides that «Where the law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) that method is reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstances, including any relevant agreement». The UNCITRAL Model Law on Electronic Signatures and the United Nations Convention on the Use of Electronic Communications in International Contracts contain similar provisions.[103]

These international instruments of hard and soft law have guided countries' legislators. Indeed, many countries have adopted the principle of functional equivalence by setting functional requirements for an electronic signature. In particular, some legislations establish that the courts evaluate the meeting of such requirements on a case-by-case basis, while other legislations have adopted a two-tier approach: those electronic signatures which are based on some form of third party identity certification are con-

[99] J.M. Smits, *Contract law-a comparative introduction,* cit., 101 ss. Formalities have the function to warn a party that she is entering a particularly important or financially dangerous contract (warning function) or to inform the party before she is bound (information function). Formalities to prove the existence of the contract have the function to provide certainty about the existence and the content of contracts (evidentiary function).

[100] See section 5, note No. 55.

[101] Some contracts need to be laid down in a notarial deed in the civil law. In these cases, the parties sign the deed and the notary must establish that the parties intend to be bound after having warned them about the legal consequences of their actions.

[102] G. Finocchiaro, *Article 3. Definitions*, in A. Zaccaria - M. Schmidt Kessel - R. Schulze - A.M. Gambino (eds.), EU *eIDAS Regulation – Article-by-Article Commentary,* München, 2020, 55. See also G. Finocchiaro, *Firme elettroniche e firma digitale*, in G. Finocchiaro - F. Delfini, *Diritto dell'informatica,* cit., 309 ss.

[103] Art. 6 of the Model Law on Electronic Signatures and Art. 9 of the UN Convention on the Use of Electronic Communications in International Contracts.

sidered equivalent to handwritten signatures; for the other electronic signatures, the courts have to evaluate such equivalence.[104]

The e-IDAS Regulation adopts a two-tier approach. It recognises three kinds of signature: the simple electronic signature,[105] the advanced electronic signature,[106] and the qualified electronic signature.[107] Only the latter signature shall have the equivalent effect of a handwritten signature,[108] while for the other evaluations are left to the courts.

In the blockchain, users sign transactions with their private keys. Transactions are data messages exchanged between accounts. As seen in section 4, the first transaction concerning a smart contract is the uploading of a new smart contract code on the blockchain. A user signs a "deploy" transaction. The smart contract code is added to the blockchain and associated with an address. Then, the smart contract code changes its state according to the transactions it receives.

When parties make use of blockchain-based smart contracts for the conclusion of legally binding contracts, the offer is made by uploading the smart contract on the blockchain, and the acceptance occurs by sending a transaction to the address of the smart contract. Both the offeror and the offeree link some data (the private key) to other data (the transactions) and approve the information included in the latter data (offer and acceptance). So, these signatures can be considered at least simple electronic signatures.

Qualified electronic signatures have to be created by a qualified electronic signature creation device and have to be based on a qualified certificate for electronic signatures.[109] A qualified signature creation device is configured software or hardware used to create an electronic signature[110] that meets the requirements laid down in Annex II of the Regulation.[111] The definition of electronic signature creation data is more abstract than the former definition of Directive 1999/93/EC[112] that referred to codes or private cryptographic keys.[113] This is due to the principle of technology neutrality, so the Regulation implicitly also mentions cryptographic private keys when it refers to electronic signature creation data.[114] Cryptographic private keys are also used to sign blockchain transactions.

The requirements of Annex II essentially concern the confidentiality and security of the data for the creation of the electronic signature.[115] According to Art. 29(2) of

104 C. Reed, *Electronic commerce*, in C. Reed (ed), *Computer Law*, Oxford, 2011, 282.

105 Art. 3(10) of the e-IDAS Regulation.

106 Art. 3(11) of the e-IDAS Regulation.

107 Art. 3(12) of the e-IDAS Regulation.

108 Art. 25(2) of the e-IDAS Regulation.

109 Art. 3(12) of the e-IDAS Regulation.

110 Art. 3(22) of the e-IDAS Regulation.

111 Art. 29(1) of the e-IDAS Regulation.

112 The e-IDAS Regulation has repealed the above Directive.

113 Art. 2(4) of the Directive 1999/93/EC.

114 K. Erler, *Article 29. Requirements for Qualified Electronic Signatures Creation Devices*, in A. Zaccaria - M. Schmidt Kessel - R. Schulze - A.M. Gambino (eds.), EU *eIDAS Regulation,* cit., 246.

115 M.C. Meneghetti, *Articolo 3*, in F. Delfini - G. Finocchiaro (eds.), *Identificazione elettronica e servizi*

the Regulation, the Commission can establish reference numbers of standards for qualified electronic signature creation devices. If the device meets those standards, compliance with the requirements of Annex II is presumed. The Commission has not established reference numbers of standards under Art. 29(2). However, it has adopted Implementing Decision (EU) 2016/650[116] under Art. 30(3). Indeed, Art. 30 of the Regulation provides that the conformity of the devices with the requirements of Annex II shall be certified by appropriate public or private bodies that have to carry out a security evaluation process in accordance with standards established by the Commission. So, the standards of Implementing Decision (EU) 2016/650 may give indications for interpreting the requirements of Annex II.[117]

A qualified certificate for electronic signature is a certificate, i.e. an attestation that links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.[118] It is issued by a qualified trust service provider and shall meet the requirements laid down in Annex I of the Regulation.[119] The certificate has the function to link the signature to an identified subject. If the certificate is qualified, there is a higher level of security in the connection between a signatory and a signature.[120] A qualified trust service provider is a natural or legal person that provides qualified trust services and is granted the qualified status by the supervisory body.[121]

Despite the principle of technology neutrality and the elaboration of a list of generic requirements, an essential element of a certificate is a particular system of electronic signature, i.e. the PKI Infrastructure,[122] which is also used to validate signatures in the blockchain. Indeed, we described in section 2 that blockchain makes use of asymmetric cryptography. Each user is provided with a pair of keys, one public and one private. The private key is secret and is used to sign transactions. The public key is known by anyone.

In light of the above, despite transactions in the blockchain are signed through cryptographic private keys, and a PKI infrastructure is used, electronic signatures can be considered qualified only in the presence of a qualified signature creation device and a qualified certificate. Therefore, the wallet that contains the keys should meet some

fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014, Torino, 2017, 43.

[116] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Arts. 30(3) and 39(2) of Regulation (EU) No 914/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [2016] OJ L 109/40.

[117] K. Erler, *Article 29,* cit., 251. Art. 1(1) of the Decision specifies that the standards apply where the electronic signature creation data is held in an entirely but non-necessarily exclusively user-managed environment. Otherwise, in the case a qualified trust service provider manages the device, the certification shall be based on a process that, pursuant to Art. 30(3)(b) of the Regulation, uses comparable security levels (Art. 1(2)). Art. 30(3)(b) of the Regulation provides that such comparable security levels shall apply in the absence of standards.

[118] Art. 3(14) of the e-IDAS Regulation.

[119] Art. 3(15) of the e-IDAS Regulation.

[120] M. C. Meneghetti, *Articolo 3,* cit., 44.

[121] Art. 3(20) of the e-IDAS Regulation.

[122] Public-Key Infrastructure. See G. Finocchiaro, *Article 3. Definitions*, cit., 58-59.

requirements that guarantee confidentiality and security of the electronic signature creation data, and there should be a certificate issued by a qualified trust service provider that attests the link between the keys and a precise identity.[123]

An electronic signature can be considered advanced if it meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.[124]

We think that the use of PKI in the blockchain satisfies requirement (a). Asymmetric cryptography – i.e. the private and the public key that every user holds to transact - is resistant to unauthorised data access, so it preserves data confidentiality. Indeed, in asymmetric cryptography, the key that is used to encrypt the data differs from the key used to decrypt it. For this reason, asymmetric cryptography is more secure than symmetric cryptography, because it is not necessary to share a key to decrypt a message.[125]

Asymmetric cryptography allows the verification by the receiver of the provenance and integrity of the received message. The sender encrypts the data with her private key and sends both the encrypted message and its hash. The receiver decrypts the message with the sender's public key. If the result is identical to the hash, the recipient can be sure that the message originated from the sender and was not modified by third parties.[126]

Nicotra and Sarzana di S. Ippolito[127] argue that such signatures might be adopted in permissioned blockchains because they are closed networks with pre-identified participants (unlike in permissionless blockchains). The possibility to identify the signatory could determine the satisfaction of requisite (b). We think that this is plausible in B2B scenarios because businesses can have the economic capacity to equip themselves with such instruments. Moreover, it is more likely that the economic value of their transactions is higher than that of B2C transactions, so there is a greater need to adopt the written form in contracts.[128] The authors claim that these solutions could also meet

[123] The Report "Blockchain and digital identity" of the EU Blockchain Observatory and Forum, at page 23, assumes that «it is possible that blockchain (…) signatures could be considered eIDAS-conform, including potentially up to the highest level, by recognising blockchains within solutions managed by trust service providers». Similarly, Giuliano concludes that blockchain technology makes use of the technological components of the digital signature. However, in the lack of a trust service provider that certifies underlying identities, there is not any equivalence with handwritten signatures. See M. Giuliano, *La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, in *Diritto dell'informazione e dell'informatica*, 6, 2018,1021.

[124] Art. 26 of the e-IDAS Regulation.

[125] In symmetric cryptography, the encryption key coincides with the decryption key. In asymmetric cryptography, the sender encrypts the message with the recipient's public key. The recipient decrypts the message with her private key that is kept secret by the receiver.

[126] I. Bashir, *Mastering Blockchain,* cit., 203.

[127] M. Nicotra - F. Sarzana di Sant'Ippolito (eds.), *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, 64.

[128] Szczerbowski observes that «parties usually prefer written form in contract of substantial economic value». See J.J. Szczerbowski, *Place of smart contracts in civil law. A few comments on form and interpretation*, in *Proceedings of the 12th Annual International Scientific Conference NEW TRENDS 2017*, available at *SSRN*.

requirement (c), e.g. through OTP tokens or biometric authentication.[129]
Lastly, requirement (d) requires controls over the integrity of signed data even after the subscription.[130] We think that the immutable nature of blockchain (thanks to distribution and concatenated hashes) combined with the use of asymmetric cryptography can ensure the detectability of any changes over time. Data are linked to hashes that uniquely represent such data. Every attempt of tampering would cause the change of the hash and the subsequent hashes in the chain.[131]
Simple electronic signatures and advanced electronic signatures shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.[132] Recital 49 of the e-IDAS Regulation entrusts the Member States to establish when electronic signatures are considered equivalent to handwritten signatures.
For instance, in Italy, the *Codice dell'Amministrazione Digitale* (CAD)[133] considers an electronic document to be in written form when the signatory signs it by using a digital signature, a qualified electronic signature, or an advanced electronic signature.[134] In addition, the same legal value is recognised to a document formed in accordance to the requirements set by the *Agenzia per l'Italia Digitale* (AGID)[135] pursuant to Art. 71 of the CAD, upon prior IT identification of its author, in such a way as to guarantee its security, integrity, and immutability and the fact that it is ascribable to the author, in a clear and unequivocal manner.
The digital signature is a qualified electronic signature which is peculiar to the Italian legal system, and that makes use of asymmetric cryptography. The advanced electronic signature is also considered equivalent to handwritten signature. Moreover, the AGID has recently set the guidelines,[136] pursuant to Art. 71 of the CAD, to sign electronic documents with the *Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese* (SPID).
SPID is the Italian electronic identification mean pursuant to Art. 6 of the e-IDAS

[129] M. Nicotra - F. Sarzana di Sant'Ippolito, *Diritto della blockchain,* cit., 64-65.

[130] S. Troiano, *Article 26. Requirements for advanced electronic signatures*, in A. Zaccaria - M. Schmidt Kessel - R. Schulze - A.M. Gambino (eds.), EU *eIDAS Regulation,* cit., 228.

[131] In its report "Legal and Regulatory Framework of Blockchains and Smart Contracts", 12, the UE Blockchain Observatory and Forum writes that blockchains would appear to meet the technical criteria of simple and advanced electronic signatures.

[132] Art. 25(1) of the e-IDAS Regulation.

[133] Legislative Decree 7 March 2005, no. 82.

[134] According to Art. 21(2) of the *CAD*, by contrast with Art. 20(1-*bis*), the juridical acts included in Art. 1350(1-12) of the *Codice Civile* are valid only if signed with a digital signature or a qualified signature. According to Art. 21(2-*ter*) of the CAD, every electronic notarial deed is valid if signed by the notary with a digital or qualified signature. The other involved parties sign the deed with a digital, qualified or advanced electronic signature, or with handwritten signature digitally acquired.

[135] The *Agenzia per l'Italia Digitale* is the technical agency of the Presidency of the Council of Ministers, whose main purpose is to guarantee the achievement of the objectives of the Italian digital agenda, and that contributes to the diffusion of information and communication technologies, to foster innovation and economic growth.

[136] «*Linee guida contenenti le regole tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD*».

Regulation. The guidelines of the AGID state that signatories can only be natural persons[137] with a SPID digital identity level two or higher.[138] The service provider affixes its qualified electronic seal[139] to the document and sends it to the signatory's identity provider. After the signature with the SPID, the identity provider affixes its own qualified electronic seal.

On this point, Art. 8-*ter*(2) of the Italian *Decreto Semplificazioni,*[140] which has introduced some binding norms for blockchain-based smart contracts, states that smart contracts satisfy the requirement of the written form upon prior IT identification of the interested parties through a process that meets the requirements set by the AGID with guidelines. The Art. is very similar to Art. 20(1-*bis*) of the CAD where it recognises the same legal value of handwritten signatures to documents formed in accordance with the requirements set by the AGID pursuant to Art. 71 of the CAD. Indeed, the Determination of the General Director of the AGID no.116/2019 of 10 May 2019 – that has established a Working Group for the preparation of such guidelines and technical standards – provides that the guidelines have to be formed in accordance with the procedure set out in Art. 71 of the CAD and the Regulation for the adoption of Guidelines for the implementation of the CAD.[141] However, unlike Art. 20 of the CAD, the Simplification Decree generically refers to a process upon prior identification of the parties without setting any requirements (whose determination is left to the AGID). Moreover, because the article does not consider electronic signatures, Manente[142] wonders whether the AGID can also provide the use of digital, qualified, or advanced signatures in blockchain-based smart contracts.

In all other cases, the suitability of the document to satisfy the requirement of the writ-

[137] Both for non-professional and professional use (also representing a legal person).

[138] They are assurance levels. The first level is for transactions with a low degree of risk and requires a single-factor authentication system (e.g. a password). The second level is for transactions with a substantial degree of risk and requires a double-factor authentication system (e.g. a password and an OTP). The third level is for transactions with a high degree of risk and requires the use of double-factor authentication systems based on digital certificates and stored on devices that meet some security requirements set by Annex III of the Directive 1999/93/EC (now Annex II of the e-IDAS Regulation).

[139] Like qualified electronic signatures, qualified electronic seals are created by a qualified electronic seal creation device and are based on a qualified certificate for electronic seals (Art. 3(27) of the e-IDAS Regulation). Electronic seals are a novelty introduced by the e-IDAS Regulation. Like electronic signatures, electronic seals are data in electronic form, which is attached to or logically associated with other data in electronic form (Art. 3(25)). But, unlike electronic signatures, electronic seals can only be created by a legal person (Art. 3(24)) and do not have the function of certifying the consent of a legal person in relation to a statement. However, there are some member States where legal persons are enabled to use electronic signatures. So, moving from Recital 24, commentators observed that the Member States may introduce additional functions to electronic seals, thus recognising electronic seals as being the same as legal persons' signatures. To deepen these aspects, see S. Gatti, *Article 35. Legal effects of electronic seals*, in A. Zaccaria - M. Schmidt Kessel - R. Schulze - A.M. Gambino (eds.), EU *eIDAS Regulation,* cit., 276 ss.

[140] *Legge 11 febbraio 2019, n. 12, di conversione del decreto legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e la pubblica amministrazione* (Law no. 12 of 11 February 2019 converting Decree no. 135 of 14 December 2018).

[141] The Determination can be accessed at *trasparenza.agid.gov.it.*

[142] M. Manente, *L. 12/2019 – Smart contract e tecnologie basate su registri distribuiti – prime note, Studio 1_2019*, March 2019, 6.

ten form can be freely assessed in court, with respect to its characteristics of security, integrity, and immutability. Maybe, judges might consider that asymmetric cryptography, hash function, and decentralised databases guarantee the integrity and the immutability of the document. The greatest difficulty seems the fact that in permissionless blockchains the keys are not ascribable to precise identities. However, sometimes it could be possible to reconnect an account to an identified person.[143]

9. Conclusions

The study provided a legal analysis of the use of blockchain technology for the formation of smart legal contracts. It clarified that, despite the term, smart contracts are not necessarily contracts. Even when smart contracts are used in the contractual domain, the mere fact that a smart contract is stored on a blockchain does not give rise to a legal agreement. Indeed, the agreement constitutes the very basis of the contract. In the light of that, smart legal contracts can be concluded off-chain and on-chain. In the former case, smart contracts are mere tools for the automatic performance of the contract (or part of it). In the latter case, the smart contract represents, in combination with the blockchain, the tool through which the parties express their contractual will. Therefore, there was the need to verify how the rules on contract formation can be interpreted to make blockchain-based smart contracts fit into contract law.

To this end, the article took into consideration contract requirements. It started from the agreement, taking into account the exchange of offer and acceptance and the time of conclusion of the contract. Then, it investigated the contractual intention and the form of the contract. It also focused on information requirements and acknowledgment of receipt, that are not contract requirements but apply before or at the moment of placing an online order, so they concern contract formation. The analysis showed that existing general principles and rules of contract law can also be adapted to this new context. Basically, the questions are the same as in electronic commerce. For instance, the transition from paper documents and physical addresses to electronic documents and addresses; the use of non-standard ways and languages for making contract proposals; the issue of a lack of trust between the parties due to forms of distance communication; the difficulty of linking the contractual will to precise identities. As a consequence, analogous legal questions imply analogous legal solutions. For these reasons, it seems that, at least for contract formation, there is not the need to provide new *ad-hoc* rules.

[143] For instance, when the address appears on a personal webpage, blog, or forum. About the pseudonymous character of public keys in permissionless blockchain, and the techniques used to trace back to underlying identities, see P. De Filippi, *The interplay between decentralization and privacy: the case of blockchain technologies*, in *Journal of Peer Production*, 7, 14 September 2016, 11-13, available at *SSRN*; M. Finck, *Blockchains and Data Protection in the European Union*, in *European Data Protection Law Review*, 1, 2018, 22; J. Barcelo, *User Privacy in the Public Bitcoin Blockchain*, in *Journal of Latex Class Files*, 6, 2007, 1; A. Gambino - C. Bomprezzi, *Blockchain e protezione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 3, 2019, 633.

Verso la decisione amministrativa algoritmica?*

Scilla Vernile

Abstract

Il contributo affronta il tema del ricorso a formule algoritmiche ai fini dell'adozione di decisioni amministrative. Dopo avere individuato i principali vantaggi che deriverebbero da un più avanzato livello di digitalizzazione delle pubbliche amministrazioni, sia in termini di maggiore rapidità ed efficienza dell'azione, sia di razionalizzazione dell'organizzazione, l'articolo analizza le maggiori criticità legate all'utilizzo dell'algoritmo in funzione decidente, anche attraverso un richiamo al caso della sua applicazione nel procedimento nazionale di assunzione degli insegnanti, oggetto di un importante contenzioso davanti al giudice amministrativo. In particolare, tra le maggiori criticità, si individuano la difficoltà di assicurare la trasparenza e la conoscibilità dell'algoritmo, specialmente ove l'attività amministrativa sia di natura discrezionale, nonché la necessità, in ogni caso, di attribuire la responsabilità della decisione all'organo per legge competente.

The article addresses the issue of using algorithms to adopt administrative decisions. After identifying the main advantages that would derive from a more advanced level of digitalization, in terms of greater speed and efficiency of administrative action, but also of rationalization of the organization of public administrations, the article analyzes the major criticalities related to the use of algorithms to adopt administrative decisions, also referring to the judicial decision on the application of the algorithm in the national recruitment procedure for teachers. In particular, the main criticalities include the difficulty of ensuring the transparency and knowability of the algorithm, especially in case of administrative discretion, as well as the need, in any case, to attribute liability for the decision to the competent body.

Sommario

1. L'adozione di decisioni amministrative tramite formule algoritmiche. – 2. I vantaggi dell'applicazione delle formule algoritmiche ai procedimenti amministrativi. – 3. L'utilizzo dell'algoritmo nel procedimento di assunzione degli insegnanti. – 4. La decisione automatizzata tra attività amministrativa vincolata e discrezionale. – 5. La conoscibilità dell'algoritmo e il nodo della responsabilità. – 6. Considerazioni conclusive.

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

Keywords
decisione amministrativa – algoritmo – procedimento amministrativo – trasparenza – responsabilità

1. L'adozione di decisioni amministrative tramite formule algoritmiche

Obiettivo dello scritto è offrire alcuni primi spunti di riflessione in merito alla possibilità di ricorrere a formule algoritmiche ai fini dell'adozione di decisioni amministrative. Il punto di partenza è rappresentato dai vantaggi che la digitalizzazione dell'attività amministrativa ha prodotto e produce in favore di coloro che si rapportano con le pubbliche amministrazioni e, ancor prima, di coloro che vi operano all'interno[1].
Quantomeno se tradotta in termini di mezzo di comunicazione ovvero di strumento di raccolta e catalogazione dei dati, la digitalizzazione ha costituito indubbiamente un passaggio fondamentale – sebbene chiaramente non esaustivo - per promuovere una maggiore efficienza dell'organizzazione e dell'attività amministrativa e per ridurre la "distanza" tra cittadino e pubblica amministrazione. La digitalizzazione favorisce la trasparenza del "funzionamento" delle amministrazioni pubbliche e consente un notevole risparmio di tempi e di costi, anche – da non sottovalutare – di carattere ambientale (si pensi alla più immediata riduzione dell'uso della carta, ma anche alla diminuzione degli spostamenti fisici che l'uso della telematica consente).
La digitalizzazione così intesa, ossia principalmente in termini di utilizzo di strumenti informatici nell'esercizio dell'attività amministrativa, per una più efficiente collaborazione tra soggetti pubblici e per garantire contatti più rapidi e flessibili con i cittadini-utenti, tuttavia, costituisce un livello "base". In tali termini, la digitalizzazione si atteggia a strumento di "supporto" per le attività delle amministrazioni, contribuendo a semplificare l'acquisizione e la catalogazione dei dati, nonché la loro circolazione, diffusione ed elaborazione[2].
Ed è a questo livello base che parrebbe mirassero le prime rilevanti disposizioni in materia e, in particolare, il d.lgs. 12 febbraio 1993, n. 39[3], recante "Norme in materia

[1] L'importanza della digitalizzazione della pubblica amministrazione si evince con ancora maggiore nitidezza nell'attuale fase emergenziale determinata dalla diffusione del virus COVID-19. Al fine di favorire l'adozione di misure di contrasto della pandemia, anche tramite nuove tecnologie e una maggiore digitalizzazione della pubblica amministrazione, il d.l. 17 marzo 2020, n. 18, convertito, con modificazioni, dalla l. 24 aprile 2020, n. 27, all'art. 76, rubricato «Gruppo di supporto digitale alla Presidenza del Consiglio dei ministri per l'attuazione delle misure di contrasto all'emergenza COVID-19», dispone che «Al fine di dare concreta attuazione alle misure adottate per il contrasto e il contenimento del diffondersi del virus COVID-19, con particolare riferimento alla introduzione di soluzioni di innovazione tecnologica e di digitalizzazione della pubblica amministrazione, il Presidente del Consiglio dei ministri, o il Ministro delegato, fino al 31 dicembre 2020 si avvale di un contingente di esperti, in possesso di specifica ed elevata competenza nello studio, supporto, sviluppo e gestione di processi di trasformazione tecnologica».

[2] Sulla rilevanza della gestione dei dati da parte dell'amministrazione digitale, G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2017, *passim*.

[3] Il d.lgs. 39/1993 costituisce il primo atto normativo organico in materia, tuttavia, specifiche previsioni

di sistemi informativi automatizzati delle amministrazioni pubbliche", per la "costruzione" di un'informatica pubblica[4].

Nella stessa direzione si sono mosse le disposizioni volte a disciplinare l'atto amministrativo informatico, indispensabile per un processo di vera e propria digitalizzazione degli atti amministrativi, "formati" e non soltanto "copiati" attraverso strumenti informatici. Disposizioni oggetto di un processo di sistematizzazione tradottosi nell'adozione del d.lgs. 7 marzo 2005, n. 82, noto come Codice dell'amministrazione digitale, per la creazione di una rete di comunicazione tra amministrazioni e tra queste e i cittadini, volto a favorire la trasparenza e la partecipazione ai processi decisionali[5] e ridurre le asimmetrie informative, al contempo snellendo passaggi burocratici per un'azione amministrativa più rapida ed efficiente.

Anche il mero utilizzo degli strumenti informatici in sostituzione di quelli cartacei, o comunque tradizionali, ha dato adito a questioni interpretative di non scarso rilievo[6]. Ciò nonostante, un consenso pressoché unanime (un dissenso, d'altronde, sarebbe ormai anacronistico) sembra ormai essere stato raggiunto con riguardo all'utilità, o meglio all'indispensabilità, dei mezzi informatici per una maggiore celerità, efficienza e trasparenza nell'esercizio delle molteplici attività di competenza dell'amministrazione, intese secondo un'accezione ampia, che includa l'esercizio della funzione amministrativa, tanto quanto l'erogazione dei servizi e lo svolgimento degli altri compiti assegnati alle pubbliche amministrazioni.

L'intento che ci si propone, allora, è di esaminare la diversa questione – portata recentemente alla ribalta da alcune pronunce giurisprudenziali del Tar Lazio e del Consiglio di Stato – del possibile utilizzo dello strumento informatico, o meglio di un software basato su una formula algoritmica, ai fini della determinazione del contenuto della decisione amministrativa[7].

---

erano già contenute in precedenti disposizioni normative, si pensi, a mero titolo esemplificativo, all'art. 2 del d.lgs. 3 febbraio 1993, n. 29, confluito nell'art. 2 del d.lgs. 30 marzo 2001, n. 165, ai sensi del quale le amministrazioni devono favorire il collegamento delle attività degli uffici, adeguandosi al dovere di comunicazione interna ed esterna, e l'interconnessione mediante sistemi informatici e statistici pubblici.

[4] L'informatica pubblica è definita come l'insieme dei sistemi informativi automatizzati a disposizione delle pubbliche amministrazioni. In termini, M. Bombardelli, *Informatica pubblica, e-government e sviluppo sostenibile*, in *Riv. it. dir. pubbl. comun.*, 5, 2002, 991 ss.

[5] In questo senso anche la delega contenuta nella l. 7 agosto 2015, n. 124, all'art. 1 sulla Carta della cittadinanza digitale, con lo scopo di «garantire ai cittadini e alle imprese, anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione, il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale, nonché al fine di garantire la semplificazione nell'accesso ai servizi alla persona, riducendo la necessità dell'accesso fisico agli uffici pubblici», su cui si v. V. Cerulli Irelli, *La tecnificazione*, in S. Civitarese Matteucci – L. Torchia (a cura di), *La tecnificazione*, vol. IV degli Studi "*A 150 anni dall'unificazione amministrativa italiana*", a cura di L. Ferrara – D. Sorace, Firenze, 2016, 279 ss.

[6] Si pensi alla questione dei vizi formali dell'atto e, in particolare, al problema della sottoscrizione, su cui si v. A.G. Orofino, *L'esternazione informatica degli atti amministrativi*, in S. Civitarese Matteucci – L. Torchia (a cura di), *La tecnificazione*, cit., 181 ss.

[7] Sugli atti amministrativi automatizzati, senza pretesa di esaustività, A. Masucci, *L'atto amministrativo informatico*, Napoli, 1993; Id., *Atto amministrativo informatico* (voce), in *Enc. Dir.*, Aggiornamento, vol. I, Milano, 1997, 221 ss.; G. Duni, *Amministrazione digitale* (voce), in *Enc. Dir.*, Annali, I, Milano, 2007; 13 ss.; Id., *L'amministrazione digitale. Il diritto amministrativo nella evoluzione telematica*, Milano, 2008; A. Usai, *Le*

Si discute cioè di un livello più avanzato di digitalizzazione, potenzialmente idoneo a incidere significativamente sull'azione, così come sull'organizzazione delle pubbliche amministrazioni, che sembrerebbe potere addirittura condurre alla "sostituzione" della persona fisica impersonante l'organo che adotta la decisione amministrativa[8] con un *software* che, tramite una formula algoritmica, sia in grado di elaborare i dati e le informazioni nella stessa inseriti (o dalla stessa acquisiti, secondo la partizione che si farà) e generare un'autonoma valutazione di tali elementi.

L'interrogativo è netto: è possibile sostituire la decisione umana con quella "algoritmica"?

Nei prossimi paragrafi si tenterà di offrire alcuni spunti di riflessione per rispondere a tale domanda e valutare entro quali limiti sarebbe possibile adottare decisioni amministrative attraverso un processo di automazione pressoché completo[9], con portata sostitutiva dell'intelligenza umana.

Occorre chiarire fin da subito che l'attualità della questione, e del dibattito che ne è scaturito, dipende essenzialmente dal tentativo di espandere il raggio d'azione dello strumento informatico in funzione "decidente" e sostitutiva di quella umana, non essendo nuovo il nostro ordinamento a forme di adozione automatica dell'atto amministrativo. L'esempio classico è rappresentato dai verbali di accertamento delle violazioni del Codice della strada, cui si affiancano altre ipotesi di minore "immediatezza" per la generalità dei consociati, ma altrettanto rilevanti per l'azione delle pubbliche amministrazioni: si pensi, a mero titolo di esempio, ai sistemi telematici d'acquisto disciplinati dal d.lgs. n. 50/2016[10].

Tuttavia, l'intento di "approfittare" delle potenzialità dello strumento algoritmico e il conseguente tentativo di promuoverne una più estesa applicazione, anche a fattispecie

elaborazioni possibili delle informazioni. I limiti alle decisioni amministrative automatiche, in G. Duni (a cura di), *Dall'informatica amministrativa alla teleamministrazione*, Roma, 1992, 55 ss.; Id., *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in *Dir. inf.*, 1, 1993, 163 ss.; U. Fantigrossi, *Automazione e pubblica amministrazione*, Bologna, 1993; D. Marongiu, *L'attività amministrativa automatizzata*, Bologna, 2005; A.G. Orofino – R.G. Orofino, *L'automazione amministrativa: imputazione e responsabilità*, in *Giorn. dir. amm.*, 12, 2005, 1300 ss.

[8] Questioni non troppo diverse da quelle che saranno affrontate nel prosieguo della trattazione riguardano il ricorso all'intelligenza artificiale ai fini dell'adozione delle decisioni giudiziarie: M. Luciani, *La decisione giudiziaria robotica*, in *Rivista AIC*, 3, 2018; S. Quattrocolo, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs. rischi e paure della giustizia digitale "predittiva"*, in *Cass. pen.*, 4, 2019, 1748 ss; F.P. Griffi, *La decisione robotica e il giudice amministrativo*, in *giustizia-amministrativa.it,* 2018.

[9] Sui possibili livelli di automazione, 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, 6 febbraio 2019, i quali individuano tre distinti livelli: a) Primo Livello. Automazione completa; b) Secondo Livello. Automazione e intervento umano ridotto; c) Terzo Livello. Automazione più predizione.

[10] Si pensi, ad esempio, all'art. 56, c. 1, d.lgs. 50/2016, a mente del quale «le stazioni appaltanti strutturano l'asta come un processo elettronico per fasi successive, che interviene dopo una prima valutazione completa delle offerte e consente di classificarle sulla base di un trattamento automatico. Gli appalti di servizi e di lavori che hanno per oggetto prestazioni intellettuali, come la progettazione di lavori, che non possono essere classificati in base ad un trattamento automatico, non sono oggetto di aste elettroniche». Ancora, ai sensi del c. 2, «nelle procedure aperte, ristrette o competitive con negoziazione e nelle procedure negoziate precedute da un'indizione di gara, le stazioni appaltanti possono stabilire che l'aggiudicazione di un appalto sia preceduta da un'asta elettronica quando il contenuto dei documenti di gara, in particolare le specifiche tecniche, può essere fissato in maniera precisa».

caratterizzate da una maggiore complessità, hanno sollevato un acceso dibattito sulle criticità "giuridiche" di un simile approccio, cui si aggiungono i limiti tecnologici, nonché forme di resistenza di tipo culturale e sociologico.
In disparte gli aspetti non prettamente giuridici, nel presente lavoro si approfondiranno alcune delle principali problematiche scaturenti dall'utilizzo delle formule algoritmiche nella determinazione del contenuto delle decisioni amministrative, con particolare attenzione a quelle emerse dall'esame di uno dei casi applicativi più noto, quello che ha riguardato l'organizzazione scolastica, con la dichiarata intenzione di mantenere, nell'affrontare il tema che ci si propone, un atteggiamento di necessaria apertura verso un'evoluzione di cui si percepisce, ancorché nella sua implicita gradualità, il carattere ineluttabile.
Né tale evoluzione parrebbe ostacolata dall'assenza di disposizioni espresse che abilitino l'amministrazione a optare per la decisione amministrativa algoritmica. La scelta di utilizzare un software che, operando secondo regole prestabilite (ferma la questione – che sarà debitamente affrontata – degli algoritmi basati su un sistema di *machine learning*), adotti la decisione amministrativa in luogo della persona fisica preposta rientrerebbe nell'ambito della potestà organizzatoria dell'amministrazione[11], sebbene ciò non escluda che si tratti di un'opzione condizionata al rispetto di limiti di cui ci si propone, almeno in parte, l'individuazione.

2. I vantaggi dell'applicazione delle formule algoritmiche ai procedimenti amministrativi

Le ricerche e gli studi volti a promuovere l'utilizzo di formule algoritmiche nei processi decisionali di competenza delle pubbliche amministrazioni sono mossi dagli indubbi vantaggi che potrebbero derivare dall'uso di uno strumento per sua natura imparziale. La neutralità del funzionamento dell'algoritmo (ma non dei criteri che lo stesso applica, come meglio si dirà) consente di escludere i pregiudizi "consci o inconsci"[12] inevitabilmente espressi dall'animo umano.
Specialmente se ci si sofferma sul profilo patologico dei fenomeni di micro e macro-corruzione, parrebbe immediata l'idoneità della formula algoritmica a contrastare tali fenomeni[13]. Senza relegare la diffusione di modelli decisionali automatizzati a una

[11] In questo senso, A. Masucci, *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte*, Torino, 2011; 86; P. Otranto, Decisione amministrativa e digitalizzazione p.a., in *federalismi.it,* 2, 17 gennaio 2018. Sulla necessità di un fondamento normativo, ancorché non necessariamente legislativo, ma consistente in regolamenti o atti a contenuto generale, in virtù del carattere derivato o secondario del potere di conferimento all'intelligenza artificiale, S. Civitarese Matteucci, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Dir. pubbl.*, 1, 2019, 5 ss., per il quale, sulla base di un parallelismo con quanto avviene per i poteri esecutori, occorre fare fronte all'esigenza della specifica legalità sostanziale che si richiede all'intelligenza artificiale applicata all'attività amministrativa che «non può che essere riferita a ciascuna singola fattispecie di "potere primario" se si vogliono assicurare i "valori del diritto amministrativo"».

[12] G. Avanzini, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Napoli, 2019, 15.

[13] Resterebbe l'eventualità, certo più remota, ma comunque immaginabile, di una "manomissione"

sorta di "rimedio" contro la c.d. *maladministration* e volendone, dunque, tralasciare la rilevanza a fini anticorruzione, il ricorso a formule algoritmiche parrebbe idoneo a "neutralizzare" la componente "emotiva"[14], gli errori umani[15], le negligenze, in qualche misura "giustificate" se si pone mente alle regole che governano la responsabilità dei dipendenti pubblici[16].

La macchina è per definizione impersonale.

Ulteriori vantaggi evidenti della decisione algoritmica si riscontrano nella semplificazione dell'azione amministrativa, chiaramente più rapida e efficiente di quella affidata alla persona fisica. I tempi e i costi dell'azione sarebbero significativamente ridotti dalla capacità della "macchina" di esaminare ed elaborare la documentazione di riferimento in maniera incommensurabilmente più rapida di qualsiasi persona fisica.

A ciò si aggiunge la capacità della macchina di acquisire e catalogare una vastità e complessità di dati tale da garantire una base conoscitiva indubbiamente più ampia di quella di cui potrebbe mai disporre la persona fisica[17], tanto più ove si introduca la distinzione tra algoritmi deduttivi e algoritmi predittivi[18], questi ultimi basati su una tecnologia di *machine learning* e capaci, pertanto, di "imparare" e acquisire dati ulteriori rispetto a quelli selezionati *ex ante* e inseriti nella formula algoritmica. In altri termini, gli algoritmi predittivi sono realizzati tramite una tecnologia che abiliterebbe la macchina a sviluppare decisioni ulteriori e diverse da quelle che potrebbero essere adottate esclusivamente sulla base dei dati inseriti nel software (comprensivi di disposizioni normative, precedenti, elementi fattuali e così via).

Sennonché, proprio con riguardo agli algoritmi basati su meccanismi di *machine learning* sorgono maggiori perplessità[19], per la difficoltà di assicurare la prevedibilità della decisione e la conseguente maggiore opacità del processo decisionale[20]. A tale profilo

delle formule algoritmiche.

[14] S. Civitarese Matteucci, *Umano troppo umano,* cit., 6-7.

[15] M.C. Cavallaro – G. Smorto, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *federalismi.it,* 16, 4 settembre 2019.

[16] Per tutti, S. Cimini, *La responsabilità amministrativa e contabile. Introduzione al tema ad un decennio dalla riforma*, Milano, 2003.

[17] Presupposto necessario sembra essere l'accoglimento di quella «lettura che vuole nei "dati" una risorsa da sfruttare, un giacimento», su cui si sofferma E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in *Dir. pubbl.*, 2, 2019, 363, il quale pone in luce le differenze regolatorie cui sottostanno istituzioni pubbliche e private che, sebbene per cause meritorie, finiscono per limitare significativamente la possibilità di utilizzare questa ricchezza conoscitiva, contribuendo a ostacolare lo sviluppo di un «modello di amministrazione innovativa che resta quasi chimerica ma è al tempo stesso ormai tradizionale: un'amministrazione al servizio dei cittadini e delle imprese, nel quale si superi la tradizionale logica per "silos" e le istituzioni siano in grado di rapportarsi in modo unitario nei confronti degli utenti; utenti identificati con alto livello di certezza, in grado di autenticare le proprie transazioni e completare quindi la fornitura di servizi da parte di un sistema pubblico internamente integrato».

[18] Cfr. F. Costantino, *Lampi. Nuove frontiere delle decisioni amministrative tra open e big data*, in *Dir. amm.*, 4, 2017, 799 ss.; Id., *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, in *Dir. pubbl.*, 1, 2019, 43 ss.

[19] Vantaggi e rischi dell'intelligenza artificiale sono stati recentemente messi in luce dalla Commissione europea con la pubblicazione in data 19 febbraio 2020 del *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia.*

[20] F. de Leonardis, *Big data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione*, in E.

si ricollega anche la questione della natura dell'attività amministrativa che potrebbe essere oggetto di una decisione automatizzata e, dunque, dell'effettivo ambito di applicazione dell'algoritmo in funzione decidente.
Tali tematiche saranno approfondite nel prosieguo della trattazione. Prima, come anticipato, si ritiene opportuno richiamare uno dei casi più emblematici di applicazione di una formula algoritmica ai fini della determinazione del contenuto della decisione amministrativa, per valutare se i risultati, invero paradossali, raggiunti in quella specifica vicenda siano indice delle criticità che la decisione amministrativa algoritmica esibirebbe ovvero se si sia trattato – più semplicemente (ancorché non meno gravemente) – di un errato funzionamento dell'algoritmo.

3. L'utilizzo dell'algoritmo nel procedimento di assunzione degli insegnanti

Un caso particolarmente rilevante[21] di applicazione della formula algoritmica ai fini della determinazione del contenuto della decisione amministrativa ha riguardato l'organizzazione scolastica e questo giustifica, di per sé, almeno in parte, il clamore della vicenda. Per altra parte, il dibattito dottrinale[22] che si è originato parrebbe avere trovato linfa nelle conclusioni – non sempre coerenti – cui è pervenuto il giudice amministrativo chiamato a pronunciarsi sulla legittimità dei provvedimenti conclusivi della procedura di mobilità nazionale avviata in attuazione del Piano straordinario assunzionale di cui alla l. 31 luglio 2015, n. 107, commi da 95 a 104 (c.d. Buona scuola), per la copertura dei posti di potenziamento, sostegno e comuni degli istituti scolastici statali di ogni ordine e grado per l'anno scolastico 2015/2016.

Calzolaio (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Milano, 2020, 137 ss., il quale individua le principali criticità della decisione amministrativa robotica nella difficoltà di raccordarsi con il diritto alla riservatezza e nell'opacità della decisione che, da un lato, non consentirebbe di ricostruirne l'iter logico, dall'altro, violerebbe il principio di trasparenza, anche a causa del fatto che la maggior parte degli algoritmi è sviluppata da aziende private, le quali potrebbero opporre ragioni di segretezza industriale alle richieste conoscitive delle stesse amministrazioni. Cfr. anche F. Costantino, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data*, cit., che sottolinea che «più l'algoritmo è potente, più risulta opaco». Secondo l'A., inoltre, l'opacità sarebbe aggravata dal fatto che gli algoritmi predittivi sono sviluppati perlopiù da aziende private.

[21] Formule algoritmiche sono spesso utilizzate nelle gare pubbliche, magari nella fase amministrativa ovvero, in caso di procedure più semplici, è possibile una gestione integralmente telematica. Ancora, l'individuazione degli aspiranti commissari sorteggiabili per le procedure di abilitazione scientifica alle funzioni di professore universitario, le sanzioni per le violazioni del codice della strada, la formazione delle graduatorie per l'assegnazione delle farmacie comunali, sono tutti esempi di decisioni adottate sulla base di una formula algoritmica più o meno complessa. Per un censimento dei procedimenti ai quali si applicano le formule algoritmiche, G. Avanzini, *Decisioni amministrative e algoritmi informatici,* cit.

[22] *Ex multis*, R. Ferrara, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito giurisprudenziale*, in *Dir. amm.*, 4, 2019, 773 ss.; G. Fasano, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica*, in *questa Rivista*, 3, 2019, 234 ss.; N. Muciaccia, *Algoritmi e procedimento decisionale: alcuni recenti arresti della giustizia amministrativa*, in *federalismi.it,* 10, 15 aprile 2020; L. Musselli, *La decisione amministrativa nell'età degli algoritmi: primi spunti*, in *questa Rivista*, 1, 2020, 18 ss.; S. Civitarese Matteucci, *Umano troppo umano,* cit.; M.C. Cavallaro – G. Smorto, *Decisione pubblica e responsabilità,* cit.; M. Timo, *Algoritmo e potere amministrativo*, in *Dir. econom.*, in corso di pubblicazione.

La procedura, suddivisa ai sensi del comma 98 in tre distinte fasi, prevedeva un'assunzione graduale dei docenti, consentendo a quelli che non fossero stati assunti nella fase A (ossia entro il 15 settembre 2015, secondo le procedure ordinarie di cui all'art. 399 del d.lgs. 16 aprile 1994, n. 297, "TU Istruzione"), di essere assunti nelle successive fasi B e C, sempre in maniera graduale in base alla posizione detenuta in graduatoria, tenendo conto dell'ordine di preferenza espresso tra posti di sostegno e posti comuni, tra scuole di primo e secondo grado e tra tutte le province a livello nazionale.
La procedura per la formulazione delle proposte di assunzione nelle fasi B e C è stata svolta tramite un software che, "incrociando" i relativi dati, avrebbe dovuto formulare per ciascun docente la proposta più rispondente alle preferenze espresse, in base alla posizione occupata in graduatoria.
Sennonché, nell'ambito della fase B, alcuni docenti sono stati assegnati alle scuole superiori di primo grado, nonostante la preferenza espressa per la scuola superiore di secondo grado, e in province diverse e lontane dai luoghi di residenza, mentre, nella successiva fase C, i docenti, collocati in graduatoria in posizione deteriore, sono stati assegnati alla classe di concorso prescelta e nelle province di residenza.
Di conseguenza, alcuni docenti assunti nel corso della fase B si sono rivolti al giudice amministrativo rilevando l'irrazionalità delle destinazioni elaborate dalla formula algoritmica utilizzata, che aveva prodotto provvedimenti immotivati, incomprensibilmente incoerenti con le preferenze indicate dai docenti, nonché con le dichiarazioni di residenza, nonostante i docenti ricorrenti fossero collocati in graduatoria in posizione poziore rispetto a quelli che, assunti nella fase C, erano stati assegnati alle scuole delle province di residenza e nelle specifiche classi di concorso.
Il Tar Lazio, sez. III-*bis*, con la sentenza 1° dicembre 2016, n. 12026, ha respinto il ricorso. Tuttavia, il Consiglio di Stato, sez. VI, con sentenza 8 aprile 2019, n. 2270, ha riformato la pronuncia di primo grado chiarendo che, anche dovendosi riconoscere il valore del progresso tecnologico e della digitalizzazione delle pubbliche amministrazioni, l'utilizzo degli strumenti informatici e, in particolare, degli algoritmi in sede decisionale, è ammesso a condizione che siano rispettai tutti i principi che regolano l'azione amministrativa.
Secondo il Supremo Consesso amministrativo, in particolare, il meccanismo attraverso il quale si concretizza la decisione deve essere "conoscibile", ossia occorre garantire la comprensibilità dell'algoritmo, mediante l'indicazione puntuale dei parametri applicati e delle modalità di funzionamento. La trasparenza dell'algoritmo, infatti, costituisce un presupposto indispensabile per consentire al giudice di sindacare le decisioni adottate sulla base dei risultati prodotti dal software e verificarne correttezza, ragionevolezza e logicità[23].
Nel caso esaminato, dunque, i giudici di Palazzo Spada hanno annullato i provvedimenti gravati per violazione dei principi di imparzialità, pubblicità e trasparenza, risul-

[23] In particolare si legge nella richiamata sentenza che l'esigenza di assoggettare l'algoritmo alla piena cognizione e al pieno sindacato del giudice amministrativo «risponde infatti all'irrinunciabile necessità di poter sindacare come il potere sia stato concretamente esercitato, ponendosi in ultima analisi come declinazione diretta del diritto di difesa del cittadino, al quale non può essere precluso di conoscere le modalità (anche se automatizzate) con le quali è stata in concreto assunta una decisione destinata a ripercuotersi sulla sua sfera giuridica».

tando preclusa la possibilità di risalire dalle decisioni adottate ai parametri inseriti nella formula algoritmica, circostanza vieppiù grave alla luce degli esiti paradossali della procedura, conclusasi con l'illogica assegnazione di docenti, collocati in posizione più alta in graduatoria, a sedi e funzioni meno rispondenti alle preferenze espresse rispetto alle assegnazioni relative ai docenti in posizione deteriore.

Analoghe conclusioni sono state raggiunte in altro giudizio vertente sulla medesima procedura di assunzione, instaurato stavolta dai docenti assunti nella fase C, per essere stati collocati in province diverse da quelle indicate nell'ordine di preferenza, nonostante la disponibilità di posti.

Il Tar Lazio, con sentenza della sez. III-*bis*, 10 settembre 2018, n. 9230, ha accolto il ricorso e sull'appello proposto dal Ministero dell'Istruzione, dell'Università e della Ricerca, Ufficio Scolastico Regionale per la Calabria, si è pronunciato il Consiglio di Stato che, con sentenza della sez. VI, 13 dicembre 2019, n. 8472, ha confermato la decisione di primo grado.

Anche in tale giudizio, il Consiglio di Stato, come già aveva fatto nella richiamata sentenza n. 2270/2019, ha voluto dapprima negare forme di stigmatizzazione nei confronti di un utilizzo più avanzato degli strumenti tecnologici a fini decisionali, ribadendo l'opportunità che la pubblica amministrazione si avvalga delle «rilevanti potenzialità della c.d. rivoluzione digitale» per gli importanti guadagni in termini di efficienza e neutralità e per la riduzione della tempistica procedimentale, di guisa che, almeno qualora si tratti di procedure seriali e 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», il ricorso a una «procedura informatica che conduca direttamente alla decisione finale non deve essere stigmatizzata[o], ma anzi, in linea di massima, incoraggiata[o]».

Tuttavia, ancora una volta il Consiglio di Stato chiarisce che l'applicazione di una formula algoritmica a fini decisionali è ammessa a condizione che sia resa pienamente trasparente e conoscibile, escludendo, peraltro, che possa costituire un ostacolo alla piena conoscibilità del funzionamento dell'algoritmo l'eventuale invocata riservatezza delle imprese produttrici dei meccanismi informatici utilizzati, poiché queste «ponendo al servizio del potere autoritativo tali strumenti, all'evidenza ne accettano le relative conseguenze in termini di necessaria trasparenza».

Alla piena intellegibilità e trasparenza della formula algoritmica deve affiancarsi, secondo quanto chiarito dal Consiglio di Stato, un controllo da parte del soggetto responsabile, escludendo che si possa prescindere del tutto dall'intervento umano, seppure "a valle". Secondo il Supremo Consesso amministrativo, infatti, si ricaverebbe dal diritto europeo (e, in particolare, dal Regolamento UE 2016/679) un principio di «non esclusività della decisione algoritmica", per cui "deve comunque esistere nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica»[24].

[24] Ai sensi dell'art. 22 del Regolamento (UE) 2016/679 del 27 aprile 2016, in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, «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 persona». Cfr. S. Sassi, *Gli algoritmi nelle decisioni*

In presenza delle due condizioni della conoscibilità dell'algoritmo e dell'imputabilità della decisione all'organo competente, che deve potere svolgere una verifica di logicità e legittimità dell'atto risultante dall'applicazione della formula algoritmica, il Consiglio di Stato ha mostrato una certa apertura anche nei confronti dell'attività discrezionale, chiarendo che «né 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». Nel prossimo paragrafo, dunque, ci si soffermerà sulla natura dell'attività che può essere oggetto di una decisione automatizzata, per giungere, infine, al nodo della responsabilità che – si può anticipare – pare costituire, *de iure condito*, il vero ostacolo per una totale devoluzione della decisione amministrativa a un software.

4. La decisione automatizzata tra attività amministrativa vincolata e discrezionale

Il ricorso a formule algoritmiche ai fini dell'adozione della decisione amministrativa, nonostante le problematiche di non poco momento comunque emerse dall'esame della procedura di assunzione degli insegnanti, parrebbe agevolmente ammesso in caso di attività vincolata[25], specialmente allorché si tratti di procedure altamente standardizzate o seriali. Il software si limiterebbe ad applicare al caso specifico quanto già puntualmente previsto dalla legge e trasfuso nella formula algoritmica (sebbene sempre secondo l'interpretazione resa dall'amministrazione competente in sede di individuazione delle regole da tradurre in formula algoritmica).

Con riguardo all'attività amministrativa discrezionale, occorre svolgere ulteriori riflessioni.

Innanzitutto, l'amministrazione potrebbe predeterminare i criteri da osservare nell'adozione della decisione discrezionale, (auto)limitando le possibili soluzioni cui potrebbe giungere la formula algoritmica mediante l'applicazione dei criteri prescelti. La discrezionalità si esaurirebbe al momento dell'individuazione dei parametri, ulteriori rispetto al dato normativo, da inserire nell'algoritmo[26].

La predeterminazione dei criteri, ossia l'indicazione preventiva dei parametri di riferimento per la composizione di interessi affidata alla formula algoritmica, garantirebbe la prevedibilità dell'azione e, di conseguenza, il controllo[27]. La scelta dei criteri diviene

pubbliche tra trasparenza e responsabilità, in *Analisi giuridica dell'economia*, 1, 2019, 109 ss.

[25] Per F. Merusi, *Ragionevolezza e discrezionalità amministrativa*, Napoli, 2011, 15, con riguardo all'attività vincolata, la decisione automatizzata «non è un fenomeno giuridico, ma un fenomeno determinato da un processo tecnologico».

[26] A. Police, *La predeterminazione delle decisioni amministrative. Gradualità e trasparenza nell'esercizio del potere discrezionale*, Napoli, 1997, *passim*, spec. 249: «la predeterminazione è (…) manifestazione espressa della volontà dell'Amministrazione che, con quell'atto, esercita in modo anticipato il potere discrezionale». Sul tema specifico della decisione automatizzata; A. Masucci, *Procedimento amministrativo e nuove tecnologie*, cit., 96, per il quale «le scelte discrezionali sono […] "scelte" dell'amministrazione predeterminate nell'atto-programma. In questo caso l'esercizio del potere discrezionale da parte dell'amministrazione viene "anticipato" al momento della redazione dell'atto-programma».

[27] A. Police, *La predeterminazione delle decisioni amministrative,* cit., 68.

determinante[28].

Se ne trae un ampliamento dell'ambito di applicazione della decisione automatizzata. Il ricorso all'algoritmo "decidente" sarebbe ammesso non soltanto nelle ipotesi di attività strettamente vincolata, ove il software fosse deputato a elaborare la decisione della fattispecie sulla base del mero accertamento, in concreto, dei presupposti di legge, bensì anche ogniqualvolta l'amministrazione stabilisca preventivamente le ulteriori condizioni di esercizio del potere, autolimitandosi[29] e "consumando", così, la discrezionalità in un momento più "tradizionale"[30].

A ben guardare, infatti, in tali casi, l'attività delegata al decisore elettronico sarebbe in ogni caso vincolata, sebbene non dalla legge, ma da quanto prestabilito dalla stessa amministrazione, che potrebbe così tenere conto anche degli apporti partecipativi che sarebbero "incorporati" in fase di predeterminazione dei criteri, non potendo certo essere esclusi soltanto perché si opta per l'utilizzo dello strumento informatico[31]. In tal modo, le esigenze di trasparenza, prevedibilità e partecipazione parrebbero salvaguardate[32].

---

[28] Ciò anche per garantire che sia riservata all'amministrazione – e non al "sistema tecnologico" – l'operazione tipica delle organizzazioni che «si mettono in grado di operare, producendo complessità interna, decidendo premesse decisionali per altre decisioni». In altri termini, all'interno delle organizzazioni, «vengono fissate premesse per una quantità indeterminata di decisioni future, le quali si raffronteranno a queste premesse decisionali. […] Le premesse decisionali servono per stabilire quali decisioni varranno come decisioni dell'organizzazione». Così F. Fracchia, *Le fake news come luogo di osservazione dei fenomeni della tecnologia e delle reti nella prospettiva del diritto*, in *federalismi.it*, il quale paventa il rischio che la tecnologia e, in particolare, la rete, con riguardo al tema ivi affrontato delle *fake news*, adottando premesse decisionali per ridurre la complessità, sottragga ai sistemi (intesi, secondo la costruzione luhmanniana, come insieme di comunicazioni sociali) diritto, politica, economia, arte e così via, «importanti spazi di soluzione del problema di cui essi si fanno carico, smarrendo quell'esclusiva che si sono guadagnati nella società moderna».

[29] Si v. P.M. Vipiana, *L'autolimite della pubblica amministrazione. L'attività amministrativa fra coerenza e flessibilità*, Milano, 1990; A Police, *La predeterminazione delle decisioni amministrative,* cit.

[30] Secondo R. Ferrara, *Il giudice amministrativo e gli algoritmi,* cit., il potere discrezionale continua a giocare un ruolo fondamentale anche nei procedimenti informatizzati, semmai acquisendo una diversa collocazione nel tempo e nelle fasi del procedimento, senza che da ciò derivi una sua inammissibile svalutazione. Per l'A., la regola giuridica tradotta in regola tecnica, allora, potrebbe essere assimilata «ad un atto amministrativo presupposto nei confronti del quale le decisioni attuative/esecutive che originano dall'utilizzo delle procedure informatizzate si configurano come meri atti di esecuzione di "regole del gioco" in altra sede e in altro momento (ossia, in un altro *step* procedimentale) proposte ed elaborate».

[31] Come chiarito da M. Occhiena, *Situazioni giuridiche soggettive e procedimento amministrativo*, Milano, 2002, 441, i soggetti interessati dalle vicende giuridiche prodotte dal provvedimento amministrativo non possono essere lasciati senza «protezione sostanziale». Né, dunque, si potrebbe rinunciare alla partecipazione degli interessati per un asserito contrasto con i principi di economicità ed efficienza alla base del ricorso allo strumento informatico in funzione "decidente", qui esaminato. Secondo l'A., infatti, ove si negasse la partecipazione dei soggetti interessati dagli effetti del provvedimento, «si finirebbe con l'introdurre surrettiziamente il principio per cui i criteri di economicità ed efficienza dell'azione amministrativa sono assiologicamente più importanti del principio di giustiziabilità delle situazioni giuridiche soggettive nei confronti degli atti e comportamenti degli enti pubblici», anche perché i costi di un eventuale contenzioso potrebbero essere superiori a quelli derivanti dalla necessità di assicurare la partecipazione.

[32] Secondo P.M. Vipiana, *L'autolimite della pubblica amministrazione,* cit., 190, «ogni qualvolta la pubblica amministrazione prefissi dei criteri decisionali operanti nei confronti della sua futura attività, si concreta un fenomeno che […] si potrebbe così compendiare: raffrontabilità dell'atto con il previo atto». E ancora, «la carica garantistica sottesa al principio di raffrontabilità, nel suo significato tradizionale,

Diversa l'ipotesi ove residuino margini di discrezionalità[33].

Invero, non pare si possa escludere a priori che l'algoritmo sia in grado di adottare soluzioni razionali (e, probabilmente, anche migliori di quelle che potrebbe adottare la persona fisica), almeno in quelle ipotesi che ammettono un numero limitato di possibili alternative, comunque prevedibili e rispetto alle quali la scelta – evidentemente di merito - sarebbe attribuita all'algoritmo. La macchina, del resto, ben potrebbe essere settata anche per "scegliere" tra soluzioni alternative, tutte conformi al paradigma normativo e al principio di logicità-congruità.

Circostanza ancora diversa si verificherebbe qualora l'algoritmo, sviluppato con tecnologie di *machine learning* o apprendimento automatico, non si limitasse a scegliere tra soluzioni già "date" e, quindi, prevedibili, ma generasse decisioni nuove e non prevedibili (superando la possibile obiezione per la quale la macchina si limiterebbe ad applicare soluzioni già apprese e inserite dal programmatore, negandole la capacità creativa e la flessibilità necessarie per assicurare imparzialità e uguaglianza, anche trattando situazioni diverse in modo diverso).

Sennonché, sono proprio queste ultime le ipotesi in cui potrebbero ravvisarsi maggiori criticità, poiché, per definizione, la tecnologia *machine learning* non consente di conoscere i parametri che saranno applicati nell'adozione della decisione finale, rendendo più opaco il processo decisionale[34].

L'intelligenza artificiale, acquisendo dati e "imparando" da tali dati, non si limita ad applicare la "regola giuridica", tradotta nell'algoritmo, ma elabora essa stessa nuove regole, in maniera autonoma e, dunque, non prevedibile[35], in virtù dell'ampliamento esponenziale della base conoscitiva dell'algoritmo.

Circostanza che si tradurrebbe nella non "controllabilità" dell'algoritmo e dei risultati dallo stesso generati, fatta salva l'obiezione che, in assenza della predeterminazione dei criteri che esauriscono la discrezionalità, anche la decisione umana sarebbe "imprevedibile" e il controllo non potrebbe che limitarsi alla valutazione *ex post* della ragionevolezza della decisione sulla base della motivazione del provvedimento, dal cui obbligo non potrebbe essere esonerata la decisione algoritmica[36].

---

non pare sostanzialmente sminuita qualora esso venga realizzato tramite autolimiti della pubblica amministrazione».

[33] Secondo A. Masucci, *Procedimento amministrativo e nuove tecnologie*, cit., 95, ove non sia possibile, tramite le "istruzioni" inserite nel software, stabilire i criteri di esercizio del potere discrezionale, la decisione andrebbe rimessa al funzionario. In particolare, secondo l'A., «nei casi nei quali non è possibile attraverso le "istruzioni" assicurare il rispetto di una valutazione differenziata delle diverse situazioni concrete che possono presentarsi, la decisione deve essere rimessa al funzionario. Questi può, di volta in volta, individuare la decisione che ritiene più consone alla fattispecie da regolare».

[34] Secondo M.C. Cavallaro – G. Smorto, *Decisione pubblica e responsabilità,* cit., l'"oscurità" del processo decisionale si traduce inevitabilmente in un limite al sindacato della decisione algoritmica.

[35] G. Avanzini, *Decisioni amministrative e algoritmi informatici,* cit., 40.

[36] A. Masucci, *Procedimento amministrativo e nuove tecnologie*. cit., 101; Id. *L'atto amministrativo informatico*, cit., 99; F. Saitta, *Le patologie dell'atto amministrativo elettronico e il sindacato del giudice amministrativo*, in *Rivista di diritto amministrativo elettronico*, 2003, per il quale l'atto amministrativo elettronico, al pari di quello tradizionale, potrebbe anche essere motivato *per relationem*. Anche l'atto amministrativo elettronico, inoltre, potrebbe essere adottato in forma semplificata ove risultasse la manifesta irricevibilità, inammissibilità, improcedibilità o infondatezza dell'istanza, su cui sia consentito rinviare a S. Vernile, *Il provvedimento amministrativo in forma semplificata*, Napoli, 2017.

5. La conoscibilità dell'algoritmo e il nodo della responsabilità

La questione si sposta, allora, a valle dell'adozione della decisione e concerne la capacità o meno dell'algoritmo di fornire, insieme alla decisione, un'indicazione precisa delle ragioni di fatto e di diritto che ne costituiscono il fondamento e, dunque, del percorso logico che ha condotto all'adozione di quella specifica soluzione[37].

Invero, anche soffermandosi in via esclusiva sugli algoritmi che operano secondo un meccanismo deduttivo, in disparte le difficoltà di assicurare la piena conoscibilità della regola tecnica algoritmica, legate al linguaggio che la stessa utilizza[38], la motivazione mantiene il suo carattere essenziale, dal momento che l'algoritmo opera sulla base di una necessaria selezione e semplificazione dei dati che non può che considerarsi già in termini di esercizio di potere anche quando consista nella mera individuazione delle disposizioni normative applicabili e nella loro interpretazione[39] e che, conseguentemente, deve risultare dal provvedimento finale[40]. Tanto più nelle ipotesi di attività discrezionale e specialmente là dove la predeterminazione dei criteri inseriti nell'algoritmo, espressione di autolimite, non fosse sottoposta a forme di pubblicità[41].

Se ciò è vero sul versante dei destinatari dell'azione amministrativa o comunque dei soggetti alla stessa interessati, le esigenze di trasparenza e conoscibilità del funzionamento dell'algoritmo parrebbero rilevare ancor di più per l'organo individuato dalla legge come competente all'adozione del provvedimento[42]. L'organo competente, secondo le regole vigenti, non potrebbe che essere responsabile degli effetti prodotti dal provvedimento, di guisa che gli deve essere garantita la possibilità di verificare, nonostante le asimmetrie conoscitive, che la formula algoritmica, tendenzialmente elaborata da un programmatore esterno o comunque da un soggetto diverso dall'organo

---

[37] In questo senso, A. Simoncini, *Profili costituzionali della amministrazione algoritmica*, in *Riv. trim. dir. pubbl.*, 4, 2019, 1149 ss., spec. 1183, il quale osserva che «affinché si possa conoscere la motivazione con la quale un algoritmo prende una certa decisione, occorrerebbe che tale algoritmo fosse – non tanto ragionevole, perché potrebbe comunque produrre decisioni commisurate allo scopo, quanto – "razionabile" (dalla *rationabilitas* canonica), ovvero come si preferisce nella terminologia tecnica più aggiornata, "esplicabile", cioè descrivibile nella sua strutturazione causale, in modo da poterne "ripercorrerne l'iter logico" – come chiedono i giudici; ma questa qualità oggi non è un carattere necessario di tutti i sistemi di decisione automatica ed anzi sono rapidamente in aumento le tecnologie basate sul cosiddetto *deeplearning* ovverosia di sistemi di apprendimento automatico che simulano l'azione del cervello. In questi casi – quand'anche si volesse riconoscere all'algoritmo la natura di "atto" – esso sarebbe strutturalmente inconoscibile (o in-esplicabile), quantomeno con gli strumenti ordinari della logica umana».

[38] Oltre alle questioni di proprietà intellettuale, tuttavia "superate" da Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472, secondo cui, una volta che lo strumento informatico è posto al servizio del potere autoritativo, si accettano le relative conseguenze in termini di trasparenza.

[39] F. Follieri, *Decisione amministrativa e atto vincolato*, in *federalismi.it,* 7, 5 aprile 2017.

[40] M.C. Cavallaro – G. Smorto, *Decisione pubblica e responsabilità*, cit.

[41] Sui diversi livelli di conoscibilità dell'autolimite, P.M. Vipiana, *L'autolimite della pubblica amministrazione,* cit., 487 ss.

[42] La tutela del danneggiato, infatti, potrebbe essere facilitata dal concetto di "colpa dell'apparato" che, evocando la disorganizzazione dell'ente nella gestione delle risorse, potrebbe "coprire" anche le ipotesi di malfunzionamento dell'algoritmo o comunque di decisioni automatizzate illegittime. Non possono tacersi, tuttavia, le difficoltà applicative del criterio della colpa dell'apparato, su cui si v. F. Fracchia, *Elemento soggettivo e illecito civile dell'amministrazione pubblica*, Napoli, 2009, 123.

competente per l'adozione dell'atto[43], traduca esattamente la regola giuridica[44] (intesa quale l'insieme degli "input" occorrenti per l'adozione della decisione finale) [45].
Il linguaggio giuridico è costretto a dialogare con quello tecnico-informatico: la selezione e la verifica dell'esattezza dei dati e delle informazioni che saranno elaborati dall'algoritmo non può che spettare al dirigente responsabile dell'adozione del provvedimento, il cui contenuto è determinato attraverso l'applicazione della formula algoritmica.
Controllo precluso, per definizione, in caso di algoritmi basati su una tecnologia di *machine learning*.
Si scontrano qui le esigenze di prevedibilità, che presuppongono una completa predeterminazione degli elementi che saranno considerati in sede di adozione della decisione finale, con le potenzialità degli strumenti informatici quanto a capacità di acquisizione ed elaborazione di una vastità e complessità di dati chiaramente superiore a quella umana e che potrebbe costituire l'effettivo valore aggiunto dell'utilizzo delle formule algoritmiche[46], fermi restando i risultati comunque apprezzabili in termini di maggiore rapidità e riduzione dei costi. Lo "scontro" potrebbe "comporsi" nell'assunzione della responsabilità della decisione da parte dell'organo competente[47].

6. Considerazioni conclusive

Alla luce delle considerazioni svolte, il rischio dell'adozione di decisioni illegittime

[43] Quest'impostazione dualistica, secondo L. Viola, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *federalismi.it*, 21, 7 novembre 2018, avrebbe il merito di ripartire correttamente la responsabilità tra il funzionario che predispone il "pre-software" e il programmatore del software che contiene la formula algoritmica. Inoltre, secondo l'A., si supererebbero in tal modo i problemi legati alla comprensibilità del software, che sarebbe assicurata dalla conoscibilità del pre-software e, quindi, dei fattori di input.

[44] Così definita da Cons. Stato, sez. VI, 8 aprile 2019, n. 2270.

[45] Ferma restando, chiaramente, la responsabilità del programmatore nei confronti dell'amministrazione per l'inesatta traduzione della regola giuridica, ove non dipenda dalla indeterminabilità o comunque dalla scarsa chiarezza della stessa. Sul punto, D. Marongiu, *Gli atti amministrativi ad elaborazione elettronica: la compilazione di un "pre-software" in lingua italiana*, in *Rivista di diritto amministrativo elettronico*, 2003, 4, per il quale «sarà chiara l'attribuzione delle responsabilità in caso di difformità tra gli atti automatici e il dettato della legge, ossia in caso di produzione di atti illegittimi da parte del calcolatore. Sarà possibile un'analisi immediata: se la difformità rispetto alla normativa (per esempio, un'erronea interpretazione) si trovava già nello schema in lingua italiana, la responsabilità sarà del funzionario pubblico che lo ha sottoscritto; se la divergenza è sopravvenuta in un momento successivo, essa sarà da attribuirsi al tecnico che ha elaborato il software».

[46] A. Usai, *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, cit., 183.

[47] F. Saitta, *Le patologie dell'atto amministrativo elettronico,* cit., 19, per il quale utilizzando «le considerazioni di ordine generale sull'esigenza di intendere la volontà insita nel provvedimento amministrativo come volontà procedimentale e sulla riferibilità all'autorità procedente anche della volontà dell'atto informatico, ci sembra possa condividersi l'affermazione che il software, rappresentando un semplice strumento di ausilio al perseguimento dell'obiettivo che l'agente si è proposto, può essere adottato anche per elaborare atti a contenuto discrezionale: questi ultimi, infatti, potranno ritenersi consapevolmente voluti quando colui che li sottoscrive ha volontariamente assunto quel determinato programma per produrre l'atto in quella determinata circostanza ed alla presenza di quei determinati presupposti».

per un errato funzionamento dell'algoritmo[48], come parrebbe accaduto nel caso della scuola, in cui le proposte di assunzione si ponevano in palese contrasto con i criteri e l'ordine di priorità dettati dalla legge, o di provvedimenti discrezionali irragionevoli, tanto ove la discrezionalità sia stata esaurita in sede di predeterminazione dei criteri, tanto ove la scelta sia stata affidata all'algoritmo, si riflette sulla responsabilità connessa all'adozione del provvedimento finale che non può essere di una macchina[49].

Almeno secondo le regole vigenti, occorre garantire la riferibilità della decisione all'organo competente individuato dalla legge[50]. Da ciò il Consiglio di Stato, con la sentenza della sez. VI, n. 8472, del 13 dicembre 2019, fa derivare un principio di strumentalità dell'informatica alle procedure amministrative, che presuppone sempre un controllo a valle della legittimità della decisione da parte dell'organo competente.

La decisione algoritmica si atteggia a "proposta" di provvedimento, anche alla luce di un immediato parallelismo con la previsione dell'art. 6, l. 241/1990, lett. e), ai sensi del quale «l'organo competente per l'adozione del provvedimento finale, ove diverso dal responsabile del procedimento, non può discostarsi dalle risultanze dell'istruttoria condotta dal responsabile del procedimento se non indicandone la motivazione nel provvedimento finale», possibilità riconosciuta proprio perché, nonostante l'istruttoria sia condotta dal responsabile del procedimento e sia quest'ultimo a formulare una proposta di provvedimento, la responsabilità degli effetti dell'atto è imputata all'organo competente individuato dalla legge (chiaramente ove diverso dal responsabile del procedimento)[51].

La decisione algoritmica non coinciderebbe con la decisione finale[52], ma confluirebbe in quest'ultima solo a seguito della verifica (o della decisione di "non verificare", pur sempre adottata nell'ambito della propria responsabilità) da parte dell'organo compe-

[48] Il provvedimento non potrebbe che essere illegittimo non soltanto ove le istruzioni fornite a monte fossero errate, ma anche in caso di difetti di programmazione o malfunzionamento.

[49] M.C. Cavallaro – G. Smorto, *Decisione pubblica e responsabilità,* cit.

[50] Si v. a tal proposito Cons. Stato, sez. V, n. 8472 del 13 dicembre 2019, che richiama la Carta della robotica approvata nel febbraio 2017 dal Parlamento europeo nella parte in cui, in particolare, chiarisce che «nell'ipotesi in cui un robot possa prendere decisioni autonome, le norme tradizionali non sono sufficienti per attivare la responsabilità per i danni causati da un robot, in quanto non consentirebbero di determinare qual è il soggetto cui incombe la responsabilità del risarcimento né di esigere da tale soggetto la riparazione dei danni causati».

[51] Circostanza che non parrebbe sufficiente a disconoscere l'importanza del responsabile del procedimento, che svolge comunque un ruolo imprescindibile per lo svolgimento del procedimento, soprattutto nella gestione dei rapporti con i soggetti partecipanti. Si v. anche D.U. Galetta – J.G. Corvalán, *Intelligenza artificiale per una pubblica amministrazione 4.0,* cit.

[52] D.U. Galetta – J.G. Corvalán, *Intelligenza artificiale per una pubblica amministrazione 4.0?,* cit., 14, affermano che «l'uso di sistemi di Intelligenza Artificiale è immaginabile (ed accettabile) soprattutto con riguardo alla fase istruttoria del procedimento amministrativo. Sicché, si può immaginare che questo debba concernere essenzialmente le attività interne alle Pubbliche Amministrazioni (c.d. back-office) e che non consistono, dunque, nell'emanazione di atti provvedimentali a rilevanza esterna». Per M.C. Cavallaro – G. Smorto, *Decisione pubblica e responsabilità,* cit., 14: «l'algoritmo dovrebbe costituire il presupposto su cui la decisione si fonda, secondo il modello, già noto, dell'apprezzamento tecnico come presupposto del provvedimento amministrativo. Così interpretata, la questione rimanda al tema classico e assai discusso del rapporto tra tecnica e amministrazione, che a sua volta trova soluzione nella nozione di discrezionalità tecnica. […] la discrezionalità tecnica non necessariamente comporta una ponderazione comparativa degli interessi, bensì tra fatti da accertare alla stregua dei canoni scientifici, tecnici, letterari, artistici ecc. Il potere di scelta in ordine allo strumento più idoneo ad assicurare la

tente.

In tal modo, il dirigente competente all'adozione del provvedimento, pure potendo avvantaggiarsi dello strumento informatico idoneo a fornirgli la soluzione "migliore", mantiene il controllo della decisione, irrinunciabile a meno di non volere modificare le regole in tema di responsabilità[53].

Si consideri, d'altronde, che, ove l'algoritmo fosse idoneo a "sostituire" l'organo competente e, dunque, a ridurne la sfera di competenza, non reggerebbe più la tesi, qui accolta, che la decisione di ricorrere allo strumento elettronico costituisca una forma di autoorganizzazione, ma sarebbe necessaria una base legislativa, che sottraesse all'organo originariamente designato il potere di adottare l'atto finale.

Ne consegue che, almeno nella prospettiva *de iure condito*, non si può non riconoscere a chi potrebbe essere chiamato a rispondere degli effetti della decisione la possibilità di discostarsene o, analogamente, di accettarla[54], quand'anche basata su un meccanismo di *machine learning*[55], ove si accogliesse la tesi dell'applicabilità della decisione automatizzata a fattispecie ad alta discrezionalità. Ciò, tuttavia, richiederebbe un livello di avanzamento tecnologico che ancora non sembra maturo[56] e, in ogni caso, a condizione che la tecnologia utilizzata consentisse al software di "gestire" gli (o comunque tenere conto degli) apporti partecipativi e che fosse possibile ricavare dalla decisione le ragioni che ne costituiscono il fondamento, a presidio delle garanzie di trasparenza e conoscibilità.

---

miglior cura dell'interesse pubblico è un potere successivo, che consegue all'esito del giudizio tecnico, laddove questo abbia un esito incerto che apre a più soluzioni. Quando invece l'attività tecnica abbia un esito certo e indiscutibile, la conseguente decisione amministrativa è per così dire "obbligata", pur rimanendo espressione di un potere riservato alla stessa amministrazione. In ogni caso, si può dire che la valutazione tecnica e l'accertamento tecnico operano come presupposto della decisione amministrativa. […] Fuori da una riconduzione della decisione automatizzata nel quadro di una partizione tra attività vincolata e attività discrezionale, la soluzione più ragionevole sembra quella di considerare la procedura automatizzata alla stregua di un accertamento tecnico, che presuppone comunque l'adozione di un provvedimento finale che ne faccia proprio l'esito».

[53] Sull'opportunità di un ripensamento delle regole in materia di responsabilità rispetto ai danni causati dal provvedimento adottato tramite lo strumento elettronico, L. Viola, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, cit.

[54] P. Otranto, *Decisione amministrativa e digitalizzazione p.a.,* cit., paventa il rischio che, in virtù dell'autorevolezza della decisione concepita dall'elaboratore informatico, l'organo competente per l'adozione del provvedimento non si discosti da quella decisione non soltanto nel procedimento cui si riferisce, ma nemmeno nell'ambito di un eventuale procedimento di secondo grado. Addirittura, secondo l'A., 26, «anche la garanzia della tutela giurisdizionale "contro" gli atti dell'amministrazione rischierebbe di essere di fatto fortemente limitata, chiedendosi al giudice di sindacare la legittimità dei provvedimenti adottati da un'amministrazione "tecnicamente impostata" all'osservanza della legge (il che rende residuale l'ipotesi dei vizi di violazione di legge e di incompetenza) e che decide all'esito di un'istruttoria ampia, secondo regole di logica, non contraddittorietà, parità di trattamento».

[55] L'amministrazione si assume la responsabilità dell'utilizzo del software. Secondo A. Masucci, *Procedimento amministrativo e nuove tecnologie*, cit., 97, «l'elaboratore è solo un mezzo a disposizione dell'amministrazione per attuare gli obiettivi definiti dall'amministrazione, dal momento che gli elaboratori elettronici producono la decisione sulla base di un programma definito (o fatto proprio) dall'amministrazione competente per l'adozione dell'atto».

[56] L'adozione di decisioni totalmente automatizzate anche in casi più complessi presuppone un livello di digitalizzazione pressoché totale delle pubbliche amministrazioni (nonché dei mezzi di trasmissione dei dati da e verso il cittadino), ma anche una totale interconnessione e interoperabilità dei dati che l'algoritmo deve esaminare per l'elaborazione della "soluzione" e, quindi, della decisione del caso specifico.

Sono proprio le difficoltà collegate all'esigenza di comprendere il percorso seguito dall'algoritmo e di "spiegare" le ragioni alla base della soluzione espressa[57] a far sì che sia più agevole prospettare la devoluzione a formule algoritmiche di decisioni vincolate dalla legge o per le quali la discrezionalità si esaurisca in sede di predeterminazione della regola giuridica, da tradurre in regola tecnica. Predeterminazione necessaria, al fine di "obiettivare" l'azione amministrativa con riguardo a uno specifico episodio di gestione dell'interesse pubblico[58], in ossequio ai principi di imparzialità e trasparenza, e che, al contempo, consentirebbe di garantire la partecipazione dei soggetti interessati dal provvedimento in una fase più "tradizionale".

Peraltro, né il ricorso all'autolimite, come forma di esercizio anticipato del potere discrezionale[59], né la necessaria ricostruzione, per le ragioni esposte, del "risultato" dell'applicazione della formula algoritmica in termini di proposta di provvedimento, parrebbero contrastare con l'economicità e l'efficienza che l'uso dello strumento informatico persegue, in virtù del risparmio in termini di tempi[60] e oneri che in ogni caso deriverebbe all'amministrazione dal ricorso alla formula algoritmica specialmente in procedimenti cumulativi, come nel caso della scuola esaminato.

Lungi dal "demonizzare" l'evoluzione tecnologica, che può consentire di raggiungere livelli insperati con le sole risorse umane, occorre guardare alla digitalizzazione 4.0[61] con la consapevolezza della necessità di un progressivo adeguamento di istituti pensati per un'amministrazione organizzata e funzionante in maniera diversa da quella verso la quale ci stiamo indirizzando, ma che, in ogni caso, non può rinunciare alla componente umana, che dovrebbe essere valorizzata in considerazione della complessità della funzione amministrativa e non "sminuita", come sembrerebbe derivare da una pretesa sostituzione della persona fisica con la "macchina".

L'algoritmo, così, finisce per restituire valore alla persona, anziché sottrarlo.

---

[57] Su tali difficoltà, da ultimo, M. Macchia, *Lo statuto giuridico dell'algoritmo amministrativo*, Osservatorio sullo Stato digitale, in *irpa.eu*.

[58] La funzione di "obiettivare" l'azione amministrativa costituisce un carattere particolarmente evidente nell'autolimite, in parte presente anche nel diverso istituto delle norme interne. Su analogie e differenze tra le due figure, F. Fracchia – M. Occhiena, *Le norme interne tra esigenze regolative dei pubblici poteri e vincoli dell'ordinamento generale. Un modello teorico-concettuale applicabile anche alle reti e all'intelligenza artificiale?*, Napoli, in corso di pubblicazione, i quali evidenziano come, nel caso dell'autolimite, l'obbligo di esercitare il potere a monte, appunto tramite l'autolimite, deriverebbe dalla legge o dai principi dell'ordinamento e, dunque, dall'esterno, mentre, nel caso delle norme interne, la loro emanazione sarebbe espressione di un bisogno autoregolativo. Di conseguenza, l'autolimite riguarderebbe un ben definito episodio di esercizio del potere, sebbene in fase di avvio, mentre le norme interne si porrebbero all'esterno rispetto all'esercizio del potere.

[59] A. Police, *La predeterminazione delle decisioni amministrative,* cit., 216.

[60] Sull'importanza del rispetto dei termini di conclusione del procedimento, sia consentito rinviare a S. Vernile, *La relatività del tempo (amministrativo): la validità del provvedimento tardivo e la tutela risarcitoria (e indennitaria) tra esigenze di tutela del privato e perseguimento dell'interesse pubblico*, in *Dir. econom.*, 2, 2015, 403 ss.

[61] D.U. Galetta – J.G. Corvalán, *Intelligenza artificiale per una pubblica amministrazione 4.0?,* cit.

Proposal toward "no-fault" civil liability regulation following Artificial Intelligence evolution in health-care*

Emiliano Marchisio

Abstract

Civil liability, in its traditional paradigm based on "deterrence", may be understood as indirect market regulation, since the risk to incur in liability for damages provide an incentive to invest in safety. Such an approach, however, appears inappropriate, beyond a certain limit, in medical liability since its continuous increases are nowadays incentivating more "defensive medicine" than further increases in safety. This disincentive doctors from relying on guidelines and standards which, at the aggregate level, are the safest path of action when compared with all alternatives.

Such a malfunction appears even more serious with respect to the use of artificial intelligence in health-care, which will greatly increase in the next future. In fact, robots and programs may "behave" far independently from instructions initially provided by programmers and constructors. Charging the latter with liability even if the damage derives from a perfectly "correct" functioning of algorithms and robots would maybe not provide any proper "deterrence", because damages would derive from a situation where there is no "fault" or "lack" in safety to blame or prevent. This could provide a disincentive to AI research, development and use, notwithstanding AI devices already show to be the safest choice when compared with all alternatives based only on human action.

Therefore, I propose that the law on redress in health-care, especially when practiced through artificial intelligence devices, should evolve from an issue of civil liability into one of financial management of losses, pursuant to no-fault redress schemes. Of course, such schemes should apply only in cases where there is no evidence that doctors and producers and programmers of AI devices acted in conditions of negligence, imprudence or unskillfulness and their activity appropriately complied with scientifically validated standards. In other cases, traditional civil liability rules would play a sound function of deterrence.

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

As a result, with reference to AI markets, "fault" and "no-fault" systems should co-exist as independent and alternative system of redress (a sort of "double track" legislation on redress for damages), in order to take advantage of the benefits brought by each of them, narrowing their flaws by their reciprocal interplay.

Summary

1. The "traditional" paradigm of civil liability based on deterrence and its different strategies of allocation of the obligation to compensate damages. – 2. Current centrality of the "traditional" paradigm of civil liability based on fault and deterrence. – 3. A contextual analysis within health-care: the "breach" of the "traditional" paradigm showed by defensive medicine. – 4. The further quest for a change of paradigm following the artificial intelligence revolution. – 5. The need for a new paradigm of (medical) civil liability law. Modern risk management and "no-blame" culture. – 6. A new paradigm of civil compensation for (medical) damages: toward evolution of the law of redress from an issue of civil liability into one of financial management of losses. – 7. Implementation of a new paradigm into legal systems. Room for harmonization in EU law. – 8. Beyond medical civil liability and toward a general "law of the horse" for artificial intelligence technologies.

Keywords

civil liability - no-fault - medical liability - health-care - artificial intelligence

1. The "traditional" paradigm of civil liability based on deterrence and its different strategies of allocation of the obligation to compensate damages

The current paradigm of civil liability laws is mainly based on the assumption that civil liability plays and should play an important role in deterrence. It is thought that any increase of liability on producers and suppliers of goods and services will increase investments in safety (because, in this view, higher investment in safety would be aimed at preventing incurring in liability), so that the tougher civil liability rules on producers and other professionals, the higher the overall level of safety within the system[1].

The idea that civil liability should have a function of deterrence presupposes that the obligation to compensate for damages should be allocated onto the person whom the legal systems identifies as the addressee of such deterrence.

Such a paradigm remained substantially constant over time (with very rare exceptions, some of which will be referred to below), even if, as it is examined below, legal sys-

[1] G. Calabresi, *The cost of Accidents: A Legal and Economic Analysis*, New Haven, 1970; R. Cooter - T. Ulen, *Law & economics*, Boston, 2008, 336-338; W.K. Viscusi - J. Hersh, *Assessing the Insurance Role of Tort Liability after Calabresi*, in *Vanderbilt Law and Economics Research Paper,* n. 12-35, 2013; C. Scognamiglio, *Danno morale e funzione deterrente della responsabilità civile*, in P. Sirena (ed.), *La funzione deterrente della responsabilità civile alla luce delle riforme straniere e dei Principles of European tort law*, Milano, 2011, 295 ss.

tems developed different strategies of allocation of the obligation to compensate for damages.

1.1. Back to ancient times: liability based on "fault"

The first, and most relevant, criterion of allocation of the obligation to compensate for damages is that of fault. The idea that redress for damages requires somebody's "fault" is deeply rooted in legal thinking from ancient times: it emerged in Justinian law and was further consolidated in the *jus commune* and canon law[2], beginning a thousand and five hundred years ago.
This idea, until recent times inspiring the whole system of civil liability, was eloquently called, in German literature, the "dogma of fault" (*Verschuldensdogma*)[3].

1.2. Evolution toward solidarity: liability based on "risk"

The above-mentioned paradigmatic centrality of "deterrence" evolved, but remained in place, when most relevant social, political and economic changes made legal thinking evolve toward an increasing quest for solidarity in all western legal systems, regardless of their civil-law or common-law basic structure[4] – even though with all odds inherent to these different traditions, where English law is traditionally less concerned with solidarity in private law than continental civil law systems.
The quest for solidarity, greatly prompted by the factual consequences and upheavals derived after the industrial revolution, brought legislators to consider unjust that damages following certain (intrinsically risky) activities should be borne by consumers and other end-users of goods and services unless a "fault" of producers or other professionals could be proven in court.
It was considered, therefore, that professional producers of goods and services should bear the risk of their activities *regardless* of their "fault" in causation of damages onto their clients and customers. This strategy of reallocation of liability, which evolved throughout the whole XX century, was believed to be efficient and ethically well-founded insofar as such professional producers were (and are) thought to be in a better position to assess the risk of their activities, to spread the cost of accidents and

[2] See, among others: H. Mazeaud - L. Tunc, *Traité théorique et pratique de la responsabilité civile délictuelle et contractuelle*, Paris, 1957, I, 422.

[3] This approach is represented by the well-known espression «*Nicht der shaden verplichtet zum schadensersatz, sondern die schuld*», formulated by R. von Jhering, *Das Shuldmoment im rőmischen Privatrecht*, Giessen, 1867, 40.

[4] See, e.g., in Italy A. De Cupis, *Il danno: teoria generale della responsabilità civile*, Milano, 1979, 66; in France L. Josserand, *Les transports,* in E. Thaller (ed.), *Traité général théorique et pratique de droit commercial*, vol. XVIII, Paris, 1910, 457; in Germany H. Sperl, *Über das Schadenersatzrecht nach dem deutschen bürgerlichen Gesetzbuche*, Wien, 1902, 154; in England see the comments made in M. Lunney - K. Oliphant, *Tort Law Text and Materials*, Oxford, 2000, 15. More in general and in comparative perspective see: S. Taylor, *Differing cultures of civil liability. In Medical Accident Liability and Redress in English and French Law*, Cambridge, 2015.

arrange for appropriate prevention policies[5].

Such evolution brought, among others, to a relevant variation in civil liability legislations (within the same paradigm based on deterrence, I believe), which lead to "asymmetric" discipline of civil liability and to the adoption of loss-spreading strategies for civil liability laws[6]. This new allocation strategy disregarded the concept of "fault" and considered as a criterion of imputation of the obligation to compensate damages the exercise of risky activities, instead.

Under a legal point of view, such an evolution widened liability imposed on professional producers as to include cases where the latter could not show that the damage was not attributable to them, cases where there was scientific uncertainty as to the cause of the harmful effects or even cases where such cause was unknown[7]. This development was pursued through similar techniques in all western legal systems, mainly: the inversion of the burden of proof[8] and the imposition of strict liability on producers and other professionals, the development of the precautionary principle in many fields of application *etc.*.

In medical civil liability the above mentioned move toward solidarity included sector-specific features, such as the imposition of an obligation of results with respect to many treatments and especially routine ones (in English law through the *res ipsa loquitur* doctrine[9], in Germany through the *Anscheinsbeweis* or *prima facie Beweis* doctrine[10] *etc.*). Some jurisdictions even turned extra-contractual medical liability into a contractual one (which favors patients, *inter alia*, as regards burden of proof) following the German doctrine of *Faktischesvertragsverhàltnisse*[11], as it happened in Italy with the theory of "*contatto sociale*"[12].

[5] G. Calabresi, *The cost of Accidents,* cit.

[6] M. Comporti, *Esposizione al pericolo e responsabilità civile*, Napoli, 1965. Under an economic point of view see R.D. Cooter, *Economic Theories of Legal Liability*, in *Journal of Economic Perspectives,* 5(3), 1991, 11 ss.

[7] R. Montinaro, *Dubbio scientifico e responsabilità civile*, Milano, 2012; in an economic analysis of law perspective see: M.G. Faure - L.T. Visscher - F. Weber, *Liability for Unknown Risk – A Law and Economics Perspective*, in *Journal of European Tort Law*, 7(2), 2016, 198 ss.

[8] On the burden of proof and its relevance in medical civil liability see, e.g. in Italy: G. Anzani, *Il riparto dell'onere probatorio nelle due specie di responsabilità civile*, in *Rivista trimestrale di diritto e procedura civile*, 2017, 238.

[9] Cfr. *Donoghue v Stevenson* [1932] AC 562.

[10] M. Stauch, *The Law of Medical Negligence in England and Germany: A Comparative Analysis*, Oxford and Portland (Oregon), 2008, 73 ss.

[11] G. Haupt, *Über faktische Vertragverhältnisse*, vol. 124, in *Leipziger Rechtswissenschaftliche Studien*, Leipzig, 1943.

[12] Italian Supreme Court, 22 January 1999, no. 589, in *Foro italiano*, 122(11), 1999, I, 3331 ss.; see, on this issue: C. Castronovo, *Obblighi di protezione*, in *Enciclopedia Giuridica*, Roma, 1990, *ad vocem*; R. Pardolesi - R. Simone, *Nuova responsabilità medica: il dito e la luna (contro i guasti da contatto sociale?)*, in *Foro it*aliano, 2017, V, 161 ss.

1.3. Further evolution: mandatory reallocation of liability

Legal systems moved even further in the direction of reallocating liability for damages through the adoption of different loss-spreading techniques and strategies, as it happened in all cases where different jurisdiction provided mandatory insurance for producers and professionals of specific goods and services.
In fact, also in this case the traditional paradigm based on (fault and) deterrence, focusing on the relationship between a damaged patient and a culpable doctor or organisation (hospital, clinic *etc.*), is held.
Mandatory insurance, in effect, is mainly thought to protect damaged consumers and other end-users of goods and services from the risk that producers or other professionals have an insufficient patrimony to pay redress *and not* to relieve the latter from deterrence. Therefore, it determines a mere reallocation of the obligation to pay compensation but does not modify the traditional paradigm of civil liability, insofar as producers or other professionals remain liable, may be called to pay redress in case insurance coverage is not applicable and are subject to deterrence indirectly – since insurers would shift onto producers and other professionals (by applying higher insurance premiums) the cost of any redress paid on their behalf.

2. Current centrality of the "traditional" paradigm of civil liability based on fault and deterrence

The evolution briefly recalled above, under § 1, even if relevant and innovative, represented a mere *incremental* advancement of the same traditional paradigm of civil liability based on "deterrence".
In fact, the developments just summarised were limited, basically, only to reallocate the "cost of accidents" from customers and users to producers and professionals (in health-care: from patients to doctors) within the same conceptual and legal framework already in place. What changed, in other terms, was balancing of interests, not rethinking techniques for satisfying them, insofar as the concept of "fault" was conceptually replaced, in some instances, by that of strict liability, simply in order to increase deterrence also to cases where fault could not be positively assessed in court, with the aim of inducing producers and other professionals to increase investments in safety correspondingly[13].
Legislation appears to consider invariably civil liability also for its potential of deterrence, so that new pieces of legislation frequently increase of civil liability as a regulatory technique, in order to foster investments in safety by producers and professionals.
Such an approach to the issue at stake is shown, e.g., in the Principles of European Tort Law (PETL) drafted by the European Group on Tort Law[14], especially as regards

[13] R. Savatier, *Traité de la responsabilité civile en droit française civil, administratif, professionnel, procédural*, Paris, 1945, vol. I, 3; M. Comporti, *Esposizione al pericolo,* cit., 27.

[14] Which may be read online at *civil.udg.edu*.

linking redress to liability to compensate damages [Art. 1:101(1)] and to liability based on fault and "strict liability" only [Title III]. The same approach seems to be upheld by scholars and even sophisticated studies, at supranational level have considered, and still consider, civil liability as performing the central function of *deterrence* along with that of compensation[15].

3. A contextual analysis within health-care: the "breach" of the "traditional" paradigm showed by defensive medicine

It ought to be noted that the paradigm of civil liability based on deterrence showed reliable and appropriate on several instances where empirical analysis indicates, in fact, that the increase of liability determined an incentive of producers and other professionals to invest in safer products and services. This happened, e.g., with reference to general consumer legislation enacted, among many others, through Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products[16].

Such paradigm, however, showed inappropriate in other cases, as health-care. A rich and valuable literature shows, in fact, that the increase of asymmetric protection of patients through increases of medical civil liability does not produce, *beyond a certain limit*, any further increment in safety[17] but, instead, determines the adoption of "defensive" strategies (the so-called "defensive medicine"[18]) and imposes very relevant negative externalities.

In fact, the over-prescription of exams, treatments and medicines determines, even if in different forms depending on the relevant national health system, much relevant increases of costs[19]. This does not benefit patients, paradoxically, since the said over-prescription of exams, treatments and medicines determine an increase of iatrogenic risks and damages, along with "false positive" results.

National health-care systems as a whole do not benefit from massive increase of defensive strategies, which lead to inefficiencies and loss of quality (such as overcrowding of hospital beds and longer waiting lists for medical exams). The constant increase

15 OECD, *Medical Malpractice. Prevention, Insurance and Coverage Options*, Policy Issues in Insurance n. 11, 2006, 27.

16 On this issue it is possible to read, among others, the five reports on the application of Directive 85/374/EEC concerning liability for defective products (1995, 2000, 2006, 2011 and 2018), which may be found online at *ec.europa.eu*.

17 OECD, *Medical Malpractice,* cit., 16.

18 «Defensive medicine occurs when doctors order tests, procedures, or visits, or avoid certain high-risk patients or procedures, primarily (but not necessarily solely) because of concern about malpractice liability»: U.S. Congress, Office of Technology Assessment, *Defensive Medicine and Medical Malpractice*, OTA-H--6O2, Washington, DC, 1994, 1.

19 See e.g., for the USA, M.M. Mello - A. Chandra - A.A. Gawande - D.M. Studdert, *National Costs Of The Medical Liability System*, *Health Affairs*, 29(9), 2010, 1569.

in medical civil liability, moreover, induces corresponding increase of insurance premiums and, in jurisdictions where the amounts of judicial redress are not foreseeable reliably, abandonment of the sector by insurers.
Defensive medicine is also detrimental in its "negative" effects. In fact, fear of claims for redress may lead doctors and hospitals to refuse provision of treatments in particularly serious cases. Looking at the aggregate effects, it is also observed an abandonment of risky specialities by doctors, hospitals and universities.
What is most relevant to note is that, in health-care, beyond certain limits, the current paradigm of civil liability based on deterrence turns completely unreliable, since further increases of civil liability do not procure any gain in safety and, to the contrary and paradoxically, conduce to a reduction of market efficiency and satisfaction of patients, whose interest was pursued by the increase of liability in the first place.

3.1. Excessive liability on doctors and hospitals leads to ... less safe health care. The paradox of wrong incentives

The lesson taught by defensive medicine is that some pieces of legislation, which were thought to foster higher safety in health-care and better risk management, produced exactly the opposite results.
It is undisputed, e.g., that definition of evidence-based safety standards and, therefore, development of reliable guidelines require doctors and hospital to share information on risks, harmful events and latent errors and failures [20]. Several legal systems, however, do not provide doctors and hospitals with appropriate safe-harbours or confidentiality shields which would induce them to share the said information without fearing a claim for compensation. This determines a disincentive to share information, since this may amount, in law, to incur in civil liability.
As an example, a research carried out in 2006-2007 on around a thousand doctors in 18 Italian hospitals showed a shocking result: the great majority of doctors considered Reporting and Learning Systems much useful for their profession but less than half contributed to it providing relevant information fearing legal consequences[21].
Another example. It is undisputed that Evidence Based Medicine (EBM) allows, nowadays, development of most accurate and reliable guidelines whose application is capable of reducing the overall risk of deaths and damages[22]. The technical possibility to gather, process and manage big data, which shall evolve sharply also due to the pursue of open-access and open-data strategies by the EU[23], makes it possible nowadays to

[20] J. Reason, *Human Error*, New York, 1990; C. Bayley, *What medical errors can tell us about management mistakes*, in P.B. Hofmann - F. Perry (eds.), *Management mistakes in Healthcare: Identification, Correction and Prevention*, Cambridge, 2019, 74 ss.

[21] Quoted by S. Albolino - R. Tartaglia - T. Bellandi - A.M.V. Amicosante - E. Bianchini - A. Biggeri, *Patient safety and incident reporting: survey of Italian healthcare workers*, in *BMJ Quality & Safety*, 2010, 19:i8-i12.

[22] See, e.g.: S.A.R. Doi, *Understanding evidence in health care: Using clinical epidemiology*, South Yarra, VIC, Australia, 2012; JH. Howick, *The Philosophy of Evidence-based Medicine*, Wiley-Blackwell, 2011.

[23] In 2003, the European Commission set up a legal framework to allow the re-use of public sector

develop medical guidelines and databases incredibly more reliable[24]. However, current civil liability rules frequently provide doctors with an incentive *not* to apply them, since their respect may not be sufficient to relieve them from civil liability[25].

3.2. A proposal coming from empirical evidence: the need to relieve doctors and hospitals from civil liability when scientifically validated standardised rules are complied with

Having regard to the above arguments, I believe that the current situation requires a (r)evolution of the civil liability paradigm. As noted, after increases of civil liability on doctors and hospitals in the recent past, at this point medical civil liability does not enhance safety and, moreover, imposes severe negative externalities on the whole health care system. Moreover, as a very unexpected consequence, it worsens even the overall safety and satisfaction of patients, which were supposed to receive benefit by the increase of liability itself.

Relevance of this situation is shown by the many attempts, all around the world, to modify current medical civil liability legislations.

I claim that the above reported negative externalities could possibly be reduced if doctors and hospitals could be relieved from civil liability for damages in all cases where there is not evidence of negligence, imprudence or unskillfulness *and* scientifically validated standards of action (guidelines *etc.*) were correctly selected and complied with[26].

information through the so-called "PSI Directive" (Directive 2003/98/EC), last revised in 2013 by Directive 2013/37/EU. Open-data policies include the EU Open Data Portal, set up in 2012, following European Commission Decision 2011/833/EU on the reuse of Commission documents. On these issues see European Commission, *Open data*, at *ec.europa.eu*.

[24] G.H. Guyatt, *Evidence-based medicine*, in *ACP Journal Club*, 114(2), 1991, A-16; Evidence-Based Medicine Working Group, *Evidence-based medicine: a new approach to teaching the practice of medicine*, in JAMA, 268, 1992, 2420-25; D.L. Sackett - W.M.C. Rosenberg - J.A.M. Gray - R.B. Haynes - W.S. Richardson, *Evidence-Based Medicine: What it is and what it isn't*, in *BMJ*, 71(2), 1996, 312.

[25] The problem seems rather well-spread in different jurisdictions regardless of their belonging to either civil law or common law systems. See, e.g., as regards the USA: L.L. LeCraw, *Use of Clinical Practice Guidelines in Medical Malpractice Litigation*, in *Journal of Oncological Practice* 3(5), 2007, 254. In the UK see S. Ash - S. Jo - M. Gunn, *Legal Considerations of Clinical Guidelines: Will NICE Make a Difference?*, in *Journal of R. Soc. Med.,* 96(3), 2003, 133 ss. In French law see E. Hondius (ed.), *The development of Medical Liability*, vol. III, Cambridge, 2010, 76. Under Italian law, Art. 7(3) of the law 8 March 2017, n. 24, expressly provides that respect of guidelines and best practices can be considered by the judge only with respect to the definition of redress and not on assessing civil liability in the first place.

[26] There is much research on the issue of medical guidelines and on the impact they have, or should have, on civil liability. On these issues see, e.g., in Italy: C.M. Masieri, *Linee guida e responsabilità civile del medico*, Milano, 2019; S. Calvigioni, *Linee guida e buone pratiche clinico-assistenziali*, in A.D. De Santis (ed.), *I profili processuali della nuova disciplina sulla responsabilità sanitaria*, Roma, 2017, 216 ss.; M. Franzoni, *Colpa e linee guida nella nuova legge*, in *Danno e responsabilità*, 2017, 278; C. Scognamiglio, *Regole di condotta, modelli di responsabilità e risarcimento del danno nella nuova legge sulla responsabilità sanitaria*, in *Corriere giuridico*, 2017, 740 ss. Comparative remarks are developed in S. Taylor, *Medical Accident Liability and Redress in English and French Law*, Cambridge, 2015. At a European level see: European Committee on Legal Co-operation (CDCJ), *Report on Medical Liability in Council of Europe Member States, A comparative study of the legal and factual situation in Member states of the Council of Europe*, 2005, in *rm.coe.int*; S.D. Ferrara - R. Boscolo-

It is not ignored that respect of standards could determine unwanted damages on patients in some cases. However, my claim is made on the basis of empirical evidence showing that standardisation, whenever possible and sensible, makes health-care systems safer, since following standard actions inspired by Evidence Based Medicine make overall accidents and damages lower than those experienced in a system where standards are not defined or complied with[27].

Said in other words, I suggest that legislations on redress for damages incurred in health care should provide incentives to strict adherence to scientifically validated standards, since this appears a safer strategy than any other.

It is unlikely that the solidarity approach to civil (liability) law, highlighted above under § 1.2, could admit that in such cases damaged patients should be deprived of redress *tout court*. This is why I believe that the proposed "paradigmatic" reform of the law of medical civil liability should be coupled with a "no-fault" redress system – as noted further below, under § 6.

It is reasonable to provide that any reform of civil liability legislation following the above-said principles should not prevent doctors from disapplying guidelines and standards when this appears appropriate in the single case. This should be an exception, however, and disapplication should be appropriately justified.

4. The further quest for a change of paradigm following the artificial intelligence revolution

The quest for (r)evolution of the civil liability paradigm based on deterrence, limiting in this phase our interest to medical liability, is made even more urgent by the so-called artificial intelligence revolution. In fact, such technological advance, along with the already mentioned big data revolution, make it foreseeable that in a relatively short time artificial intelligence shall play an increasingly more relevant role in health care, especially through machine learning and deep learning technologies, also with respect to the forthcoming massive robotisation of medical sector[28].

Devices based on artificial intelligence, however, evolve over time (and will do it much more in the next future) on the basis of the information and feed-back gathered and processed by thousands of different shared sources (so-called "machine learning" and

Berto - G. Viel (eds.), *Personal Injury and Damage Ascertainment under Civil Law*, Switzerland, 2016, esp. 537 ss.; S.D. Ferrara - E. Baccino - T. Bajanowski - R. Boscolo-Berto - M. Castellano - R. De Angel - A. Pauliukevičius - P. Ricci - P. Vanezis - D. Nuno Vieira - G. Viel - E. Villanueva, *Malpractice and medical liability. European Guidelines on Methods of Ascertainment and Criteria of Evaluation*, in *International Journal of Legal Medicine*, 127, 2013, 545 ss.

[27] See, e.g.: A.B. Haynes - T.G. Weiser - W.R. Berry et al., *A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population*, *New England Journal of Medicine*, 360, 2009, 491 ss.; P.G. Shekelle et al., *Making Health Care Safer II: An Updated Critical Analysis of the Evidence for Patient Safety Practices*, Rockville (MD): *Agency for Healthcare Research and Quality*, 2013, which may be read at *ahrq.gov*.

[28] See, e.g.: *Artificial Intelligence and Machine Learning for Healthcare*, Sigmoidal, December 21, 2017, in *sigmoidal.io*; D. Hernandez, *Artificial Intelligence Is Now Telling Doctors How to Treat You*, in *WIRED*, June 2, 2014, which may be read at *wired.com*; PwC (June 2017), *What Doctor? Why AI and robotics will define New Health*, which may be read at pwc.com.

"deep learning"). This process clearly shows that the relationship of cause and effect, as regards causation of damages, may be not linear as we are used to believe. To the contrary, one may consider rather frequent (and even more frequent in the future, due to technological evolution) the possibility that robots and programs "behave" far independently from instructions initially provided by programmers and constructors.
I believe that application of the traditional paradigm of civil liability would determine, in this instance, further negative externalities. Under such paradigm, in fact, redress to damaged patients would require allocation of the obligation to compensate on producers and programmers of artificial intelligence devices (– the only "somebody" available to be imposed strict liability on[29]) either as culpable persons or, by way of strict liability, even without proof of any fault.
It is likely that the first alternative would not be followed, even if this solution is sometimes suggested in law literature[30], since the current solidarity approach[31] would not allow damaged patients not being paid redress unless a fault can be proven in court.
Therefore, it is much likely that strict liability will be the preferred strategy to deal with redress of damages caused by artificial intelligence devices[32]. I claim that this alternative, however, would not necessarily foster safety, since producers and programmers could not do much to foresee unforeseeable "behaviour" of robots and programs, which would be influenced by innumerable variables provided by databases, big data gathering and the end-users themselves.
In my view, therefore, civil liability could possibly induce no relevant virtuous investment in safety because no investment could prevent such kind of risks. On the other hand, the application of the traditional paradigm of civil liability, especially when designed as a strict liability regime, would expose producers and programmers to unforeseeable and potentially unlimited claims for civil liability without any possibility of reducing risks by increasing investment in safety (as far as damages following "unforeseeable" behaviour of AI algorithms are concerned). This would be likely, I believe[33], to disincentive them from entering into the market or developing it, thus hindering technological evolution; or to provide an incentive to move R&D and production into more favourable jurisdictions.
This would be a much relevant negative externality, since new technologies would determine a sensible increase in safety within health-care systems and reduce the overall number and relevance of damages and deaths (as available data already show with

[29] This consequence is highlighted by the significant title of K. Hao, *When algorithms mess up, the nearest human gets the blame*, 2019, in *technologyreview.com*.

[30] See, e.g.: B. Casey, *Robot ipsa loquitur*, in *ssrn.com*.

[31] See above, § 1.2.

[32] In favour of a strict liability regime see, e.g.: L. Buonanno, *Civil Liability in the Era of New Technology: The Influence of Blockchain*, in *European Law Institute,* at *europeanlawinstitute.eu*.

[33] Of course, several alternatives may be (and are) proposed in law literature. In favour of a strict liability regime see above, under footnote 41; in support of the application of the "traditional" paradigm of civil liability based on fault *tout court* see above, under footnote 39. A comparative analysis with reference to the different approaches upheld in the USA, Europe and China may be found in M. Infantino - W. Wang, *Algorithmic Torts: A Prospective Comparative Overview*, Transnational Law & Contemporary Problems, 28, 2018-2019, 309.

respect to the current situation[34]).

4.1. A proposal coming from empirical evidence: the need to relieve producers and programmers from civil liability when robots correctly comply with scientifically validated standardised rules

Current legislations on civil liability may represent a disincentive to the development and expansion of artificial intelligence and to the exploitation of the following benefits.

In fact, the possibility that robots and programs "behave" far independently from instructions initially provided by programmers and constructors led the European Parliament to propose «creating a specific legal status for robots, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons with specific rights and obligations»[35]. I believe that such a proposal is undesirable, since robots cannot and should not be considered as "persons" under current civil legislation[36]. However, it is clear that in such a proposed personality would be mainly used as a legal instrument aimed at circumscribing civil liability onto the robot and, thus, at shifting away all corresponding redress obligations from producers and programmers, in all cases when robots are capable of acting rather autonomously from their original design[37].

Such an issue represent one aspect (one of the most relevant, in fact) within the debate on whether modern technology requires *new specific* legislation or existing legislation and concepts may be adjusted to it; this being the so-called debate on the "law

[34] See, e.g.: K.W. Kizer - L.N. Blum, *Safe Practices for Better Health Care*, in K. Henriksen - J.B. Battles - E.S. Marks et al. (eds.), *Agency for Healthcare Research and Quality (US),* Rockville (MD), *Advances in Patient Safety: From Research to Implementation*, vol. IV, *Programs, Tools, and Products*, 2005, which may be read at *ncbi.nlm.nih.gov*.

[35] European Parliament, Committee on Legal Affairs, *Draft Report with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)), 31 May 2016, § 31, lett. f. See also, e.g.: A. Amidei, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in U. Ruffolo (ed.), *Intelligenza artificiale e responsabilità*, Milano, 2017, 63 ss.; G. Guerra, *La sicurezza degli artefatti robotici in prospettiva comparatistica*, Bologna, 2018.

[36] The issue is very wide and it is not possible to address it here appropriately. A discussion of the issue may be found in G. Wagner, *Robot, Inc: Personhood for Autonomous Systems*, in *Fordham Law Review*, 88, 2019, 591; G. Wagner, *Robot liability*, Münster Colloquium on EU Law and Digital Economy, Liability for Robotics and the Internet of Things 12.3.2018, in *ssrn.com*; H. Eidenmüller, *The Rise of Robots and the Law of Humans*, in *Zeitschrift für Europäisches Privatrecht*, 765, 2017, 771- 772; S. Chopra - L.F. White, *A Legal Theory for Autonomous Artificial Agents*, Michigan, 2011; B.-J. Koops - M. Hildebrandt - D.-O. Jaquet, *Bridging the Accountability Gap: Rights for New Entities in the Information Society?*, in *Minnesota Journal of Law Science & Technology*, 11, 2010, 497.

[37] This need is evidenced in law literature: see, e.g.: M.U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, in *Harvard Journal of Law & Tech*nology, 29, 2016, 399.
As noted below, we claim that such goal should be reached not upholding the current paradigm of civil liability, therefore finding a "culpable" person in the robot, but changing such paradigm, through the adoption of a no-fault system of redress, which would allow compensation to damaged patients independently from the identification of a "person", either producer or programmer (or the robot), to be held liable for that.

of the horse"[38].

Also in this case, as it happened with respect to medical civil liability, it appears that the problems and disincentives evidenced above are somehow connected to the issue of standardisation and standardised action. Therefore I claim that the negative externalities supposedly determined by the traditional paradigm of civil liability on artificial intelligence markets, could possibly be reduced if producers and programmers could be relieved from civil liability for damages in all cases where there is not evidence of negligence, imprudence or unskillfulness *and* the robot (both in its physical components and in its artificial intelligence aspects) complied with production and programming scientifically validated standards.

It is not ignored that mere respect of standards could determine unwanted damages on patients in some cases (which also in my proposed "no-fault" system would be allowed redress, as noted below). However, my claim is made on the basis of empirical evidence showing that in several cases (being destined to increase drastically in the next future) adoption of artificial intelligence and robots determines a relevant increase in safety within health-care systems and reduce the overall number and relevance of damages and deaths when compared to health-care based only on human action[39].

This means that provision of incentives to technological innovation, provided that it respects scientifically validated standards, appears a safer strategy than any other.

5. The need for a *new paradigm* of (medical) civil liability law. Modern risk management and "no-blame" culture

The law binds economic and social activities in order to contribute to the pursue of welfare; on the other hand, however, the law cannot define arbitrarily its goals and (especially) means. It need to take into the highest consideration the real functioning of economic and social contexts addressed, in order to develop well-grounded, affordable, reliable and effective rules[40].

The failure of the current paradigm of medical civil liability legislation based on deterrence, observed and empirically proved, requires a radical modification thereof. A similar evolution toward an alternative *paradigm* might be aimed at also with respect to artificial intelligence markets, which are likely to be prone to similar negative externalities when civil liability is applied as a regulatory strategy based on deterrence.

Such modification, as already observed, appears urgent in these days since it has be-

[38] Such debate may be dated back to F. Easterbrook, *Cyberspace and the Law of the Horse*, in *University of Chicago Legal Forum*, 1996, 207 and L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, 113, 1999, 501. More recently see, among others: R. Calo, *Robotics and the Lessons of Cyberlaw*, in *California Law Review*, 103, 2015, 514; E. Stradella, *Approaches for Regulating Roboting Technologies: Lessons Learned and Concluding Remarks*, in E. Palmerini - E. Stradella, *Law and Technology. The Challenge of Regulating Technological Development*, Pisa, 2013, 345.

[39] See, e.g.: K.W. Kizer - L.N. Blum, *Safe Practices for Better Health Care*, cit.

[40] E. de Jong - M.G. Faure - I. Giesen - P. Mascini, *Judge-Made Risk Regulation and Tort Law: An Introduction*, in *Eur. Journ. Of Risk Research*, 9(1), 2018, 6 ss.

ing harshly influencing the functioning of markets *in the past years*, also by providing incentives to "defensive medicine" and imposing on health-care systems much higher costs for inefficiencies, extra-costs, redress of damages *etc.*. It is going to prevent development of markets toward intensive use of artificial intelligence and robotisation *in the future*, because of obsolete rules that would impose obligation to compensation to producers and/or programmers even in cases where machine learning or deep learning processes are in place and there is no "linear" causation of damage to a given patient. Moreover, it is going to impose on jurisdictions adopting such paradigm a competitive disadvantage in favour of jurisdiction more ready to follow-up with the needs and quests of the markets referred to.

What is surprising is that in branches of research other than law rather similar problems were deeply studied and scholars, on the basis of empirical research, reached the conclusion that risky activities incorporate a certain percentage of risk depending not on the person performing them but on the activities themselves[41]. It is rather a shared opinion, in these sectors, that errors happen and will happen – regardless of how civil liability is severe. This is the reason behind the proposal of discarding the "blame culture", which inspire and underpins current (medical) civil liability law, and replace it, at least in some instances (as briefly discussed below) by a "no-blame culture", rooted in risk management[42] and scientifically validated standardisation.

Notwithstanding literature on risk management is rather consistent on this point, lawyers and legislators seem likewise rather consistent in taking into consideration risk management only when applying existing legal concepts (so they design risk management adapting it to existing concepts), not in order to re-shape them (i.e.: they do not adapt concepts to the needs of appropriate risk management).

6. A *new paradigm* of civil compensation for (medical) damages: toward evolution of the law of redress from an issue of civil liability into one of financial management of losses

At this point a digression is required. It was noted, above, that negative externalities caused in health-care, and likely to be caused in artificial intelligence markets, by the traditional paradigm of civil liability could be reduced if doctors and hospitals, and producers and programmers of artificial intelligence medical devices, could be relieved from civil liability under certain conditions; in particular, when their activity is

[41] T. Aven, *Risk assessment and risk management: Review of recent advances on their foundation*, in *European Journal of Operational Research*, 253, 2016, 1 ss.; J. Aldred, *Justifying precautionary policies: Incommensurability and uncertainty*, in *Ecological Economics*, 96, 2013, 132 ss.; T. Aven, *The risk concept—Historical and recent development trends*, in *Reliability Engineering and System Safety*, 99, 2012, 33 ss.; D.V. Lindley, *Understanding uncertainty*, Hoboken, NJ, 2006; C.E. Althaus, *A disciplinary perspective on the epistemological status of risk*, in *Risk Analysis*, 25 (3), 2005, 567 ss.

[42] See, on this point, the "Swiss cheese model" developed in J. Reason, *The Contribution of Latent Human Failures to the Breakdown of Complex Systems*, in *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences*, 327, 1990, 475 ss.

not negligent, imprudent or unskilled and appropriately complied with scientifically validated standards[43].

Such a relief, however, could not lead to preventing damaged patients and end-users from redress. In fact, especially on the patients' side (which is the case of greatest interest, here), the right to redress for health damages is commonly recognised, in most jurisdictions, as deriving from acknowledged human and constitutional rights to health[44]. Therefore, any such prevention would certainly be inconsistent with the "solidarity" approach which now pervades juridical systems, recalled above under § 1.2.

With respect to this issue, my proposal is exactly that of developing a new paradigm aimed at maintaining redress for damages on the patients' side but shifting away from doctors and hospitals (when scientifically validated standard of action are complied with) and from robot producers and programmers (when scientifically validated standard of production and programming are complied with), the obligation to pay for such redress.

In other words, the law of redress needs to evolve from an issue of civil liability into one of financial management of losses, which would take into a much higher account the "systemic" need of appropriate functioning of complex institutions and markets (as modern health-care systems).

In fact, what could appear to favour single patients in the short run (e.g.: sentencing a doctor to compensate a certain damage suffered by the patient following a very complex surgical intervention, regardless for any negligence, imprudence or unskillfulness being ascertained in court) may eventually damage *all future patients* if it prevents the whole health-care system from functioning appropriately and developing into a more technological, evidence-based and safer system (because of the incentives and disincentives brought about by the sentencing itself; in the above example: doctors would refuse complex surgical interventions *tout court* not to incur in unforeseeable liability).

The possibility of balancing the two apparently conflicting goals noted above is not unknown, since "no fault" legislation on redress following medical damages may be found in some jurisdictions (esp. New Zealand but also Finland, Denmark and Sweden[45]). It is clear that the concept of "no-fault" is used, here, with reference to a system where redress is provided by a dedicated fund and not by a "culpable" or "strictly liable" agent (and not with reference to strict liability schemes, which also prescind from "fault" but operate in the opposite direction, by *imposing* liability on the agent *regardless of any culpability*).

[43] Such evolution was hoped also in OECD, *Medical Malpractice,* cit., 62 ss., however without deepening the issue.

[44] Limiting attention, here, to the international level, the right to health was firstly referred to in the Preamble to the Constitution of the World Health Organization (1946); then included, in Art. 25, in the Universal Declaration of Human Rights (UDHR, 1948) and in Art. 12 of the International Covenant on Economic, Social and Cultural Rights (ICESCR, 1966).

[45] A presentation of such systems may be found, for a first introduction, in OECD, *Medical Malpractice,* cit.

6.1. The need to improve the example coming from "no-fault" legislations

Even if the above-mentioned "no-fault" legislations provide a good example of financial management of losses in health-care markets and valuable ideas for future legislation on artificial intelligence devices, they appear only partially appropriate to reach the goals evidenced above.

First of all, in fact, such pieces of legislation are not targeted to the problem of standardisation but are mainly conditioned to the damaged patient waiving civil litigation, instead. Therefore, being mainly aimed at reducing litigation and "defensive medicine", they have a much narrower scope with respect to the issues dealt with here, in particular, as regards the needs brought about by the discussed technological evolution. I propose, instead, that redress of statistically "inevitable" damages coming notwithstanding compliance with scientifically validated standards, in health-care (especially when coupled with artificial intelligence), should *not* be imposed, in principle, on persons performing the relevant activities or supplying products onto the market.

Said in other words, I believe that, in health-care, legal systems should bear the risk that application of scientifically validated standards could determine harmful consequences in individual cases insofar as, under a systemic point of view, such application allows a significant reduction of the overall risks and damages. This idea is not disruptive the way it seems at a first sight, if one thinks of some small and limited pieces of legislation (without any capability of extensive application by way of interpretation) which provide similar mechanisms of compensation in standardised medical activities bearing some statistical risks but much more beneficial effects: it is the case, e.g., of no-fault compensation following adverse effects attributed to vaccination, where adverse effects are very rare in comparison with the more than 2.5 million deaths prevented only in 2008 by vaccination[46].

Secondly, the pieces of legislation mentioned above are rather different from one another in different aspects and seem targeted to the different jurisdictions where they belong to, so that it appears difficult to transplant them, as they are, into different legal systems. Contextual differences between the exporting and the importing jurisdictions may also determine remarkable differences in the results one may expect from legal transplant. E.g., the simple adoption of a "no-fault" system may not reduce, in itself, excessive litigation (and, therefore, "defensive medicine").

It was noted, in fact, that the rather positive outcome experienced in New Zealand seems to depend on «the absence of a culture of suing in New Zealand» which pre-existed in the country[47]. Such a finding makes it unreliable that introduction of similar legislation could lead to similar results in jurisdiction where civil litigation is much

[46] World Health Organisation, *State of the world's vaccines and immunization*, Geneva, 2009, available on-line at *whqlibdoc.who.int*. On this issue see also: C. Looker - H. Kelly, *No-fault compensation following adverse events attributed to vaccination: a review of international programmes*, *Bulletin WHO*, 2011, on-line at *who.int* where see further references.

[47] K.A. Wallis, *No-fault, no difference: no-fault compensation for medical injury and healthcare ethics and practice*, in *British journal of general practice*, 67(654), 2017, 38–39.

higher and showed increase in the last decades[48]. It is necessary, therefore, to take into account cultural differences between countries and assess how much they may influence the outcome of the proposed reform, if the case developing corrective measures in order to reach the goals aimed at.

Thirdly, "no-fault" legislations are currently showing deficiencies as regards incentives to safety, in absence of the deterrence brought about by civil liability. Pure "no fault" models, in fact, raise concerns as to their appropriateness to limit the risk of moral hazard, exactly as it happens in New Zealand, since «the principal weakness of no-fault schemes is the difficulty of ensuring that the socially optimal amount of care is taken by potential loss-causers, as the links between their potential to cause loss and the costs of their actions are severed»[49].

Any reform toward evolution of the law of redress from an issue of civil liability into one of financial management of losses through "no-fault" systems, therefore, should not apply out of the scope defined above, i.e.: relief from liability in absence of negligence, imprudence or unskillfulness *and* in compliance with scientifically validated standards. Out of this scope, "no-fault" rules would unreasonably remove the deterrence effect that civil liability may still produce. This is why I believe that "no-fault" rules should be combined with "fault" rules in order to take advantage of the benefits brought by each of them, narrowing their flaws by their reciprocal interplay.

Moreover, in all cases where "no-fault" schemes apply, they should be matched with a discipline capable of providing incentives to safety. I believe that such an approach should be uncoupled from deterrence on individuals (e.g.: deterrence induced by civil liability should not be replaced with deterrence induced by disciplinary sanctions on employees) and should rather be inspired by organizational and procedural criteria, thus shifting paradigmatic centrality from individuals to systemic risk management, in adherence to the principles noted above under § 5.

6.2. Open issues and room for further research. Brief remark

The proposed evolution toward a new paradigm of civil liability in health-care, especially when coupled with the use of artificial intelligence devices, requires, of course, solution of many variables, which it is not possible to discuss here.

Among others, it would be necessary to define production of "scientifically validated" standards under the proposed "no-fault" systems. Definition of a third, independent, party in charge with redress to damaged patients in application of a "no fault" scheme, of its functioning and its funding, would also be needed. Similarly, definition of a standardized amount of compensation under a "no fault" scheme should also be provided.

Such issues cannot be discussed here, since this article is aimed at presenting general

[48] OECD, *Medical Malpractice,* cit., 16 ss.

[49] B. Howell - J. Kavanagh - L. Marriott, *No-fault public liability insurance: evidence from New Zealand*, in *Agenda*, 9(2), 2002, 147 and 137.

scopes and principles of my proposal, while the themes briefly listed here constitute rather detailed aspects thereof. However, as regards these aspects, it seems possible to take inspiration, at least in part, from jurisdictions where they were already developed in legislation, such as Sweden and New Zealand[50], even with the cautions highlighted above, under § 6.1.

7. Implementation of a *new paradigm* into legal systems. Room for harmonization in EU law

I believe that the proposal described above could have a strong potential of impact on legal systems. Therefore, I believe that the described development of a *new paradigm* of civil compensation for (medical) damages, from an issue of civil liability into one of financial management of losses, could, and should, have a sequel on public engagement.

Such an engagement would be mainly at national level but it appears that the European Union could develop it within its R&I policy agenda. In fact, EU harmonization of (medical) civil liability law is a rather controversial issue[51]; however, it is possible to highlight that grounding for such harmonization could be mainly based on several provisions of the TFEU, namely: the EU shared competence with member States on consumer protection under Art. 4(2)(f) TFEU; the EU shared competence with member States on safety in public health under Art. 4(2)(k) TFEU; the EU competence to carry out actions to support, coordinate or supplement the actions of the Member States in protection and improvement of human health under Art. 6(1)(a) TFEU; the EU taking into account, in the definition and implementation of its politics and actions, of the need to promote a high level of protection of human health under Art. 9 TFEU; the need that the EU, in defining and implementing any of its politics or activities, takes into account the need of consumer protection under Art. 12 TFEU; the particular relevance recognized to the need of an high level of health and consumer protection, in particular based on new developments based on scientific facts, when EU Commission issues its proposals for approximation of national legislations within the pursue of the goals of the internal market, which apply also to EU Parliament and Council under Art. 114(3) TFEU; the need to guarantee an high level of protection to human health in the definition and implementation of all politics and activities of the EU, in the pursue of the improvement of public health, under Art. 168(1) TFEU.

[50] A. Antoci - A. Fiori Maccioni - P. Russu, *The Ecology of Defensive Medicine and Malpractice Litigation*, *PloS one*, 11(3), 2016, e0150523; P.C. Weiler, *The Case for No-Fault Medical Liability*, in *MD Law Review*, 52(4), 1993, 908; A. Towse - P. Danzon, *Medical negligence and the NHS: an economic analysis*, in *Health Economics*, 8(2), 1999, 93. OECD, *Medical Malpractice,* cit., 13 ss., also mentions the cases of Denmark and Finland.

[51] See, e.g.: F. Toriello, *La responsabilità medica in prospettiva (incerta) di armonizzazione europea*, in *Responsabilità medica*, N2, 2017, 291.

8. Beyond medical civil liability and toward a general "law of the horse" for artificial intelligence technologies

For reasons of methodological stringency, this research was limited, as an exemplary field of investigation, on medical civil liability, where the proposed research address very important challenges. This sector is characterized by great complexity as regards both organisation and service supply, so that it represents a very interesting subject to research in with respect to civil liability. As a matter of fact, medical errors and mistakes are considered as mainly consequences of intrinsic complexity of relevant organisations and markets[52].

Moreover, it relates to the pursue of public health, which is recognised as a human right and a constitutional interest protected in most jurisdictions and legal systems[53] and has the opportunity to evolve, in the next few years, toward a much higher recourse to artificial intelligence and robotisation, which makes it important and urgent for civil liability regimes to adapt to foster such evolution instead of hindering or preventing it.

Finally, health-care is experiencing remarkable negative externalities because of the current regime of civil liability and has a great relevance over public expenditure, since public health appears to take a rather high percentage of the annual GDP in the jurisdictions examined[54] and current inefficiencies and negative externalities contribute to a large extent to such costs.

However, the conclusions eventually reached will aim at providing a new theoretical framework capable of application also to other sectors characterized by similar constraints and needs (as it happens, e.g., in meteorology, engineering, emergency service organisations *etc.*).

In this sense, I believe that no-fault redress schemes should rise, in relevant sectors and with reference to relevant cases, to the role of an independent and alternative system of redress on equal footing to "fault" civil liability – a sort of "double track" legislation on redress for damages. As I noted in dealing with medical civil liability, I believe that this is particularly true for sectors characterised by the so-called artificial intelligence revolution (especially when coupled with machine- and deep-learning), so that I claim that such technologies require a "law of the horse"[55] paradigmatically *different* from regulatory alternatives existing nowadays; a "law of the horse" that should be designed pursuant to a "no-fault" paradigm.

More generally, as a fist approximation, it is likely that my proposal could apply when (cumulative conditions) intrinsically risky activities are characterised by high depend-

[52] J. Reason, *Human Error,* cit.

[53] See above, footnote 44.

[54] With reference to the most recent years available (i.e.: 2016), the World Bank reports that current health expenditure amount to an average of 10.02% of the GDP in the world and 10,22% in the Euro area. More in particular, e.g.: 10,44% in Austria; 9,25% in Australia; 17,07% in the USA; 11,14% in Germany; 10,53% in Canada; 10,36% in the Netherlands; 11,54% in France; 8,97% in Spain; 8,94% in Italy; 9,8% in Portugal; 9,76% in the United Kingdom; 10,04% in Belgium.

[55] See above, footnote 38.

ence on science and/or technology; it is possible to develop reliable standard procedures, based on evidence and scientific method, to carry out these activities; adoption of standards produce, in the exercise of such activities, an overall reduction of negative outcomes when compared with discretionary case-by-case decisions.

"Immuni". Un'*exposure notification* app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*

Marco Plutino

Abstract

Il governo italiano ha fatto costruire una app di notifica delle esposizioni per ridurre il rischio di contagio al Covid-19. Tale app viene esaminata nelle sue fonti di disciplina legale, nelle sue caratteristiche e nei suoi limiti tecnici e di fatto per valutarne l'impatto in termini di limitazione dei diritti fondamentali.

The Italian government has commissioned an exposure notification app to reduce the risk of contagion to Covid-19. This app is examined in its sources of legal discipline, in its characteristics and in its technical limits and in fact to assess its impact in terms of limitation of fundamental rights.

Sommario

1. Il contrasto al COVID-19 tra sicurezza e protezione dei dati in un contesto permeato dalle tecnologie digitali. – 2. L'app Immuni e, in generale, le app di *tracing* e *exposure notification:* norme e politiche dell'Unione e scelte del d.l. 28/2020. – 3. Profili tecnici e giuridici dell'app. – 4. Considerazioni conclusive.

Keywords

contact tracing – pandemia - diritti fondamentali - sicurezza nazionale – diritto alla salute

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo è stato sottoposto a referaggio anonimo.

1. Il contrasto al COVID-19 tra sicurezza e protezione dei dati in un contesto permeato dalle tecnologie digitali

L'emergenza sanitaria dovuta alla circolazione tra essere umani del nuovo virus denominato COVID-19 ha fatto compiere un salto di qualità al tema del ruolo dello Stato in relazione all'impatto dell'innovazione tecnologica nella vita quotidiana dei suoi cittadini. Si è aperta una discussione pubblica sulle potenzialità e le forme di utilizzo della tecnologia per perseguire finalità pubblicistiche che è andata oltre le nicchie in cui era confinata da un po' di tempo, connesse a questioni della sicurezza e della tutela della legalità (intercettazione telefoniche, telecamere a circuito chiuso: CCTV), come ad esempio in riferimento alle modalità di svolgimento del lavoro subordinato pubblico e privato (lavoro "agile", c.d. *smart working*) e alle sue ricadute anche nel campo dell'istruzione e della formazione (didattica a distanza). Del resto l'uso della tecnologia a tutela della salute (*digital health*, ad es. telemedicina) è già massivo, e con il progredire dell'evoluzione tecnologica si porranno e in parte già si pongono delicate questioni relative alla tutela del nucleo essenziale dei diritti fondamentali, come ad esempio in riferimento alle potenzialità e ai limiti della medicina personalizzata e della genomica, alle tecnologie di identificazione a radiofrequenza (RFID, *Radio Frequency IDentification*), con chip apponibili su superfici o inoculabili anche sotto-cutaneamente per diverse finalità possibili fino alla stupefacente frontiera dei MEMS (*Micro Electro-Mechanical Systems*), sistemi elettromeccanici miniaturizzati grandi pochi nanometri, sorta di sabbia tecnologica capace di carpire e trasmettere dati di ogni genere[1].

Entro questo dibattito già da tempo era emerso con evidenza, come nell'ultima questione appena citata, il problema dell'intreccio tra interessi commerciali ed interessi nazionali, di particolare significato quando sono in discussione l'uso di masse di dati che riguardano tendenzialmente l'intera comunità nazionale. Non appare soddisfacente la distinzione che viene spesso effettuata tra tecnologie invasive adottate da parte di soggetti statali o comunque pubblici e quelle adottate da soggetti privati, ed in particolare imprese commerciali. In un mondo in cui le informazioni, e quindi i dati, costituiscono sempre più la base di ogni *business* ed equivalgono pertanto a ricchezza e potere, la tecnologia consente per sua natura ampie possibilità di intrusioni, più o meno volute, più o meno legittime, più o meno concordate, di soggetti formalmente estranei rispetto ai titolari del contratto di utilizzo di una piattaforma, di un sistema operativo o di un software al fine di utilizzare i dati per finalità non istituzionalmente prevista dal contratto o espressamente escluse.

La realtà degli ultimi anni ha offerto un'ampia gamma di queste circostanze, con risvolti talora estremamente preoccupanti. Oggi una parte consistente dell'attività di *intelligence* di uno Stato è assorbita dal cyberspazio, cioè semplicemente dalla Rete, e anche le attività più esplicitamente ostili (c.d. *cyberwar*) avvengono con uso delle tec-

[1] Su alcune di queste tematiche v. ora M. Fasan, *La tecnologia ci salverà? Intelligenza artificiale, salute individuale e salute collettiva ai tempi del coronavirus*, in *BioDiritto – Online First,* 20 marzo 2020, 1 ss., in corso di pubblicazioni in *BioLaw Journal,* 2, 2020 C. Botrugno, *Telemedicina ed emergenza sanitaria: un grande rimpianto per il nostro paese*, ivi, 13 aprile 2020, *passim*.

nologie e non con l'uso di armi convenzionali (campo nelle quali pure si pone il ruolo dell'intervento tecnologico, con particolare riguardo al tema genericamente chiamato "Intelligenza Artificiale"). Del resto, il cyberspazio consente di sovrapporre allo spazio fisico quelli che sono stati definiti nuovi "strati di senso" e di informazione che rivoluzionano la percezione individuale e collettiva circa i luoghi, il loro modo di essere e di fruizione. È pertanto normale che sia gli Stati che i soggetti privati con interessi commerciali nutrano estremo interesse per le sue potenzialità.

La confluenza operativa di soggetti pubblici e privati su un unico terreno di gioco, fortemente permeabile alle incursioni rispetto ai tentativi di alzare protezioni, difese perimetrali di una rete informatica per scongiurare accessi non desiderati alle risorse di un sistema (c.d. *firewall*), pone le questioni della sicurezza informatica tra quelle di cui uno Stato deve prendersi cura per tutelare i propri cittadini. Interessi commerciali e statali sono talora frammisti, talora conflittuali. Entità commerciali possono operare per conto di interessi statali o esser legati da accordi ignoti all'opinione pubblica. Ne deriva che possono essere sostanzialmente unitarie le preoccupazioni e grosso modo unitario dovrebbe essere l'approccio di fronte all'uso di dati (anonimi, personali o sensibili che siano) da parte di soggetti privati o pubblici.

Il nostro ordinamento appare non poco evoluto sul piano dell'approccio normativo e del resto è integrato e coordinato con l'ordinamento dell'Unione Europa che ha fatto della regolazione dei dati, quindi anche della tutela, un tratto identitario del proprio modo di collocarsi nel mondo come "comunità di diritto" e spazio di tutela dei diritti fondamentali, raggiungendo *standard* molto elevati, globalmente riconosciuti. L'Unione appare consapevole che il privato imprenditore possa operare per un tornaconto contrario all'interesse pubblico o come *instrumentum regni* al servizio di interesse pubblici previ accordi occulti. La dotazione da parte di talune entità commerciali di un enorme potere economico e, per così dire, culturale, le fa operare in modo non dissimile da entità sovrane, e del resto quanto più è grande il loro potere di fatto più gli Stati che rappresentano medie o grandi potenze, o gli Stati ove si colloca la base legale di quelle compagnie (che spesso coincidono coi primi) o anche dove l'azienda realizza i profitti, i mercati più remunerativi, cercano di garantirsene i servizi, di trarne vantaggio, o almeno di stabilire un proficuo rapporto.

I mercati remunerativi di queste compagnie sono le comunità e i loro dati, quindi i dati di una comunità nazionale che, senza le opportune garanzie, possono essere trasferiti fuori dai confini nazionali.

Queste grandi compagnie infine per la loro dimensione e il campo d'attività devono devono necessariamente delle super-potenze in tema di sicurezza informatica al fine di tutelare i propri sistemi e i propri segreti industriali. La sicurezza informatica dei sistemi statali e delle imprese nazionali è oggi al cuore del ruolo di uno Stato, parte di una "sicurezza nazionale" e della tutela di interessi nazionali. Ne deriva che gli Stati spesso hanno bisogno del ricorso alle tecnologie di questi giganti (e il tema che tratteremo ne costituisce un esempio) e che queste compagnie spesso cercano riparo e benefici sotto normative nazionali che rappresentano di fatto, e quantomeno, politiche industriali.

Si realizza in definitiva una commistione di interessi e tensioni per cui l'uso delle tecnologie, in particolare concernenti il trattamento dei dati, sul versante privato è

oggetto di interessi commerciali enormi e sul versante pubblico può finire per essere inglobata nella logica per cui "*salus rei publicae suprema lex esto*" e in nome della sicurezza nazionale tutto o quasi (tutto, in paesi non da Costituzioni democratiche) tende a essere considerato come legittimo e giustificato (ancorché non necessariamente legale), sorveglianza di massa incluse.

2. L'app Immuni e, in generale, le app di *tracing* e *exposure notification*: norme e politiche dell'Unione e scelte del d.l. 28/2020

In questo contesto radicalmente nuovo nel quale "abitiamo" (per usare un'espressione heideggeriana ad indicare la necessità di un approccio orientato alla funzione e allo scopo dell'uso delle tecnologie) l'emergenza COVID-19, a cagione della pericolosità di un virus nuovo, non poco contagioso e pericoloso e dai tratti ancora non del tutto conosciuti, ha imposto le risposte maggiormente efficaci compatibilmente con gli assetti di regime. Alcuni Stati hanno da subito contrastando la diffusione del virus con un uso massivo e inedito della tecnologia, anche informatica, dall'uso di droni per scongiurare assembramenti, alla richiesta dei dati delle "celle" telefoniche alle compagnie telefoniche per monitorare i tassi di scostamento delle popolazioni rispetto agli obblighi di contenimento presso il proprio domicilio[2], dall'installazione di applicazioni, basate su diverse tecnologie, con le più diverse funzionalità e talora incidenti, anche pesantemente, su diversi diritti (circolazione, salute, iniziativa economica, riunione ed altri, non escluse finalità repressive) all'uso di tecnologie da parte delle autorità pubbliche molto intrusive come sistemi di videosorveglianza facenti ricorso a rilevazioni biometriche, riconoscimento facciale, fino alle tecnologie diagnostiche e mediche[3].
Sono in particolare le applicazioni - c.d. app - software di grandissima diffusione e fortuna che consentono di attivare funzionalità, servizi o strumenti i prodotti tecnologici su cui gli Stati si stanno concentrando per gestire la fase intermedia di presumibile convivenza con il virus in modo da non nuocere troppo alle ragioni dell'economia, al

[2] Tale via, che richiede la collaborazione non dei c.d. *Over The Top*, ma dei fornitori di linea, quindi delle compagnie telefoniche (c.d. *Telco*), è stato largamente utilizzato, ed anche in Italia da esempio dalle regioni che hanno potuto verificare il livello di spostamenti da parte delle popolazioni mediante il monitoraggio di dati anonimi (quindi non personali) al fine di verificare i tassi presumibili di inosservanza degli obblighi di confinamento a casa durante il c.d. *lockdown*. Questi dati per quanto aggregati e anonimi hanno consentito anche di verificare le tipologie dei luoghi frequentati (es. cittadini in spiaggia, o nei boschi).

[3] Una tecnologia che riprende i vecchi braccialetti elettronici ma rientra già nel c.d. *Internet of things*, consente di misurare le distanze con le radiofrequenze, con intrusioni in parte minori per la privacy (perché non connesso ad app, con le quali può entrare però in relazione). Un simile tracciamento potrebbe monitorare la distanza (anche in casa, aprendo scenari sicuramente problematici), o misurare parametri corporei o, con efficacia, scandire la presenza di persone in luoghi affollati. Tuttavia, una tecnologia di questo tipo richiederebbe attente valutazioni, proprio per il tipo di controllo costante cui darebbe corso, molto simile – soprattutto sul piano simbolico - ad una misura limitativa della libertà personale. Del resto in Cina esso è stato utilizzato per verificare la permanenza domiciliare dove obbligate e ad Hong Kong è stato implementato su soggetti in ingresso nel paese per monitorarne gli spostamenti. Comunque, sul tema un'intervista al Presidente dell'Istituto italiano di Tecnologia, G. Metta, *Premi e bonus per stare distanti: la mia tecnologia soft per la Fase2*, in *Il Sole 24 Ore*, 9 maggio 2020.

benessere collettivo e al godimento stesso dei diritti. Si tratta di realizzare una difficile quadratura tra la necessità di tutelare eterogenei diritti dei cittadini ed assicurare altrettanto vari interessi pubblici, a partire da quelli costituzionalmente rilevanti (tra quali rientra anche la medesima tutela dei vari diritti).

In questo quadro anche l'Italia si doterà di un'applicazione, denominata "Immuni" finalizzata a contrastare la diffusione del virus in funzione delle garanzie di quel difficile e dinamico equilibrio di cui si è appena detto. Il presente contributo ha la finalità di esaminare i profili di impatto sui diritti fondamentali di questa app a poche settimane dalla sua inaugurazione alla luce dello stato attuale delle conoscenze, ormai abbastanza avanzato, al fine di verificare l'adeguatezza rispetto al quadro costituzionale, come si è venuto ormai configurando nel *multilevel government*.

Preliminarmente colpisce, nel quadro europeo, la scelta di soluzioni nazionali a fronte di una libera circolazione dei fattori (del resto in tensione) e delle persone in particolare: infatti anche su questo piano è da verificare come interferiranno le app con le libertà in questione, attualmente stressate. Va però osservato che l'intera fase nella quale i singoli Stati si stanno dotando di queste app è stata guidata dalle istituzioni comunitarie. L'Unione europea non è riuscita ad avere un approccio unitario nel contrasto iniziale del COVID-19 né circa la possibilità di dotarsi di una app unica ostando probabilmente il fatto che in ultima analisi le app potrebbero essere destinate, in fasi per lo più successive, ad essere integrate con database nazionali, gelosamente custoditi dagli Stati. Tuttavia si è rivelata capace, anche con i suoi più precisi parametri e le più compiute normative, di orientare il processo di adozione di queste app e non solo con prese di posizione politiche e orientamenti tempestivamente adottati volti ad ispirano le politiche nazionali. Al momento è da verificare se le soluzioni tecniche diversificate ma simili adottate dai vari paesi europei consentiranno il funzionamento dell'app anche oltre i confini dello Stato adottante (c.d. interoperabilità delle soluzioni), aspetto che pare fondamentale per consentire un ripristino dei movimenti di persona tra paesi UE che in questo momento attraversa una fase di tensione per la diffidenza reciproca tra gli Stati[4].

Tra le normative rilevanti vanno citate la Carta dei diritti fondamentali dell'Unione europea in part. all'art. 52, la risalente direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. "Direttiva e-Privacy"), ancora vigente in attesa dell'adozione di un Regolamento in materia, e il 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 (che abroga la direttiva 95/46/CE; c.d. regolamento generale sulla protezione dei dati, noto anche con l'acronimo "GDPR")[5].

[4] È del resto questa la finalità ultima che ha portata al tentativo di costruire uno standard europeo di cui diremo di seguito. Su questo tema sono state diramate delle indicazioni con un report dell'European Centre for Desease Prevention and Control il 9 aprile ove si prefigura un futuribile progetto comune europeo.

[5] Una disamina sintetica del loro apporto M. Farina, *La* data protection *ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio*, in *BioDiritto – Online First*, 20 marzo 2020, in corso di

Tra le prese di posizioni merita di essere ricordata l'opinione dell'European Data Protection Board (EDPB) che chiarisce i rapporti tra la citata direttiva e il citato regolamento[6]. Un'altra presa di posizione importante è stata quella dei Comitato dei garanti europei il quale ha espresso favore sull'intendimento della Commissione europea di esprimere nella propria proposta l'adozione dell'app su base volontaria nel segno dell'adozione di una responsabilità collettiva, accompagnata pur sempre dalle più ampie garanzie in tema di protezione dei dati al fine di acquisire un atteggiamento di fiducia da parte dei cittadini europei che consente anche una migliore resa della tecnologia. Sullo sfondo l'Unione si sta incamminando verso una normativa organica sull'Intelligenza Artificiale, ad oggi a livello di un Libro Bianco della Commissione (febbraio 2020).

Di seguito si procederà a descrivere le caratteristiche tecniche dell'app "Immuni", a partire dal recente intervento con decreto legge del governo (30 aprile 2020, n. 28), il quale ha tra l'altro offerto una risposta alla prima questione relativa alla base legale di simili restrizioni dei diritti fondamentali con l'intervento di un atto con forza di legge e di cui sarà investito il parlamento in sede di conversione[7]. Il decreto intende fissare alcune disposizioni destinate ad essere in parte integrate con un successivo decreto ministeriale, previo parere del Garante della Privacy. Tale descrizione, inerente ad una materia così tecnica, intende fungere da elementare base di conoscenza al fine di procedere poi a svolgere alcune riflessioni più approfondite. Va infine chiarito che mentre scriviamo non è ancora arrivata la valutazione di impatto del Garante della privacy sull'app[8] ma che l'atteggiamento è stato finora tutt'altro che di chiusura[9] e che d'altra parte la tutela della privacy è solo uno degli aspetti toccati dalla scelta dello Stato italiano di far ricorso a questa tecnologia.

Veniamo alla descrizione di Immuni. Coloro che risiedono sul territorio nazionale (la questione dei soggiornanti occasionali rifluisce tendenzialmente in quella della c.d. interoperabilità delle app) possono installare sui propri sui dispositivi mobili dotati di

pubblicazione in *BioLaw Journal,* 2, 2020.

[6] Dal momento che la prima, pur riguardando le comunicazioni elettroniche, estende la sua portata anche ai trattamenti comuni a diverse tipologie di titolari, come ad esempio l'immagazzinamento di informazioni mediante *cookies* e si pone come *lex specialis* volta a precisare ed integrare le previsioni generali ora dettate in tema di protezione dei dati personali. Ma che viceversa il GDPR non pone obblighi supplementari rispetto alle materie che sono soggette ad obblighi specifici fissati nella direttiva del 2002, valendo per il resto la previsione dell'art. 173 del Regolamento.

[7] Ad es. C. Mirabelli, *A tempo e controllata dal Parlamento. Solo così l'app tutelerà salute e diritti*, in *Avvenire*, 24 aprile 2020. Si badi che l'autore fa riferimento all'art. 16 Cost. e alla riserva ivi contenuta per motivi sanitari; quindi parla anche della limitazione in punto di privacy che afferma dover essere proporzionata all'obiettivo. L'app per come attualmente configurata non ha la potenzialità, indicata dal giudice emerito, di tracciare gli spostamenti.

[8] E' stato reso un parere nel corso di un'audizione informale l'8 aprile 2020 dove sono state espresse preferenze che appaiono sostanzialmente confermate dalle attuali scelte.

[9] Ad esempio, il Garante ha consentito alla Protezione civile di scambiare dati sensibili con altri soggetti come forze dell'ordine, comuni, enti, anche privati, sia quale comunicazione di dati sanitari sia al fin arginare la trasmissione dei contagi, con quello che è stato, ed è, null'altro che un tracciamento svolto senza l'ausilio di tecnologie. V. d.l. 14/2020, disponente una deroga al regime ordinario di gestione dei dati personali.

sistemi operativi[10] l'applicazione software in parola. L'installazione è su base volontaria e il mancato utilizzo «non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento» (art. 6, c. 4)[11]. Prima di attivare l'app gli utenti ricevono informazioni «chiare e trasparenti, al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudo-anomizzazione utilizzate e i tempi di conservazione dei dati» (art. 6, c. 2, lett. *a*); sul concetto di pseudo-anonimizzazione cfr. *infra*). Per quest'ultimo aspetto è previsto che la conservazione dei dati relativi ai contatti, conservati «anche nei dispositivi mobili degli utenti», sarà limitata al «periodo strettamente necessario al trattamento», deciso dal Ministero della Salute, e i «dati sono cancellati in modo automatico alla scadenza del termine» (art. 6, c. 2, lett. *e*), in ogni caso con la decretazione della cessazione dello stato di emergenza (disposto con delibera del Consiglio dei ministri del 31 gennaio 2020) o entro il 31 dicembre 2020, quando in alternativa alla cancellazione può essere disposta la trasformazione in dati anonimi di tutti i dati personali trattati.

Il Ministero della Salute è infatti il titolare del trattamento dei dati e si coordina in ragione delle competenze con una vasta serie di soggetti pubblici per gli ulteriori adempimenti necessari alla gestione del sistema (art 6, c. 1) e relativamente allo stadio di avanzamento del progetto (cit.). Per quanto riguarda le finalità del sistema, e in conseguenza circa le finalità dei dati raccolti, i dati sono quelli necessari ad "allertare" gli utenti entrati in una esposizione a rischio con soggetti (a loro volta, evidentemente, utenti e utilizzatori dell'app) positivi al virus, al fine di consentire nei loro confronti, alle condizioni che descriveremo analiticamente, l'eventuale adozione nei loro confronti delle misure di limitazione dei diritti previste dall'ordinamento e delle misure di assistenza sanitaria (art. 6, c. 2 e lett. *b*). I dati raccolti non possono essere trattati per finalità diverse da quelle indicate, salvo l'utilizzo in forma aggregata o comunque anonima, per fini di sanità pubblica, profilassi, statistici e di ricerca scientifica (art 6, c. 3, con rinvio agli art. 5, par. 1, lett. *a)* e, par. 2, lett. *i)* e *j)* del Regolamento (UE) 2016/679).

I dati di prossimità dei dispositivi saranno resi anonimi o, «ove ciò non sia possibile», pseudo-anonimizzati, e in tal caso vanno adottare misure adeguata ad evitare il rischio di re-identificazione degli interessati cui si riferiscono i dati pseudo-anonimizzati oggetto di trattamento (art, 6, c. 2, lett. *d)*, il quale afferma che devono essere garantite «su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento»); viene esclusa in ogni caso il ricorso alla tecnologia della geolocalizzazione (art. 6, c. 2, lett. *c*). La valutazione di impatto viene «costantemente aggiornata» e vengono adottate dal Ministero della Salute le misure tecniche e organizzative idonee a garantire «un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati», sentito il Garante per la protezione dei dati perso-

[10] Per la telefonia mobili, i c.d. cellulari, occorre pertanto uno smartphone. Il rifermento ai sistemi operativi non costituisce solo un vincolo tecnico per l'installazione dell'app ma come si vedrà è gravida di conseguenze sul piano dell'architettura e delle funzionalità dell'app.

[11] La circostanza era già stata anticipata con nota del Ministro per l'Innovazione tecnologia e la digitalizzazione del 21 aprile 2020.

nali (art. 6, c. 2)[12]. I diritti degli interessati possono essere esercitati anche con modalità semplificate (art. 6, c. 2, lett. *f*).
La piattaforma che gestisce il sistema è di titolarità pubblica, realizzata dal Commissario straordinario di governo per l'attuazione e il coordinamento delle misure occorrenti per il contenimento e contrasto dell'emergenza epidemiologica COVID-19 esclusivamente ricorrendo a infrastrutture localizzate sul territorio nazionale, gestite per quanto riguarda i profili attinenti ai dati dalla "Sogei", società *in house* del Ministero dell'Economia, e per quanto riguarda la tecnologia sottostante all'app da "Pago s.p.a.", interamente partecipata dallo Stato, realizzatrice dell'infrastruttura PagoPa (sistema nazionale dei pagamenti a favore della P.A.). Quanto ai programmi di titolarità pubblica sviluppati per la realizzazione della piattaforma e l'utilizzo dell'applicazione «sono resi disponibili e rilasciata sotto licenza aperta» (art. 6, c. 5; c.d. "*open source*", del tipo noto come MPL 2.0).

3. Profili tecnici e giuridici dell'app

La descrizione il più possibile piana delle soluzioni normative consente di approfondire alcune questioni. Il rischio che una limitazione dei diritti fondamentali, da meglio specificare, avvenisse come una base legale discutibile e insufficiente, comunque non di rango legislativo, lasciando il parlamento emarginato dal circuito decisionale, è stato fugato e la questione è stata affrontata con una fonte adeguata e dai contenuti abbastanza dettagliati.
L'app prevede che il contratto possa essere stipulato solo da persone che abbiano compiuto i 14 anni, i quali dovranno accettare la *privacy policy* e i termini di servizio. L'adozione volontaria, con cui è da intendere tanto, presupposta la gratuità per l'utente, il *download* facoltativo[13] che l'istallazione e l'uso volontario, sono certamente da intendere in prima battuta come un'espressione di libero consenso ad una eventuale limitazione dei diritti che ne consegue.
Le finalità dell'app, un aspetto determinante per valutare necessità, adeguatezza e proporzionalità delle limitazioni, è espressamente finalizzata ad una ricostruzione il più possibile tempestiva e accurata delle catene epidemiologiche. Non si tratta di una generica app "*contact tracing*" in quanto traccia "eventi" ben qualificati, e non generici "contatti" (i quali pure sono tecnicamente eventi) nè, tantomeno, "movimenti". Sarebbe pertanto più opportuno parlare, allo stato delle funzioni, di una app di *exposure notification* o, quantomeno, di mero *proximity tracing* con esclusione del *tracing* in quanto tale, che richiederebbe la geolocalizzazione quale tecnologia in grado di conoscere non solo il "se" del contatto ma anche il "dove"[14]. Occorre naturalmente specificare

[12] Che la questione non sia peregrina è dimostrato da un attacco hacker ricevuto dall'app Covid 19 Alert! predisposta con funzioni simili dal governo olandese.

[13] In opposizione al *download* automatico realizzato dal sistema in occasione di un apposito aggiornamento. Alcuni dispositivi presenti, se non sul mercato, tra gli utenti non ricevono più aggiornamenti e a questo problema tecnica andrà trovata una soluzione.

[14] La geolocalizzazione, come sappiamo dalla tante app private che si basano su di essa, ha straordinarie potenzialità che tornerebbero molto utili anche per un migliore contrasto al virus potendo indicare ad es.

quale tipo di esposizione venga rilevata. A questa funzione essenziale e basilare si potrebbero aggiungere funzionalità per garantire tramite l'app un'assistenza sanitaria per soggetti a rischio di contagio. Un'anticipazione di queste funzioni, allo stato assai poco intrusiva, è data dalla richiesta al primo accesso dell'app, da soddisfare sempre su base volontaria, di inserire la provincia di residenza dell'utente al fine di consentire alle autorità sanitaria di mostrare informazioni rilevanti a livello locale all'utente se gli venisse notificato un contratto a rischio (v. *infra)* e di contribuire alla tracciatura del quadro epidemiologico da parte delle autorità locali e del Ministero della Salute, titolare dei dati.

La volontarietà che presiede alla costruzione del sistema appare espressione del principio di autodeterminazione che è fondamentale in quanto proiezione della dignità della persona[15]. Allo stesso tempo è però da ribadire che se tale via è preferibile a condizione che l'efficacia della tecnologia sia preservata (su questo aspetto v. *infra*), allo stesso tempo non v'è dubbio in generale limitazioni dei diritti fondamentali possano anche prescindere dal consenso per finalità pubbliche e che in questa ottica il Regolamento europeo sui dati personali consente senz'altro di prescinderne per ragioni di salvaguardia della salute pubblica e per molte altre ragioni (v. art. 23 GDPR; v. anche artt. 6 e 9[16]).

La differenza tra dati anonimi, che non sono personali, e pseudo-anonimi, che sono dati personali sono basati su un ID e comunque attribuibili ad un individuo, che resta perciò individuabile attraverso il ricorso a informazioni aggiuntive, ci porta ad un aspetto tecnico di rilievo, ovvero la cifratura che attraverso un controllo con la matrice consente di risalire al nome e al cognome di una persona o comunque ad individuarlo con certezza[17]. Queste informazioni aggiuntive sono conservate separatamente e anche laddove con disposizione non proprio cristallina si afferma che i dati «resi anonimi oppure, ove non sia possibile, [siano] pseudoanonimizzati» sono previste precise garanzie per evitare che il soggetto in questione (il soggetto a rischio di contagio) possa essere identificato dalle autorità pubbliche (e non solo). Per comprendere meglio la questione occorre descrivere anche un altro profilo problematico

la qualità del contatto, la tipologia dei luoghi dove è avvenuto, la dislocazione dei focolai, consentendo facilmente la realizzazione di grafi e così via. Tutte realizzazioni che si cercherà per quanto possibile (e spesso non sarà possibile) di replicare anche con tecnologia *bluetooth* e con dati decentralizzati. Tuttavia, la geolocalizzazione con le sue potenzialità potrebbe impattare con il principio di proporzionalità e necessità di cui agli art. 8 CEDU e artt. 7 e 8 CDFUE.

[15] G. Pitruzzella – O. Pollicino, *La via europea tra libertà e solidarietà*, in *Il Sole 24 Ore*, 28 aprile 2020.

[16] Nonché il considerando 46 che recita: «Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana».

[17] È stata espressamente esclusa qualunque forma di attingimento ai dati della rubrica, alla conoscenza del numero di telefono su cui è installata l'app, come l'invio di SMS quali forme di notifiche, le notifiche essendo interne all'app.

per fare qualche considerazione d'insieme. Appare non del tutto chiaro il riferimento alla conservazione dei dati relativi ai contatti tra i dispositivi mobili nei medesimi ovvero "anche" sui dispositivi degli utenti, lasciando intendere che altra è di regola la conservazione. La disposizione non si riferisce ad una trasmigrazione di dati e loro conservazione presso un server centrale, in quanto la scelta per la decentralizzazione, ovvero di dati conservati sui dispositivi, ha sciolto molto chiaramente il dilemma decentralizzazione/centralizzazione (su server)[18], una delle principali questioni di cui si è occupato il dibattito pubblico e di cui si è interessata l'Unione europea (sono possibili del resto soluzioni intermedie). Alla fine, si è optato per la soluzione decentralizzazione, con dati confinati negli smartphone, del tipo Dp3T, *Decentralised Privacy-Preserving Proximilty Tracing*. Il riferimento a tali dati che passano su server come ai dati che non sia possibile rendere anonimi (quindi pseudo-anonimi) si dovrebbe chiarire alla luce della creazione di una piattaforma informativa finalizzata a gestire il sistema di allerta ed integrata, per le ulteriori finalità, con le «ordinarie modalità in uso nell'ambito del Sistema sanitario nazionale» (art. 6, c. 1). Questa integrazione non è forse sufficientemente chiarita dal decreto legge, e del resto occorrono provvedimenti attuativi, ma si può provare a descrivere il funzionamento specifico dell'app allo stato attuale (e quasi definitivo) delle conoscenze.

Il soggetto A scopre di essere positivo *aliunde* e non grazie all'app. L'app infatti come abbia detto non fa diagnosi ma notifica rischi accompagnate da informazioni. Il positivo che decida di utilizzare l'app può risolversi, senza averne obbligo, di inserire questo stato nell'app, entrando in un sottomenù dove visualizza una password temporanea (*one time password*). Il soggetto prende contatto con l'operatore sanitario (ad es. per via telefonica) e lo comunica al fine di essere inserito nel server, e così ecco chiarito al riferimento al server, che tornerà anche di seguito. Dopo l'inserimento il soggetto positivo valida la password e fornisce il consenso all'invio definitivo dei dati. I dispositivi degli altri scaricano quotidianamente dal server la lista dei codici dei positivi (dati pseudo-anonimi). Se l'app riconosce tra i codici della propria memoria quello di un positivo – ad esempio il soggetto A - visualizza una notifica all'utente, che attesta una situazione di rischio di contagio in quanto esiste un "tek" (una chiave a 16-bit di esposizione temporanea, *temporary exposure key*), ovvero un collegamento di esposizione tra i due soggetti nei 14 giorni antecedenti. Tale esposizione è riconoscibile e rilevata dal sistema solo nei limiti dei segnali inviati e ricevuti (che implica un riferimento spaziale) e del tempo (la durata) dell'esposizione, che sono parametri fondamentali sia per valutare l'efficacia dell'app che la sua capacità di operare conformandosi al sistema dei diritti fondamentali. L'adozione di un sistema con codici crittografati, generati casualmente, a ripetizione, rendono praticamente impossibile l'abbinamento tra il codice e la persona dell'utilizzatore del dispositivo[19]. A questo punto il soggetto B ottiene una notifica (non dal server ma direttamente dall'app) di essere entrato in contatto ed a

[18] Variamente graduabile. Ad esempio, la Germania aveva optato per un sistema semi-centralizzato, con alcuni solo dei dati conservati presso server, anche se poi ha dovuto rimettere in discussione la scelta perché l'ingresso di Google e Apple, con le API, hanno spinto verso l'adozione di sistemi decentralizzati.

[19] Nella versione precedente il dispositivo riceveva direttamente la notifica dal server di essere soggetto "a rischio", con più evidente centralizzazione dei dati.

rischio contagio, ma non sa quando ciò sia avvenuto e chi sia il soggetto in questione. Il rischio viene calcolato, secondo un algoritmo integrato nell'app, dal dispositivo. L'utente potenzialmente positivo alla luce della ricostruzione della catena del contagio riceve a sua volta informazioni e istruzioni dalle autorità sanitarie tenuto conto della sua provincia senza divenire identificabile[20].

Con successive funzionalità l'app potrebbe essere utilizzata per comunicare con le autorità e ricevere cure personalizzate ma tali funzioni sono da implementare con attenta cura alle modalità di realizzazione e alle implicazioni, quantomeno se si vogliono preservare i caratteri attuali dell'app. Attualmente spetterebbe a colui che si venisse a trovare a rischio di contagio di seguire le istruzioni dell'autorità sanitaria locale ed eventualmente prendere contatto, senza avere alcun obbligo di farlo (ma del resto avendone convenienza), con il sistema sanitario.

Pertanto, ipotizzando che il soggetto A abbia conosciuto di essere positivo da una sintomatologia a cui è seguito un tampone (o da una politica pubblica di tamponi) grazie alla sua (eventuale) segnalazione tramite app i soggetti B, C, D, ... avranno appreso con un segnale ricevuto via dispositivo di essere stati esposti al possibile contagio. Come si vede non si tratta di una vera e propria ricostruzione della catena di contagio se non limitatamente a chi è entrato in diretto contatto da un positivo, in quanto non appare possibile risalire a coloro che hanno avuto contatti con i potenziali contagiati, salvo che a loro volta non prendano contatto con le autorità e prestino consenso, nelle modalità già viste, all'invio di ulteriori *alert*. La finalità dell'applicazione è di contenere la diffusione del COVID-19 attraverso un'informazione che può condurre ad una diagnosi precoce e, prima ancora, ad adottare cautele nella vita quotidiana al fine di non esporsi a rischi. Appaiono pienamente rispettate le indicazioni del "Comitato europeo per la protezione dei dati" secondo cui anche di fronte ad un'emergenza pubblica vanno osservati necessità, proporzionalità, limitazione delle finalità e stato di diritto. Ci si può anzi chiedere se sussista un'adeguatezza della strumentazione predisposta rispetto agli obiettivi comunque di grande pregio costituzionale. Sul punto torneremo, ma va ricordato fin da ora che l'app è solo uno degli strumenti a disposizione e che in ogni caso la ricostruzione delle catene di contagio potrà proseguire a partire da un positivo nelle modalità attualmente (fisiche, per così dire) perseguite.

In una fase successiva si potrebbe arrivare ad una cartella sanitaria (o fascicolo sanitario) e prendendo contatto con il sistema sanitario si entrerebbe in un sistema nazionale di diagnostica e cura, l'app fungendo anche da diario clinico. Il Commissario Arcuri ha affermato che «sarà necessario che [l'app] si possa connettere con il Servizio sanitario, che dia informazioni perchè si possa intervenire tempestivamente ed efficacemente» lasciando intendere come la prima fase dell'app potrebbe non essere sufficiente e che nel tempo saranno rilasciate altre funzionalità.

Allo stato il soggetto potrebbe continuare a circolare liberamente senza alcuna diagnosi e quindi tendenzialmente senza poter essere monitorato, se non lo voglia, e senza poter subire una sanzione per il suo comportamento. Mentre se per qualche ragione avesse una diagnosi di positività sarebbe sottoposto a precisi obblighi a prescindere

[20] Siamo fuori dall'ambito del c.d. "caso sospetto", di cui alla circolare del Ministero della Salute del 9 marzo 2020. V. anche circolare del 20 marzo 2020.

dall'app e tra di essi non sopravverrebbe quello di utilizzare l'app, con tutto ciò che ne consegue.

Il processo complessivo appare in linea e forse leggermente scarso rispetto alle indicazioni OMS, le quali affermano: «trova il contagiato, isolalo, testalo, tratta ogni caso e traccia ogni contagiato» (le famose tre T: *testing*, *tracing*, *treating*)[21]. L'app ruota sui positivi e consente di trovare i contagiati ma senza che l'autorità pubblica lo sappia, affidandosi per questo alla responsabilità dell'individuo, sul quale non incombe un obbligo di auto-segnalarsi, e sulla fiducia che essa può suscitare.

In termini di garanzie sulla tutela dei dati personali, attualmente queste garanzie sono pressocchè assolute. I dati di prossimità delle app che si incrociano tra loro possono dare origine a dati potenzialmente sensibili[22], in quanto relativi a condizioni di salute, ma i dati sono crittografati (anonimizzati) direttamente sui dispositivi (e non su server). Ad un certo punto sono destinati a diventare veri dati personali (pseudo-anonimi) in quanto il ruolo di un server (pubblico) è di diramare la lista dei codici anonimi dei contagiati. Non c'è un server che disponga insieme degli identificativi dei dispositivi (i codici ID) e delle chiavi di crittografia.

Nelle ultimissime "demo" dell'app i dati anonimi volontariamente messi in condivisione dall'utente tramite l'inserimento della provincia di appartenenza possono essere condivisi dal titolare del trattamento dei dati con gruppi di ricerca in forma aggregata e anonima e per scopi di ricerca, come per scoprire altri aspetti del virus (ad es. le caratteristiche all'area aperta). Si tratta di virtualità rese semplici da scelte di centralizzazione dei dati ma che anche con un sistema decentralizzato non precludono attività significative come la realizzazione di grafi sociali rappresentativi dello stato dei contagi.

Un aspetto davvero problematico è che la natura volontaria dell'app cade in un contesto tecnologico e culturale, quello italiano, non dei più innovativi e avanzati. Solo il 66% delle persone ha uno smartphone e solo il 53% di costoro installa la più nota app in uso. La volontarietà dell'app riguarda ogni aspetto del processo dalla scelta del *download* al suo utilizzo o al modo in cui la si intende utilizzare. Funzionando con il *bluetooth* l'app può essere con grande facilità attivata e disattivata (senza essere disinstallata). Nessuna penalizzazione è prevista a riguardo, neanche dopo un conclamato stato di positività. Inizialmente sono state offerte stime con modelli matematici e statistici sull'utilizzazione ottimale dell'app al di fuori della possibilità italiane palesate da questi dati. Successivamente il ministro ha fissato informalmente dei *target* molto più bassi in ragione del fatto che la misura interagirà con altre.

Ciò non vuol dire che l'app sia inutile sotto determinate soglie, come affermano molto medici e scienziati. Un siffatto approccio implica un uso del tutto parziale della "razionalità" scientifica, indifferente a vincoli giuridici e al bilanciamento ragionevole tra gli interessi che costituiscono a loro volto esercizio di altre forme razionalità scientifica, di scienze come quella giuridica di discipline come il diritto costituzionale il cui ogget-

[21] V. raccomandazioni del 27 febbraio 2020, frutto della missione congiunta OMS-Cina (16-24 febbraio 2020) e linee guida del 13 marzo 2020. Sul punto G. Perrone, *Il regolamento sanitario internazionale dell'OMS alla prova dell'emergenza COVID*, in *BioDiritto – Online First*, 26 marzo 2020, in corso di pubblicazione in *BioLaw Journal,* 2, 2020.

[22] Appartenente alle "categorie particolari" di cui all'art. 9 del GDPR.

to di studio integra anche parametri teleologici[23].
Da un lato per incapace che possa essere *di per sé* a garantire l'obiettivo massimo potenziale (in caso di utilizzo dell'app da parte di tutta la politica si porrebbero del resto una serie ulteriore di questioni giuridiche e di fatto) l'app può incidere comunque in modo positivo sull'indice di contagio. Essa non nasce certo per "mimare" condizioni simili a quelle dell'immunità di gregge, ma solo per evidenziare l'esposizione ad un rischio. In secondo luogo, è la politica che deve prendere una decisione ragionevole e valutabile in questi termini sul bilanciamento non solo tra diritti ma anche tra possibilità della tecnica (obiettivi potenziali) e soluzioni pratiche alla luce del suddetto bilanciamento.
La questione fondamentale dunque non è tanto che l'app debba condurre ad una stima precisa dei contagiati (censiti e no) perché il suo obiettivo è una più possibile diffusa individuazione precoce dei casi e tracciare, per quanto possibile, le catene di contagio. Dall'app non deve giungere alcuna falsa sensazione di sicurezza e non è una alternativa al distanziamento, vera via maestra per combattere il virus, e del resto ogni app finora, anche quelle più intrusive, è stata sempre accompagnata da politiche specifiche (test sierologici, etc.). Dovrebbe servire per indicare quando il distanziamento non è stato tenuto, si intende nei limiti dei parametri tecnici dettati dalle autorità pubbliche e delle possibilità tecniche.
Semmai problemi derivano da questi ultimi aspetti, ulteriori rispetto al prevedibilmente limitato utilizzo dell'app. La tecnologia *bluetooth* è assai meno offensiva della geolocalizzazione, con la quale la nostra posizione è costantemente segnalata e memorizzata, per non dire dell'incrocio di consimili dati degli smartphone con quelli delle carte di credito o addirittura delle telecamere pubbliche[24]. Con il *bluetooth* e senza ulteriori interazioni con altre tecnologie in via molto generale e generica due persone che si incrociano a distanza ravvicinata sono in condizione di scambiarsi dati con segnali tramite i dispositivi che si cercano con un raggio a intermittenza (*beacon*) e, con il potenziale contatto, riconoscono a vicenda. Se il caso coreano mostra che anche dati in teoria anonimi possono condurre, per circostanze di fatto, a concrete identificazioni da parte di privati, e successivamente dell'opinione pubblica, di positivi o di soggetti a rischio, ma questo rischio è sempre insito nel prodursi di particolari circostanze e non certo esclusivo del ricorso alla tecnologia, il caso di Singapore invece mostra come queste app, di cui Immuni è certamente una versione al tempo più prudente e più perfezionata, portano problemi e non solo benefici. A Singapore non solo l'app è stata poco scaricata dalla popolazione ma anche utilizzata in modo non ottimale, e non ha rilevato la metà dei contagi fino a richiedere un *lockdown* a seguito di una seconda

[23] La sequenza ideata da S. Blackburn, *Filosofia*, Bari, 2011, 112 descrive perfettamente il lavoro di squadra delle scienze: «L'elettrone ha la stessa carica a Londra, Parigi, Dehli e Pechino. Ci è voluto una fortunata coincidenza di forze politiche, sociali, economiche e culturali per consentirci di scoprirlo». Ci sono profili su cui le scienze possono pretendere di avere l'ultima parola, profili in cui solo l'interazione tra le scienze può avere l'ultima parola, e profili dove la politica può avere l'ultima parola sulla base delle risultanze di una scienza o dell'integrazione di diversi contributi scientifici.

[24] Sul punto v. D. De Falco - M. L. Maddalena, *La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia*, in *federalismi.it,* 13 aprile 2020, 2 ss. ove però manca, a dispetto del titolo, un confronto davvero serrato sui profili tecnici caratteristici del caso coreano, il quale del resto sembra contrastare con il principio della minimizzazione delle limitazioni rispetto agli scopi.

ondata di contagi più pesante della prima (per quanto il numero dei decessi sia rimasto limitato).

Nel caso italiano sarà fondamentale una informazione pubblica chiara e trasparente perché paradossalmente mentre si continuano a regalare dati personali a grandi compagnie con i rischi che si è detto in apertura, fanno capolino nell'opinione pubblica correnti di opinioni sfavorevoli a queste "App di Stato" (come se l'auspicabile digitalizzazione della P.A. non si basasse in definitiva su di esse...). A tale proposito, per indugiare ancora sul tema della volontarietà, non dovrebbe essere escluso il ricorso ad incentivi all'utilizzo dell'app, dove l'espressione andrebbe chiarita e specificata visto che in teoria può far riferimento tanto al *download* (o alla istallazione) che all'utilizzo, ma è solo quest'ultimo che interessa effettivamente ai poteri pubblici e che è esposto non solo a pratiche di discontinuità, del tutto legittime, ma verrebbe a rischiare anche potenziali mendacità che senza incentivi dovrebbero essere quasi del tutto escluse[25]. Ogni incentivazione dovrebbe pertanto dispiegarsi senza pregiudicare i caratteri fondamentali dell'app, a partire dall'uso di dati anonimi o semi-anonimi e comunque decentralizzati.

Del resto, l'utilizzo dell'app e il suo gradimento presso i cittadini dipendono anche da alcune specifiche tecniche, come la capacità di non consumare troppa energia della batteria (infatti dovrebbe funzionare in tecnologia BLE, *bluetooth law energy*, come già in altre precedenti esperienze) e sul modo più o meno soddisfacente con cui si integrerà con i sistemi operativi.

Qui sorgono altre questioni specifiche, dove si sono registrati sviluppi nel corso della costruzione dell'app degni di interesse e che in parte abbiamo anticipato. L'app dovrà funzionare in *background*, cioè deve poter restare aperta e correttamente funzionante sullo smartphone anche quando si utilizzano altre funzioni[26].

Per preservare la volontarietà dall'app nel senso pieno dovrebbe essere possibile disattivarne il funzionamento senza disinstallarla, spegnando il *bluetooth;* soluzione anzi prevista di *default* da alcuni sistemi operativi attuali in funzione di risparmio energetico; dall'altro dovrà essere possibile anche prevedere che una volta installata volontariamente possa, sempre su base volontaria, restare sempre attiva (salva sopravvenuta

[25] Restano possibili situazioni particolarissime, al netto di quanto si dirà in conclusione. Si immagini l'ipotesi in cui il dispositivo venga lasciato a casa o su una scrivania a lavoro con il *bluetooth* acceso e un positivo si avvicini per un tempo sufficiente di esposizione. L'*alert* qui darebbe luogo ad un caso di falso positivo. Per il resto, l'incentivo rappresenta senza dubbio una (modesta) incisione sul libero consenso inteso nel senso più rigoroso, ma i veri ostacoli appaiono altri, ovvero che i meccanismi di incentivazione per restare legittimi dovrebbero a loro volta essere conformi alle norme in tema di tutela della privacy ed altri parametri (come le normative anti-discriminazione) per cui ad es. non sarebbe possibile un accredito monetario che dovrebbe interagire giocoforza con altre app che richiedono identificazione, e anche le paventate partecipazioni a lotterie *ad hoc* riservate a coloro che installano l'app dovrebbe avvenire esclusivamente tramite la app e senza pregiudicare la privacy. Si può discutere se debbano essere esclusi alla luce del criterio del«rispetto del principio di parità di trattamento» (art. 6, c. 4, d.l. 28/2020) incentivi basati su categorie ad es. considerate a rischio per condizioni di salute o stili di vita. Tendenzialmente la parità di trattamento, se intesa come principio di eguaglianza e divieto di non discriminazione, nei contesti europei introietta la c.d. regola di giustizia che consente differenziazioni ragionevolmente giustificate.

[26] Una delle ragioni per cui il modello Singapore non ha dato buona prova è che occorreva tenere sempre l'app sempre in primo piano.

volontà contraria, del resto facilmente perseguibile anche con la disinstallazione...). Questi aspetti ci fanno entrare nel merito delle questioni poste dall'intervento delle grandi compagnie tecnologiche, due delle quali sono oligopolisti del mondo dei sistemi operativi per i dispositivi (Android di Google e IOs per Apple). Successivamente ed anche in conseguenza delle prime problematiche offerte dalle app si è prodotta una novità che ha sconvolto non poco anche il processo di ideazione delle app, perchè ha inciso sulla loro architettura in alcuni casi, come in quello italiano, già a processo avviato. Oggi le app sono integrate con i sistemi operativi dei dispositivi mobili, una soluzione praticamente necessitata per un funzionamento ottimale e quindi anche al fine di conquistare la fiducia e simpatia dei cittadini. Inizialmente l'app Immuni ne prescindeva ma i problemi operativi che ne discendevano hanno non solo in Italia portato ad affrontare il problema e sciogliere il nodo alla radice. Le due *big tech* proprietarie dei sistemi operativi hanno stretto una (inedita) alleanza per allineare i sistemi *bluetooth* ai rispettivi sistemi operativi mobili e su quel "framework" hanno proceduto a concludere accordi con i vari governi per mettere a disposizione le proprie soluzioni per una implementazione ottimale delle app nazionali, anche in tal caso stabilendo la natura *open source* di queste API (*Application Program Interface*, ovvero una interfaccia di programmazione; porte che permettono agli sviluppatori di interfacciarsi con il software) dove nome, aspetto, interfaccia e dinamiche di funzionamento sono ampiamente personalizzabili dal programmatore. Ciò ha portato ad una radicale riorganizzazione delle app, le quali in prospettiva potrebbero essere addirittura superate, con necessità peraltro di affrontare gli aspetti legali della questione[27], che si ritrovano una più o meno necessitata interposizione di interfacce che integrano meglio l'app nel sistema operativo. Queste API d'altro canto interagiscono in modo ottimale solo con applicazioni che adottano il sistema di gestione dei dati decentralizzato. Una soluzione tecnica tra l'altro preferita (a scanso di un primo orientamento) dall'Unione europea in quanto foriera di minori rischi perché evita concentrazioni di dati in server, per quanto pubblici, ed ormai praticamente obbligata.

Ma il tema delle API non rileva solo per la scelta della decentralizzazione ma anche perchè il miglioramento funzionale delle app dipende in parte significativa dai programmatori dei sistemi operativi (e delle suddette API) che fanno interagire i sistemi operativi con le specifiche tecniche dei dispositivi mobili. Il punto fondamentale è che sul mercato sono disponibili una varietà enorme di modelli sia pure con un numero limitato di sistemi operativi e questi ultimi si adattano il più possibile alle specifiche del modello in ragione della gamma di prezzo e non solo. Ciò ha condotto ad affrontare diverse questioni, dal modo di *download* dell'app (con l'aggiornamento dei sistemi operativi o meno) al funzionamento ottimale dell'app rispetto ai consumi e al problema del funzionamento in *background*, al modo di ottimizzare la tecnologia prescelta per far "girare" l'app, il *bluetooth*[28].

[27] L'ingresso di Apple e Google nel campo consentirebbe che le funzioni attualmente svolte dall'app potrebbero essere di seguito svolte direttamente dal sistema operativo, rendendo inutili le app, sempre preservando la volontarietà e la decentralizzazione dei dati. Ciò appare un discorso futuribile, in quanto richiederebbe una modifica degli aspetti normativi.

[28] Per ragioni tecniche Google, a differenza di Apple, richiede che l'app funzionerà con il dispositivo con la funzione di geolocalizzazione attiva nel sistema operativo (Android), per un funzionamento

È proprio quest'ultima la questione più rilevante in punto di diritto che intendiamo trattare prima di trarre delle conclusioni. Con questa tecnologia i dispositivi si riconoscono ad una determinata distanza. La potenza del segnale del *bluetooth* è calibrabile dagli sviluppatori mediante appositi algoritmi proprio grazie alla API, in modo da tener conto dei singoli modelli di dispositivi, di diverso valore e dunque potenzialità[29].
Appare fondamentale per valutare l'app comprendere chi riceverà il segnale di allerta (il *trigger*, grilletto) per verificare se siano ragionevoli le condizioni, in quanto da esse dipendono possibili, anche se non automatiche, restrizioni ai diritti fondamentali. E per questo una questione non da poco è quella del tempo di esposizione al rischio. La soglia rilevante di questa prossimità non è stata ancora definita e non c'entra con la fissazione della misura da parte delle autorità del distanziamento fisico, ma è destinata ad interagire in modo problematico con essa. Verosimilmente il *bluetooth* funzionerà a distanze maggiori rispetto a quelle previste dalla legge e del resto il rischio di esposizione richiede di considerare anche un altro aspetto molto rilevante, che è il tempo di esposizione.
Nelle caratteristiche attuali non potrà arrivare un *alert* per aver sfiorato o toccato una persona (risultata positiva) incrociata camminando o essere rimasto per diversi secondi o qualche minuto in sua prossimità (come alla fermata di un autobus). Ma sarebbe azzardato affermare che tale situazione non è considerata perché ha potenzialità inoffensive (v. *infra).* Secondo il protocollo di Google e Apple il tempo di esposizione che sarà memorizzato sul dispositivo sarà solo quello tra i 5 minuti e i 30 minuti. Un contatto inferiore è considerato irrilevante e uno superiore non sarà registrato in quanto tale, ma saranno registrati i singoli eventi di durata significativa che sono avvenuti nel corso di un tale contatto. L'app non contiene alcuna virtualità di tracciamento di rapporti interpersonali o di abitudini sociali.
La tecnologia *bluetooth* del resto è assai meno precisa della geolocalizzazione, la quale non è essa stessa in grado di rilevare una differenza di poche decine di centimetri. Il *bluetooth* a seconda dei modelli può rilevare altri dispositivi anche a diverse decine di metri (fino a cento, attualmente nei modelli di alta gamma), come ovviamente a distanza minime, ma individua un dispositivo entro un raggio d'azione e non lo colloca in una posizione specifica, per quanto imprecisa, e rilevata come tale.
Infine, attualmente non è risolta la questione dell'integrazione tra l'infrastruttura dell'app e le strutture tecnologiche del Sistema sanitario nazionale. Al momento i dati non sarebbero messi in contatto con il SSN perché allo stato l'app non ha le caratteristiche tecniche per integrarsi e dialogare con quelle strutture. Il server allo Stato serve a consentire tecnicamente di avere un hub per inviare le liste mettendo a frutto gli intrecci di dati. Ulteriori funzionalità andrebbero aggiunte previo aggiornamento, volontario a sua volta.
L'integrazione dell'app nelle API infine ha un ultimo rilievo sulle app regionali. Da

ottimale, ma senza che "Immuni" acquisisca le informazioni di localizzazione. Pertanto, si ribadisce che il funzionamento sarà con tecnologia *bluetooth.*

[29] Sul mercato esistono modelli in grado di connettere via *bluetooth* due dispositivi a distanza di cento metri, e quindi il rischio di falsi positivi sarebbe enorme, come peraltro è apparso nell'esperienza di Singapore. Un cenno a questo problema nel testo *infra.*

quando le *big tech* sono entrate nel settore delle app di tracciamento ed esposizione offrendo i loro servizi è sfumata la possibilità di immaginare un ben integrato sistema repubblicano di app. Diverse regioni (es. Veneto, Lombardia, Friuli-Venzia Giulia, Toscana) stanno lavorando ad app proprie, anche già in via di sperimentazione. Queste app potrebbero ben essere utili per una circolazione locale, considerando che gran parte delle persone effettuano spostamenti limitati. Ma i due colossi *big tech* hanno dichiarato che consentiranno l'integrazione con le API di una solo app per ogni Stato e quindi queste app regionali probabilmente non saranno altrettanto raffinate e integrabili con quella statale. Del resto, incontrerebbero limiti ben maggiori nel campo dell'incisione dei diritti fondamentali.

4. Considerazioni conclusive

Nel momento in cui scriviamo sono trascorse tre settimane dalla prima riapertura del 4 maggio. Essa è avvenuta in circostanze tutt'altro che ottimali e più che altro per l'impossibilità di protrarre il *lockdown,* per cui sarebbe stato fondamentale già disporre dell'app come degli accorgimenti organizzativi (per es. nei trasporti pubblici) e delle politiche sanitarie (test sierologici, strategie precise su tamponi, etc.) volte a minimizzare i rischi. Tutto ciò è avvenuto solo molto parzialmente e non è noto ancora quando ci sarà il varo dell'app. Qualche critico si è spinto a dire che l'app ha fatto la fine delle mascherine a prezzo calmierato (che non si trovano[30]) ma il governo ha confermato che l'app è prossima ad essere rilasciata. Del resto, è destinata ad operare sulla base di una condizione di positività conclamata ma che opera in un quadro non soddisfacente di tracciamento e trattamento, se consideriamo che questo virus è reso pericoloso soprattutto dal fatto che è trasmesso prevalentemente da asintomatici (beninteso, perché la loro condizione è più insidiosa).

Alcuni aspetti dell'app devono ancora precisati, tra di essi abbiamo già fatto cenno ai modi e ai tempi di esposizione per l'*alert*. Si parla di parametri diversi a seconda delle circostanze ma il *bluetooth* ha potenzialità molto limitate in ciò. Torneremo sul punto dell'intreccio tra vincoli tecnici e giuridici, che appare dirimente.

Allo stato restano aperti alcuni problemi. Manca l'identificazione puntuale dei server e della loro collocazione, comunque pubblici e dislocati sul territorio nazionale, per quanto i rischi siano comunque limitati dalla scelta della decentralizzazione. Occorrerà certamente vigilanza su come saranno realizzate eventuali "fasi due" per le funzionalità dell'app, quando aumenteranno i soggetti coinvolti (es. regioni, Asl) e le potenzialità intrusive (col fascicolo sanitario). L'intermediazione delle API non dovrebbe invece destare alcuna preoccupazione in termini di possibile trasmigrazione di dati verso server collocati all'estero, e del resto alla base di quell'intervento è stata posta la condizione della decentralizzazione dei dati.

Attualmente l'app è stata giudicata in modo molto favorevole dall'M.I.T. anche sotto profilo della sicurezza. Il codice sorgente è stato resto noto e i tecnici saranno in grado di verificarne ogni carenza o *vulnus* in termini di sicurezza, a partire da eventuali *back-*

[30] P. Battista, *Ma che fine ha fatto l'app Immuni?*, in *Corriere della Sera*, 25 febbraio 2020.

doors[31]. Online esiste una comunità molto attiva che già sta operando quotidianamente per discutere e contribuire a migliorare efficienza e sicurezza dell'app.
In Italia il Copasir, organismo parlamentare di vigilanze sulla sicurezza nazionale, si è espresso con una relazione che promuove l'app con alcune riserve, che a dire il vero sono apparse per molti aspetti, un po' come in certi atti di indirizzo parlamentari, più dei manifesti politici dei singoli gruppi che delle preoccupazioni o dei suggerimenti concreti. La gran parte delle raccomandazioni infatti riguardano profili in realtà già definiti e in modo tale da superare quelle riserve; per il resto esistono aspetti marginali non ancora disciplinati e in tal caso non si tratta tanto di riserve ma utili indirizzi che si muovono ponendo condizioni entro linee europee già ben definite. I profili di sicurezza nazionale potenziali sono indubbi ma la relazione non dà molto spazio a diversi motivi di polemica dei giorni precedenti, a partire dalle modalità di selezione dell'azienda costruttrice dell'app, al suo modo di essere, e alla sua appartenenza ad un consorzio che lavorava su soluzioni centralizzate[32]. Lo stesso vincolo della gratuità della costruzione e dell'aggiornamento dell'app (quest'ultimo aspetto ha reso necessario un appalto di servizi, cui fa cenno l'ordinanza del Commissario datata 16 aprile 2020), sicuramente ripagata da un importante ritorno di immagine, può destare qualche perplessità sulle ragioni che portano un'azienda a impegnare decine di unità di personale per mesi e per migliaia di ore/uomo[33] senza alcun ritorno diretto, ma una risposta sta

[31] Gli sviluppatori dell'app "Immuni" avrebbero predisposto un'ulteriore cautela consistente nella produzione di "*dummy traffic*", trasmissione di dati spazzatura generati dai dispositivi in modo da inquinare il segnale per malintenzionati che volessero carpire informazioni tramite un'analisi di traffico. Inoltre, prima di essere distribuita l'App affronterà un "*penetration test*", i cui risultati dettagliati saranno divulgati.

[32] La società, una società per azioni ben nota, la Bending Spoons, ha sede legale in Italia e nel suo capitale ci sono piccole quote provenienti da stati non democratici, tramite fondi lussemburghesi gestiti da finanzieri italiani. Il Copasir anche per questa ragione si è mostrato molto interessato ad approfondire la procedura di selezione della società, molto solida e dotata di indubbia reputazione nell'ambiente sia per i risultati economici che per le soluzioni nel campo della sicurezza (150 dipendenti, 300 milioni di applicazioni scaricate, 90 milioni di dollari di ricavi nel 2019). La procedura di scelta tuttavia è stata opaca. Solo dopo l'approvazione del decreto legge che fa da base legale all'app sono stati pubblicati i documenti degli esperti della task force che avrebbe dovuto stabilire i criteri per la scelta della società incaricata di costruire l'app ed è emerso che l'organismo aveva raccomandato di testare in via parallela due app di altrettante società ma che il ministro competente non ha rispettato questa raccomandazione e ha scelto di testare una sola app, "Immuni", ritenendola «più rispondente alle attuali necessità». Inoltre, è emerso che il gruppo di esperti aveva subordinato la scelta dell'app a una serie di requisiti tecnici che quantomeno al momento della produzione del report non erano stati rispettati da alcuna società concorrente. La situazione tuttavia successivamente si era molto modificata.
Un altro fattore di interesse è stato rappresentato dal fatto che la Bending Spoons fa parte di un consorzio europeo pubblico-privato "no profit" (il cui acronimo è PEPP-PT), quindi non commerciale ma neanche istituzionale, costituito da poco per creare uno standard in tema di app di questa tipologia e con sede legale in Svizzera, sostenuto da una Fondazione avente sede a Basilea e sotto la vigilanza del governo svizzero (quindi non UE). Tale consorzio in qualche modo riconosciuto anche dalle istituzioni comunitarie – tanto che si parla di un modello europeo - ha avuto vicenda anche travagliate, con l'abbandono polemico da parte di alcuni soggetti (anche italiani). L'opinione pubblica italiana ha parlato non poco di questo consorzio, del resto operativo in tutta Europa senza grandi polemiche, ma il Copasir non ha sollevato questioni degne di rilievo. Il ruolo del Consorzio è venuto scemando con l'intervento in campo di Apple e Google che hanno portato avanti, con le proprie API, un modello decentralizzato (DP3T) che ha finito per esercitare anche una sorta di tutela o comunque porre vincoli tecnici alle società costruttrici delle app.

[33] *Sulla app nessun guadagno. Fiducia e privacy fondamentali*, in *Corriere della Sera*, 23 aprile 2020, intervista al

nella selezione che vedeva ben 319 aziende interessate, quindi indubbiamente attraente a prescindere dal compenso. Il funzionamento dell'app dovrebbe esaurirsi con la fine dell'emergenza, con la disponibilità del vaccino o la scomparsa del virus e non dovrebbe collegarsi formalmente ad altre operazioni di digitalizzazione della P.A. ed in particolare della Sanità.

In conclusione, la soluzione italiana appare sicuramente in linea sia con la Costituzione che con la normativa europea a partire dall'art. 23 del Regolamento generale sui dati personali (ad anche all'art. 15 della Direttiva e-Privacy) che, ormai sotto l'ombrello dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, consentono limitazioni a mezzo di misure legislative di alcuni diritti nella misura in cui la limitazione rispetti "l'essenza dei diritti e delle libertà fondamentali" e sia "una misura necessaria e proporzionalità in una società democratica" al fine di salvaguardare un'ampia serie di obiettivi tra cui la sicurezza pubblica e la sanità pubblica (art. 23 cit.; non dissimile l'art. 15 cit., che prevede anche che i dati siano conservati «per un periodo di tempo limitato»). La base legale è stata assicurata col decreto legge n. 28/2020. Le previsioni in esso previste sono proporzionate anche alla luce di quanto sollecitato dell'European Data Protection Supervisor in astratto (vedi rapporto annuale 2019) a mezzo della descrizione delle misure, dell'indicazione di massima dei diritti limitati, dell'indicazione della finalità della misura pianificata e della scelta delle misure meno impattanti. Il criterio della gradualità appare rispettato con la scelta delle misure meno invasive ritenute idonee e sufficienti per i fini istituzionali dell'app e optando per la piena volontarietà dell'uso dell'app. Si è rinunciato ad una tecnologia tracciante *tout court* e qualunque finalità di controllo e/o repressiva, palesandosi anzi una spiccata componente "solidaristica"[34], che rientra molto relativamente nell'idea della c.d. sorveglianza attiva tanto richiamata, e spesso auspicata in questi casi. Non solo la volontarietà ma per il modo stesso con cui funziona si stenta a considerarla come uno strumento di limitazione significativa di un qualche diritto fondamentale. Diversi diritti sono stati limitati in questi mesi a prescindere dalla app e anche in modo draconiano, poco ragionevole e proporzionato. L'ordinamento sembra aver recuperato un po' di equilibrio, e ad un esame approfondito di tipo prognostico l'app non appare gravare in modo rilevante, nello stadio delle sue funzionalità attualmente previste, su alcuno di essi. In ogni caso l'esercizio dei diritti degli interessati potrà essere esercitato «anche con modalità semplificate» (art. 6, c. 2, lett. *f*), richiamo forse anche ultroneo stante la tutela apprestata in generale dall'art. 82 GDPR[35].

La prudenza della soluzione italiana rovescia l'approccio finora invalso poco rispettoso della tutela della dignità umana alla luce dell'equilibrio che deve sussistere tra diritti e interessi che si intrecciano[36], fino al punto da potersi interrogare sul grado

dott. Ferrari, A.D. Bending Spoons.

[34] Utilizzo l'espressione di O. Pollicino, *Data tracing, no a deleghe in bianco*, in *corrierecomunicazioni.it*, 24 marzo 2020, 7.

[35] *Ibidem*. Il contributo non si riferisce alla soluzione adottata, in quanto precedente al decreto e quindi si esprime in chiave normativa. Sul ruolo del principio solidaristico anche in riferimento all'attuale emergenza v. M. Noccelli, *La lotta contro il coronavirus e il volto solidaristico del diritto alla salute*, in *federalismi.it*, 13 marzo 2020, 2 ss.

[36] Criticato con severità ad es. da V. Baldini, *Dignità umana e normativa emergenziale: (in)osservanza di un*

di funzionalità dell'app rispetto all'obiettivo, che andrebbe valutato però nell'insieme delle soluzioni adottate, non solo di tipo tecnologico. In ogni caso qualche cenno di confronto con le soluzioni adottante o adottande all'estero può essere significativo. Limitandoci al campo democratico, in alcune esperienze estere il cittadino che usa l'app è spesso schedato come paziente (ad es. in Australia), o il server governativo è gestito da un privato (Amazon, ancora Australia); di frequente viene mappata la diffusione dei casi (sia pure con la garanzia si una rapida distruzione dei dati); in Norvegia l'app è prodotta da una no-profit governativa ma utilizza il ben più intrusivo gps e i dati stazionano per trenta giorni su un server governativo. Per non dire dei modelli asiatici democratici e tacendo ovviamente sugli altri[37]. I grandi paesi europei sono più indietro del nostro nelle risoluzioni. La Germania si sta distinguendo per il suo approccio, almeno a livello federale, assai circospetto sull'uso di simili tecnologie, anche nelle soluzioni molto riduttive all'italiana, a causa del retaggio totalitario dei sistemi di sorveglianza di massa (anche fino ad anni non troppo remoti: si pensi alla esperienza della Germania est) che porta i cittadini ad essere tendenzialmente contrari a forme di potenziale intrusione. Le amministrazioni regionali e locali sembrano più interessate a questi strumenti e aperte anche a raccolte massive di dati ma non è certo alle entità federate che spetta decidere su interessi per definizione unitari. Nel momento in cui consegniamo il lavoro il dibattito tedesco appare in un certo stallo. In Francia si fanno considerazioni non molto diverse da quelle italiane ma l'eccezione francese, a partire da una certa preferenza per il ruolo del pubblico e quindi anche per soluzioni centralizzate, ha costituito per settimane un ostacolo a fare passi importanti verso le realizzazioni, con richieste di soluzioni tecniche da parte del governo francese alle *big tech* piuttosto singolari quando ci si è resi conto dell'inevitabilità di forme di collaborazione. L'approccio francese consente di concludere sui rischi in punto di sicurezza informatica. Il rischio che *hacker* riescano a forzare i sistemi e a compiere azioni come mandare *alert* ingiustificati o provare a identificare soggetti alla luce delle persone con le quali si è stati in contatti ed altro ancora sono sempre possibili, per quanto le soluzioni invalse in Europa, a partire dalla decentralizzazione dei dati, diano buone garanzie quantomeno di danni più limitati rispetto a quelli di server certamente assai meno violabili di singoli dispositivi ma la cui violazione, cui abbiamo assistito in tanti campi negli ultimi anni, avrebbe effetti gravi.

Concludendo, piuttosto che come una minaccia diretta ai diritti fondamentali, il problema fondamentale dell'app, nella versione attuale, potrebbe essere legato alle conseguenze del rischio di alimentare direttamente o indirettamente un alto numero sia di falsi negativi che di falsi positivi. Se i primi non dipendono dall'app, essa d'altra parte può non segnalare diversi eventi rischiosi che solo una calibratura molto invadente del *bluetooth* potrebbe garantire, senza peraltro riuscire a distinguere le situazioni effettivamente a rischio dalle altre. Questa situazione è assimilabile a quella dei falsi positivi,

paradigma formale o (colpevole…) elusione di un parametro (anche) sostanziale? Aspetti problematici di un difficile equilibrio, in *dirittifondamentali.it*, 2, 2020, spec. 203 ss.

[37] Sul modello cinese utile A. Canepa, *Lotta al COVID e diritti dei cittadini nella Repubblica Popolare Cinese. Le peculiarità di un ordinamento socialista asiatico*, in *federalismi.it*, paper "Osservatorio Covid-19" (a cura di L. Cuocolo), 13 marzo 2020, 168 ss.

che magari pur avendo rispettato le distanze legali (ammesso che siano necessarie e sufficienti ad evitare il contagio, che, ricordiamo, non dipende solo dalle distanze, ma anche da norme igieniche), ricevono l'*alert*. Quindi da questo punto di vista pur essendo ogni iniziativa rimessa ai privati, si potrebbe determinare un numero eccessivo di richieste di approfondimenti a cui le strutture pubbliche potrebbero essere non in grado di far fronte rapidamente[38]. Non è peregrino il rischio di auto-confinamenti spontanei da parte di privati per ragioni prudenziali, magari sulla base di una imperfetta conoscenza delle modalità operative dell'app (la tecnologia tende ad essere ritenuta infallibile...), del tutto inutili e ingiustificati. Oppure il numero eccessivo di *alert* che un medesimo soggetto riceve porterà ad una assuefazione che rischia di travolgere anche quelle circostanze in cui la situazione ha dato luogo ad un rischio anche elevato.

Si pongono in altri termini tutti quei problemi che derivano da una certa ottusità della tecnologia, e a cui solo attenzione e buon senso (quest'ultimo assenta per definizione nelle tecnologie) degli esseri umani può porre rimedio.

Anche ammettendo un tasso alto di utilizzo di Immuni esistono molte situazioni che sfuggirebbero al suo monitoraggio e molte altre che entrerebbero nei suoi *radar* senza presenza di un effettivo rischio. Una app - almeno una app relativamente semplice - non rileva un muro o una barriera, non distingue se lo spazio è chiuso o aperto, non riconosce il ruolo peculiare che nella situazione concreta può giocare ad es. il *droplet,* non sa se le altre persone, come anche chi utilizzi Immuni, indossi dispositivi di protezione (ammesso che servano nella circostanza in questione). Immuni non potrà sapere se il prossimo incrociato dal dispositivo solo per un attimo ad una distanza limite per la legge e forse inclusa nel raggio d'azione del *bluetooth* ma ritenuta non rilevante ha fatto un colpo di tosse o se chi utilizzi l'app sia stato pochi secondi o quattro minuti a distanza non di sicurezza (in entrambi i casi, con un positivo), né potrà leggere correttamente la situazione di un lungomare affollato con persone a passeggio che rispettano le distanze di sicurezza (ma ove non fosse l'*alert* tendenzialmente mancherebbe) o di una spiaggia che è altrettanto affollata ma con una situazione ben più statica (dove l'*alert* sarebbe più probabile).

Il rischio forte è che un'app di questo tipo, pur nata per incidere in modo davvero minimo sul godimento dei diritti fondamentali, non solo serva a poco ma il suo modesto contributo sia controbilanciato da una certa confusione derivata (l'esempio del lungomare o della spiaggia appaiono emblematici). Al limite da qui potrebbe derivare una rilevante incisione sui diritti fondamentali, determinando i maggiori condizionamenti di fatto.

Le app come Immuni metaforicamente potrebbero essere descritte con varie metafore ottiche relative al campo visivo. A seconda dei limiti di fatto o tecnici, e anche per il loro incrocio, può dirsi che per quanto sia ben congegnata Immuni veda troppo per certi versi, troppo poco per altri e non vede affatto diverse "aree cieche". Si conferma

[38] Il decreto legge del 30 aprile prevede che la ricerca e gestione dei contatti per essere condotta in modo efficace deve prevedere delle risorse umane dedicate tra operatori sanitari e di sanità pubblica e personale amministrativo. In Italia si tratterebbe di circa 6.000 (una circolare del ministro della Salute quantifica queste risorse in circa una unità ogni 10.000 abitanti). Il loro compito consisterebbe nel monitorare pazienti in quarantena, eseguire tamponi, inserire tempestivamente dati nei diversi sistemi informativi.

la sua funzione assolutamente complementare, ma solo la pratica potrà dire che nel calcolo tra benefici e costi (non in termini stretti di diritto) ne valga la pena.
Mentre la politica fa le sue valutazioni, sarebbe ragionevole attendersi una campagna di informazione non solo sui profili di sicurezza dell'app ma anche sui modi di funzionamento, in modo che il fruitore possa essere messo in condizione di essere, per quanto possibile, il miglior giudice del rischio che corre. Un ulteriore aspetto di volontarietà dell'app dovrebbe consistere in questo, conformemente all'approccio europeo alla tecnologia digitale e alle risorse "esperte": le donne e gli uomini devono essere posti in condizioni di comprendere il funzionamento l'app per decidere, per non perdere il controllo della situazione, senza cui la volontarietà circa il seguito da dare agli *alert* dell'app diventa una bizza (magari per non andare a lavoro). Per avere sempre l'ultima parola, perché nell'app c'è l'algoritmo e il *software*, magari scritti ed eseguiti alla perfezione; la tecnologia può aiutare e ampliare gli spazi dell'autonomia, ma l'autonomia si misura nell'intenzionalità e nella vita vissuta, che è un'altra cosa.

The PoSeID-on Blockchain-based platform meets the "right to be forgotten"*

Giovanni Maria Riccio - Adriana Peduto - Fabiola Iraci Gambazza - Luigi Briguglio - Elena Sartini - Carmela Occhipinti - Iván Gutiérrez - Domenico Natale

Abstract

Adoption of disruptive technologies, such as blockchain and artificial intelligence, is more and more raising citizens' suspiciousness based on (i) lack of trusted information, (ii) perception of intrusiveness on privacy and human rights, (iii) disrespect of legal obligations (including GDPR), and (iv) misalignment and lack of cross-fertilization between technology and legal experts. This paper aims at demonstrating how the technology is not a per se issue, as it can be used to create an ecosystem which can deliver a significant and measurable value to citizens and customers and the whole community. In this perspective, this paper describes the legal framework, the method and the results that are behind the compliance analysis of the Blockchain-based platform developed within the context of the PoSeID-on project.

The paper, in order to identify the ethics and legal requirements used to perform the assessment of the PoSeID-on technology, introduces the ethics and regulatory framework on human rights, privacy, and data protection. The procedure for the assessment of the technology is described as well. An overview of the Poseidon project and its implemented Blockchain-based platform allows the reader to fully understand the objectives of the project, as well as the peculiarity of the specific implemented technology that has been designed to overcome many obstacles (e.g. regulation compliancy, individuals and organizations trust, investment size). Consequently, the paper describes the results of the compliance assessment performed on the PoSeID-on Blockchain-based platform. The paper concludes by showing that important aspects such as trustworthiness and sustainability can definitely contribute to improve the social acceptance of disruptive technologies, such as the PoSeID-on one, and consequently their wide adoption.

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo è stato sottoposto a referaggio anonimo.

Giovanni Maria Riccio - Adriana Peduto - Fabiola Iraci Gambazza - Luigi Briguglio - Elena Sartini - Carmela Occhipinti - Iván Gutiérrez - Domenico Natale

Summary

1. Introduction. – 2. The legal and ethics framework. - 3. Requirements and assessment. - 4. The PoSeID-on Project and Blockchain-based platform. – 5. Compliance assessment. – 6. Trustworthiness, sustainability, and ethics-driven technologies. – 7. Conclusions.

Keywords

PoSeID-on - right to be forgotten – blockchain - GDPR – data protection

1. Introduction

This paper is structured in 5 main paragraphs:

- "The Legal and Ethics Framework" aims at describing the legal and ethics conceptual framework of privacy and data protection as fundamental human rights. These fundamental rights are analysed historically so that the reader may comprehend the rationale behind GDPR's introduction. In particular, this chapter analyses the historical evolution of the "right to be forgotten", from its first interpretation and implementation in EU Member States' national courts according to the case-law of the European Court of Justice and finally to the definition set forth in Art. 17 GDPR.
- "Requirements and Assessment Procedure" describes the legal and ethics requirements with which designers and the implementers of a system dealing with personal data management are expected to be compliant. These requirements are fundamental elements of the assessment criteria. Moreover, the chapter describes the tools and techniques adopted for compliance assessment, including the procedure and the assessment report.
- "The PoSeID-on Project and Blockchain-based platform" describes the PoSeID-on project objectives and the specific features and advantages introduced by its implemented Blockchain-based platform. Details on the rationale behind the design choices are provided as well.
- "Compliance Assessment" begins by outlining the conceptual framework in which Art. 17 GDPR is included and the requirements identified to ensure its respect within the project. Then, the chapter describes how the platform generated by the PoSeID-on project is compliant with said requirements and, consequently, with the European legal and ethics framework. In particular, the chapter will consider the use of blockchain technologies by the platform and the fact that the solutions adopted are fully respectful of legal obligations, including those held by the GDPR. Due to the specific technology, that is based on "immutable storage", major focus is reserved to the right to be forgotten.
- "Trustworthiness, Sustainability, and Ethics-driven Technologies" describes how misrepresentation and/or lack of information can impact on trustworthiness and consequently on the social acceptance of disruptive technologies. On the other

hand, the ethics-driven approach adopted by the PoSeID-on project allows to overcome obstacles, such as regulation compliance, individuals' and organizations' trust, investment size. To that extent, a techno-regulatory interoperability lays the foundation for innovation, trustworthiness and sustainability.

This paper closes with "Conclusions" where the main achievements of the PoSeID-on project's research activity are summarised, focusing on the design and development of an ethics-driven approach for guaranteeing privacy and data protection, and specifically the right to be forgotten.

2. The legal and ethics framework

In order to properly understand the rationale behind the legislative solutions of the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")[1] and notably behind the right of erasure (or the right to be forgotten) it is necessary to review the path that these rights have traced during the last decades, firstly in the national case-laws and, in the last decade, in decisions of the European Court of Justice that have strongly influenced the text of the Art. 17 GDPR.

The right to privacy and the right to data protection are two fundamental rights aimed at protecting individual freedoms, as well as to enable the individual to exercise other fundamental rights such as free speech or the right to assembly.

The recognition of the right to privacy or to a "private life" as "fundamental" for both the individual and for society as a whole, has been made either at the international level (Universal Declaration of Human Rights - Art. 12), and at European level (the European Convention of Human Rights - Art. 8)). In particular, the EU constitutional "fathers", also taking into consideration decisions of the EU Member States courts, as well as their constitutional traditions, established that the right to privacy and the right to the protection of personal data are fundamental rights (respectively provided in Arts. 7 and 8 of the Charter of Fundamental Rights of the EU, 2007[2]).

In this respect, for the purposes of the present paper, the focus will be on Art. 8 of the Charter of Fundamental Rights of the European Union. Indeed, Art. 8 provides that «Everyone has the right to the protection of personal data concerning him or her» and, in the second paragraph of the above-mentioned article, that «Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law». Art. 16 of the Treaty on the Functioning of the European Union (TFEU)[3] provides similar statements, which are also recalled by the first recital of GDPR.

Even if the recognition of data protection as fundamental rights arrived only with the entry into force of the Charter of Fundamental Rights of the European Union, the introduction of protection of personal data has been already provided in the Direc-

[1] "General Data Protection Regulation (GDPR)", 2016.

[2] European Parliament, Charter of Fundamental Rights of the EU, 2007.

[3] Consolidated version of the Treaty on the Functioning of the European Union, 2012.

tive 95/46/EC[4].

After 20 years, an update was necessary for at least two main reasons. On one hand, the margin of discretion left to EU Member States led to several discrepancies among them, due to national implementation and provisions/decisions of the national data protection authorities. On the other hand, the technological evolution caused a dramatic change of the regulated scenario, which required a different and proper regulation since the actual one was not sufficient to meet all the new challenges.

In light of these considerations, in 2016, GDPR was finally approved, replacing and superseding Directive 95/46/EC. Specifically, GDPR provided for detailed explanation of data subject rights, set forth from Art. 15 to Art. 22, including among them, the right to erasure, also known as right to be forgotten (even if the two notions are not perfectly corresponding).

In particular, the right to be forgotten is a subjective right (not an absolute one) that can be understood as the right to an informative self-determination concerning the right, the power, of an individual to decide for the transformation into anonymity of the data related to him or her, or for its erasure/deletion[5].

This concept, from a historical perspective, first emerged in decisions ruled by US Courts in the last decades of the past century, as an evolution of the "right to be let alone", and in more recent times in Europe, at the turn of the 80s and 90s of the last century.

Following this evolution it is possible to say that the right to be forgotten holds that a piece of information concerning an individual, although true and appropriate, cannot be brought back to public opinion, after a considerable period of time, from its original diffusion or from the fact that the news itself occurred, provided that there is no longer a specific public interest, (i.e. the information is not relevant) tied to its publication or disclosure. This means that it is necessary to conduct a balancing operation among the interests, whereby the interest in information will therefore prevail on the right to be forgotten only where the piece of information is still relevant.

To better understand the scope of this right it is worth to quickly analyze some of the most important EU case laws. In this respect, however, it is important to stress that even if the great majority of these case laws concerns the balancing between the said right and the free press, the perimeter of scope of the right to be forgotten is not limited to that area, but, on the contrary, pursuant to the wording used in Art. 17 of GDPR its potential application is much more general.

Before GDPR, the main European jurisdictions developed an interpretation and application of the right to be forgotten, that has confirmed the existence of this right, although through an interpretative process shaped on a case-by-case analysis.

In 1973, the German Constitutional Court affirmed that, even if a right to publish information about the personal life of a criminal when it's sure she or he is guilty does

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[5] A. Berti, *Il diritto alla cancellazione*, in R. Panetta (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019.

exist, the effect of constitutional protection of the personality would represent a limit to communication. Indeed, debating and spreading specific information beyond the essential ones about the offender private life is not allowed.

Again, it is worth to mention the decision of the Court of first Instance of Rome (November 21, 1996) which attempted to give a first definition of the right to be forgotten as: «the legal situation of which the precautionary protection is invoked appears identifiable in what defined "right to be let alone"». More recently, the Italian Court of Cassation (decision no. 16111/2013), stated that «the subject's right to claim that his or her past personal affairs are publicly forgotten is limited in the right to report only when there is an actual and current interest in their dissemination, in the sense that what has recently happened is directly connected with those events and renews their relevance, otherwise the public resolves an improper connection between the two bits of information in an illegal infringement of the right to privacy»[6].

Similarly, the French case-law specified that the right to be forgotten could be invoked by a person who, having paid his or her debts to justice by completing a path of social rehabilitation, legitimately asked not to be perpetually associated with events of her or his past, as they probably no longer reflect his/her current personality[7] (in contrast, a minority French doctrine has also questioned the need for a subcategory of the right to be forgotten, which specifically affects people who have suffered judicial convictions).

On the other side, in 1997 the Court of Appeal of Montpellier held that the right to be forgotten couldn't be recognized in an absolute form. Depending on the circumstances, such as the length of time passed from the crime, the gravity of the facts, at the end of the condemnation time, the judge admitted the legitimacy to obtain the erasure of the criminal information, when its recall no longer meets any ethic, historical, or scientific need.

Besides, in the Case EWHC 799/2018, the Queen's Bench underlined that the concept of journalistic news had to be interpreted in a matter not so flexible to include every activity that contains information or opinions[8]. Instead, in Spain, the right to be forgotten must be balanced with the historical interest of the facts[9]. Furthermore, the Belgian Court declared that a person who was condemned has the right to be forgotten, based on the Art. 8 of the European Convention of Human Rights of the Council of Europe and the 19 of International Act about civil and political rights[10].

However, at the EU level, the landmark case that better clarified the balance between the right to communication and the right to be forgotten was the *Gonzalez vs. Google Spain* (case C-131/12, Mario Costeja Gonzalez and AEPD – *Agencia Española de Protección de Datos*) decided by the Court of Justice of the European Union (CJEU) .

An analysis was conducted considering three different perspectives (i.e. the processing of personal data, the applicability of the Spanish laws to Google, and the obligation

6 Italian Supreme Court, judgment no. 16111 of 26 June 2013.

7 *Tribunal Grande Instance Paris*, 25 March 1987, in *Dalloz,* somm. 198, 1998.

8 Judgment available online at *judiciary.uk*.

9 Spanish Supreme Tribunal , 2013.

10 *Tribunal de Première Istance,* 1997.

to intervene to protect the right to be forgotten) concerning the relationship between the Internet and the right of erasure[11]. The CJEU concluded that, in order to be able to verify the applicability of Arts. 12(b) and 14(1)(a) of Directive 95/46/EC, it was necessary to ascertain whether the interested party had the right to the information concerning him to be no longer linked to his name, through a list of results deriving from a search carried out starting from his name. The right to be forgotten invoked by the interested party would prevail not only towards the operator of the search engine - and its underlying economic interests - but also in the interest of the public to access the information in question when searching the name of this person - unless it appeared, for some reason, that the role played by this person in public life was fundamental enough to justify the interest of the community in accessing this news. According to the CJEU, however, there was a limit to the claim of the right to be forgotten: obviously the search engine operator could not delete the personal data on the source of the information, but its duty should be limited to the deindexation or delisting of the reference among those included in the search engine's results.

After the Costeja Gonzales case, in November 2014, the Working Party Article 29 ("WP29") published the guidelines about the implementation of the right to be forgotten, in which a common line of interpretation for the national data protection authorities to follow was provided in order to ensure a correct adaptation of the internal regulations to the CJEU ruling[12].

After these guidelines, the French data protection authority – CNIL (*Commission nationale de l'informatique et des libertés*) - had ordered Google to delete the links redirecting users to obsolete news, not only stored within the European territory or on European sources of information but also outside Europe.

In the United Kingdom, the Google C-131/12 judgment has prompted the European Union Committee at the House of Lords to draft a report, in which it was argued that the new EU data protection legislation expressly provides that the search engines cannot be qualified as data controllers. As for the other national privacy guarantors, the Dutch Data Protection Authority (CBP) has not drawn up any guidelines regarding deindexing activities but refers to the indications of the WP29. The Spanish Data Protection Authority (AEDP) has introduced an ad hoc space on its website in which it explains the right to be forgotten, providing the guidelines to be followed for the privacy authorities.

Nevertheless, first the Google Spain ruling, then the interventions and decisions of the various data protection authorities and the guidelines of the WP29, influenced the

[11] CJEU, C-131/12, *Google Spain* (2014).

[12] Article 29 Working Party, Opinions and Recommendations. For the sake of completeness, it is appropriate to recall the previous judgment of the ECHR of 16 July 2013 (*Węgrzynowski and Smolczewski v. Poland*, app. 33846/2007). This ruling addresses a case similar to Google Spain, but with a different methodological approach. The European Court of Human Rights has ruled, with the decision of 16 July 2013, on the balance between freedom of the press and the right to reputation in cases of dissemination of articles via the internet. In the case in question, however, the right to be forgotten is not really emphasized. Specifically, the Court considered the elimination of an article from the website of an online newspaper a disproportionate measure, despite the fact that the national judges had considered the text published in the paper's adaptation of the newspaper defamatory, bringing it back to the context of protecting freedom of expression the web archives of newspapers.

drafting of the European Regulation on Data Protection.

As mentioned, Art. 17 of GDPR provides the right to obtain the cancellation of personal data, without delay, provided that specific conditions are met[13]. The second paragraph of the same article holds that the data controller who, in the presence of the conditions described, is obliged to delete personal data, must necessarily «taking into account the available technology and implementation costs, adopts reasonable measures, including technical, to inform the data controllers that they are processing personal data of the request of the interested party to delete any link, copy or reproduction of his personal data». Therefore, the reference to the right to be forgotten, placed only in brackets in the article next to "right to erasure", and in the context of a provision dedicated to the erasure of personal data, seems to frame this right within the right to erasure.

Indeed, the heading of the article was, during the preparatory work, "right to be forgotten or right to erasure", a formula then abandoned because the adversarial conjunction could have generated confusion.

Despite the mention made by Art. 17 of GDPR, the right to be forgotten as well as the right to erasure are not defined. However, the case-law of the CJEU made clear the boundaries of this notion, granting to individuals the right of being deindexed from search engines, and to the correct contextualization of data that are no longer actual.

In this respect, two judgments of the CJEU on the right to be forgotten on 24 September 2019 are useful to understand how the right to be forgotten is being conceived within the EU. The first decision relates to case C-507/17 between the CNIL and Google Inc. and concerns the territorial extension of the de-indexing. There is no obligation, deriving from Union law, to carry out such deindexing on all versions of its engine for the provider, but it must be done, however, in the search engine versions of all EU member states[14]. The other ruling of the CJEU (case C-136/17) raised from another question posed by the French Council of State, concerning the processing of sensitive data by search engines. The Court reiterated that the indexing activity carried out by search engines must be considered "processing of personal data" and therefore subject to the limitations currently provided for by the GDPR, and previously by Directive 95/46/EC, as regards the treatment of sensitive data[15].

This brief and necessarily incomplete overview on the right to be forgotten explains how this right has changed from its debut in the legal discourse. In fact, at the beginning of its application by the national courts, it was considered to belong exclusively

[13] The conditions are: a) personal data are no longer necessary with respect to the purposes for which they were collected or otherwise processed; b) the interested party revokes the consent on which the treatment is based, and there is no other legal basis for the treatment; c) the interested party opposes the processing for his/her particular situation and there is no prevailing legitimate reason to proceed with the processing, or she/he opposes in relation to personal data that are processed for direct marketing purposes; d) personal data have been unlawfully processed; e) personal data must be erased to fulfil a legal obligation under Union law or under the law of the Member State to which the data controller is subject; f) personal data have been collected in relation to the offer of information society services in accordance with the provisions of art. 8 regarding the consent given by minors.

[14] CJEU, C-507/17, *Google v. CNIL* (2019).

[15] CJEU, C-136/17, *GC and others* (2019).

to public figures and not to private citizens. In fact, only public figures were interested by the mass-media analysis, while private persons were outside this process and were only spectators of this news. The spreading of Internet and the facilitation of collecting and indexing information has determined that also private persons may be covered by this right. In fact, these persons may be "googled" as well and their personal information may be easily found through a search on the major search engines; thus, it is essential that the events which may be harmful for their reputation are not that effortlessly located by other users. Furthermore, the balance between the right to be informed or the right to research, on the one side, and the right to not being eternally "labelled" for an old behaviour, may coexist, provided that the information would not be cancelled from the source where it has been published, but exclusively deindexed.
However, the right to erasure cannot be limited to this aspect, because, as above exposed, Art. 17 provides a wider provision, with several limits. In other words, the right incorporated in Art. 17 is not absolute, but can be exercised only in specific situations, which are listed in the first paragraph of the article itself. In particular, this case occurs where «the data subject withdraws consent on which the processing is based» and «there is no other legal ground for the processing». Other interesting hypotheses, for the purposes of this paper, are mentioned by letters (a) and (d) of para. 1 of Art. 17 which respectively state that the right to erasure can be applied if the personal data have been unlawfully processed.
On the other side, this right is balanced by the provisions held in para. 3 of Art. 17, which enumerates the cases in which to right to erasure cannot be applied. The most relevant assumptions for our goals are those listed in letters (b) and (e), and which respectively allow the retention of the data if this retention is necessary in order to comply with a legal obligation or for the establishment, exercise or defense of legal claims.

3. Requirements and assessment procedure

In light of the abovementioned legal and ethics framework, special care must be devoted to (i) analyse the architecture's specifications of a system that manages personal data, (ii) selecting the technology available from the state of the art, and (iii) how the technology is instantiated. Indeed, these factors could raise legal and ethics concerns and have deep impacts on data protection.
In this regard, apparently, the right to be forgotten may be in conflict with blockchain technologies, as long as these technologies are shared and synchronized with digital databases based on a consensus algorithm and stored on multiple nodes and stored in an "append only" mode. Indeed, all the data are collected, stored and processed in a decentralized way, where each node of the network contains all the data and it can control them; blocks can be added, but they cannot be deleted (i.e. immutability property of blockchain).
Therefore, the right to be forgotten/to erasure cannot be guaranteed.
Nevertheless, in order to find some elements of compatibility, some solutions have been already advanced by the CNIL in September 2018 with the publication of the

official document "*Premieres éléments d'analyse de la CNIL*" according to which the possibility to plan the destruction of the private key (that is used to decrypt the data in the blocks) has been foreseen so as to render inaccessible the data that remain stored within the chain (i.e. data is not effectively erased from blockchain)[16], but at that point cannot be consulted[17]. In practice this solution makes data lost in a "black hole" and, at the current state of the art, it is impossible to recover these data.

Another possible solution might be the one concerning the implementation of some of the erasure methods that can make data "forgettable" in blockchain, even if they do not guarantee the permanent deletion of data. An example is represented by pruning, a technique used with bitcoin, that allows a reduction of the storage of data for the user of the blockchains[18], deleting the old and historical blocks[19]. However, this solution could impact on the reliability of the blockchain itself, and trade-off considerations must be taken into account (i.e. size of erased data versus size of the blockchain)[20]. Moreover, it is important to stress that, even if pruning consists in the removal of old blocks, all the information necessary to recreate the older state is still saved on each node[21].

The last solution is to "fork" the blockchain (i.e. resetting the rules of the chain) with the creation of a new ledger[22]. However, due to the nature of the blockchain, this solution implies the coordination of all involved nodes, and its implementation and management could be difficult to achieve and also unprofitable.

Many other futuristic solutions are also mentioned in the literature, proposing inter-alia reversibility or edit-ability features. However, these solutions are not mentioned in this paper in consideration of the fact that they don't focus on evaluating solutions based on blockchain technologies already available in the current state of the art. Moreover, these proposed solutions usually don't address the erasure of data, that in the end remain stored in the blockchain, and require the destruction of the private key as well.

Besides the aforementioned possible solutions, the European Parliamentary Research Service published in July 2019 a study entitled "Blockchain and the General Data Protection Regulation. Can Distributed Ledgers be Squared with European Data Protection Law?", in which three solutions to reduce the gap between the GDPR and blockchain, called "Policy Options", are presented. The publication considers the GDPR as a neutral technological regulation, and as such flexible enough to be adapted upon the evolution of new technologies.

The first solution presented concerns the adoption of a regulatory guidance, due to

---

16 CNIL, *Blockchain*, September 2018.

17 The European Union Blockchain Observatory & Forum, *Blockchain and the GDPR*, 16 October 2018.

18 G. Ateniese – B. Magri - D. Venturi - E. Andrade, *Redactable Blockchain – or – Rewriting History in Bitcoin and Friends,* 2016, in *eprint.iacr.org*.

19 S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* in *bitcoin.org*.

20 E. Palm, *Implications and Impact of Blockchain Transaction Pruning*, in *diva-portal.org,* July 2017.

21 European Parliamentary Research Service, *Blockchain and the General Data Protection Regulation. Can Distributed Ledgers be Squared with European Data Protection Law?,* July 2019.

22 M. Finck, *Blockchains and Data Protection in the European Union,* in *European Data Protection Law Review*, 4(1), 2018, 17 ss.

the difficulty to understand the blockchain structures and the application of, and correlation with, the GDPR, regarding some concepts such as data controller and right to erasure. The second one, concerns the implementation of codes of conduct and certification mechanisms; while the last one is an interdisciplinary research finding common approved solutions (such as: the creation of governance mechanisms, development of protocols, etc.)[23].

These proposed solutions, available at the state of the art, represent a set of suggested recommendations for the development team that is approaching a personal data management system.

Moreover, it is requested to the development team to integrate the legal and ethics requirements, defined in Table 1, in the system requirement specification[24]. These requirements focus on the individual rights of the data subject, and consequently these directly or indirectly guarantee the compliance with GDPR art.17, as well as the Arts. 15-21.

A relevant role is played by Arts. 5 (Principles) and 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject) of the GDPR, dealing with the transparency of the system: these articles encompass additional requirements that provide guidance in terms of transparent governance of data, communication and modalities for the exercise of the rights of the data subject. These requirements lay the foundation for the assessment procedure of the building personal data management system. In other words, each requirement has to be satisfied and the development process has to gather and provide detailed justification for the compliance.

Table 1: Legal and ethics requirements

Requirement Id	**Requirement description**	**GDPR**
LER1	Secure and reliable identification, authentication and data access should be ensured.	Arts. 5, 15, 25 and 32
LER2	A withdrawing mechanism should be available in the platform.	Arts. 7 para. 3, and 17
LER3	A mechanism should be implemented to identify the specific data that is to be blocked or restricted.	Arts. 18, 21 and 25
LER4	Extracted data should be limited to the identified and authenticated person concerned and communicated securely (e.g. encrypted).	Arts. 5, 25 and 32
LER5	Appropriate information should be provided to individuals to exercise their rights and to ensure transparency.	Arts. 5, 12, 13 and 14, and 37

[23] European Parliamentary Research Service, *Blockchain and the General Data Protection Regulation,* cit.

[24] PoSeID-on, *PoSeID-on blockchain - Interim implementation*, 2019.

LER6	Appropriate procedures for the governance of the system and its operations should be identified and adopted in case of exercise of the rights.	Arts. 5 and 12

4. The PoSeID-on Project and Blockchain-based platform

The PoSeID-on project – which stands for "Protection and control of Secured Information by means of a privacy enhanced Dashboard" – is a Research and Innovation project financed under the EU Horizon 2020 programme. Started in 2018, the project has been running for 30 months as of this paper's completion.

PoSeID-on arose from the General Data Protection Regulation (GDPR) implementation challenges, and the security issues related to the management of digital identities. Its final aim, indeed, is to transform the perception of GDPR as an administrative burden into a more widely accepted approach to see GDPR as an opportunity and an added-value for citizens, public, and private entities, reinforcing transparency and trust in society, especially towards public administrations.

To achieve this objective, PoSeID-on is developing an innovative and intrinsically scalable platform for personal data protection, aimed to safeguard the rights of data subjects as well as to support organizations in data management and processing, while ensuring compliance to the GDPR. The platform, accessible through electronic identification (eID) accounts, enables users to securely grant, revoke and check Personal Identifiable Information ("PII", i.e. information related to a Data Subject, that can be used to directly or indirectly identify the person) permission to digital service providers. As a result, the PoSeID-on platform empowers users in managing the PII processed by public and private organizations, and at the same time it helps those organizations to guarantee the rights of data subjects and be in line with the privacy legal framework.

The solution is based on the use of innovative technologies, such as a custom permissioned blockchain, which can allow secure data management and personal identifiable information exchange.

The goal of including an implementation based on a blockchain platform is to provide the secure and trustable means to operate with individual permissions. Indeed, it increases the confidence of European citizens in the operations that administrations and companies make with their personal data. The perception of control rises, and respect for the application of regulations - such as the GDPR - is greater.

To summarize the capabilities of the decisions made during the design phase, the following guidelines have been defined throughout the development process for addressing the ethics and legal requirements defined in Chapter 2:

- Personal data is not stored nor transmitted in the blockchain network, which handles permissions transactions over personal data. However, permissions themselves belong to PII.
- A permissioned blockchain network will ensure a secure and reliable identification, authentication, and data access, acting as a distributed and secure means to

audit PII transactions, enabling a secure control over personal data.

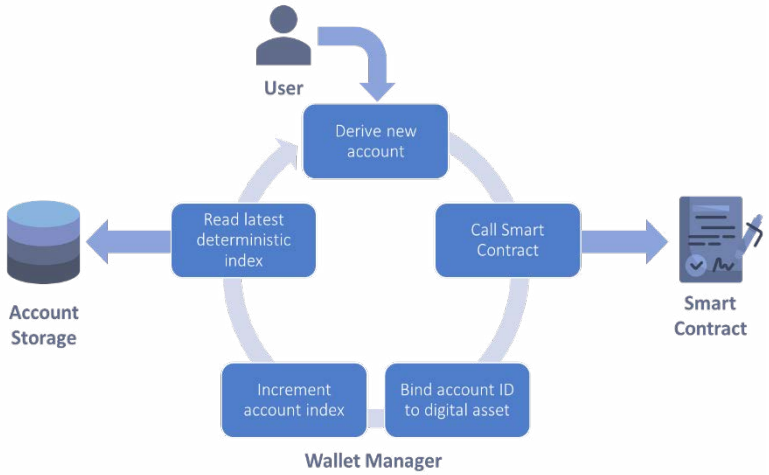
- Smart contracts, that define the user-centric permission management functionality, will be the mechanism to get the information only to the right person, ensuring the privacy of personal data transactions.
- The user operations will allow the Data Subject to enforce permission on specific data, whenever Data Controllers or Data Processors ask to use them on a service.
- The development of an application programming interface (API) allows the Data Subjects to access their own personal data and retrieve them within personal area (a.k.a. personal wallets) from mnemonic words. Only the Data Subject can know and access his/her wallet. The wallet can be created again in case of key loss, using the same mnemonic that was used the first time and giving the user the full control.
- A blockchain client is mandatory to control and get informed on the status of transactions in the blockchain. This decentralized access mechanism will prove that Data Processors are doing what they claim to do. It will be incorporated in the Privacy Enhanced Dashboard (PED) of PoSeID-on for ease of use.

Blockchain general philosophy is thought to permit the traceability of the user actions. Depending on the context of application and the platform/technology used, the level of knowledge the system has about the user identity can be greater or lesser. The strictest may require strong, even advanced, identifiers. While others (typically networks meant for public use) will allow pseudonymizing user identities by cryptographic means. Even if the Data Subject's Personal Identifiable Information (PII) is encrypted, it is still associated with a pseudonymous identity. The objective of this project is to ensure a use of blockchain that allows anonymizing operations to the point that the citizens themselves can exercise the data subject rights according to the GDPR.

To the controversial solutions from the current state of the art, mentioned in Chapter 2, the PoSeID-on project alternative approach for ledger management is based on the so-called "Burnable Pseudo-Identity" principle. This ensures that the PII of the Data Subject is not traceable by anyone looking to the transactions. The underlying principle of this proposal overcomes most of the state-of-the-art proposals by (i) implementing a mechanism of continuous refresh and rotation of identities in order to further reduce traceability; and (ii) giving back the PII control to the Data Subject by letting her/him the choice to "remember" or "forget" their identifiers. The aim of this shared mechanism is to allow user interactions in a way that they can only be traceable during the time the user is using the PoSeID-on services, and it can be compliant with GDPR and "right to be forgotten" when the user stops using these services (or upon request).

The behaviour of this method is described in Figure 1. The first step is the creation of the wallet that will contain the pseudo-identity, formed by the set of accounts belonging to the user. The wallet (as a container) and the accounts inside it are protected by encryption. A new account is derived when the user needs to interact with the blockchain network. That account is the one selected to call the Smart Contract. As this is the first time that the account is used, it is not related to other transactions and

will not leave any history trace when updating the ledger. Nevertheless, the account will be bound off-chain to the interaction, so the user can decide when to destroy it. When an account is already used and verified, the account index is incremented. That deterministic index is used to select the next account and get it prepared for the next user interaction.



(Figure 1: Schema of "Burnable Pseudo-Identities" principle)

The created mechanism is user-centred, since it allows users to have absolute control of the information known about them. Furthermore, although all protections are maintained, the difficulty of using blockchain is made transparent, and the problems related to understanding and storing cryptographic keys are smoothed out.
Each Data Subject will have an identity in PoSeID-on through the binding of a set of their pseudo-identities, made up of identifiers and actions. Only one action is performed per identifier and authorised Data Processors can provide their services managed by PoSeID-on. Once the Data Subject identity is burned, the cryptographic pseudonymous identifiers can't be re-engineered by the application, it will never again be used by the system and the Data Subject can't be traced in the future.
The pseudo-identities are created by the users, or by the PoSeID-on platform with authorization of the user. It involves a random seed (as an entropy source) and a secret for symmetric identity encryption. The user is the only one who knows the secret and the identity remains hidden and securely protected while it's not being used.
All these actions take place to ensure the compliance with ethic requirements. One of them is the prohibition of using an identifier after its lifetime period. Any data verified and chained to the ledger that is erased will cause a cryptographic error and a chain break. So, the data must be created in a way that it can be unlinked if needed. This is the purpose of the Burnable Pseudo-Identity. The other reason is the unlinkability, by which an irreversible way of creating new child keys from parent keys (but not otherwise) is not linkable with previous information.

5. Compliance assessment

In order to comply with the self-responsibility and accountability principles, on which the architecture of the GDPR is based, the Consortium stands by the opinion that the measures implemented ensure a full data protection assessment. In particular, these measures fulfill the transparency principle sets forth in Art. 5(1)(a) GDPR, and then better specified in Arts. 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject) and subsequent of GDPR, which requires that personal data are processed in a transparent manner in relation to the data subject.

Furthermore, this assessment analyses the technological implementation and guarantees the exercise of the rights of the individuals, whose personal data will be used by the platform and by third parties, and notably the right erasure regulated by Art. 17 GDPR.

From a strictly legal point of view, it has to be noted that the procedures to be executed are not compulsory as they are not formally necessary under the current regulations. Anyway, as mentioned, the approach of the GDPR is aimed, on the one hand, at empowering the data subjects, and, on the other hand, at leaving to the data controller and data processor(s) the choice of adopting the organizational and technical measures considered to be relevant for efficiently guaranteeing the personal data protection. For the PoSeID-on platform, the following seven measures have been considered, according to the Legal and Ethics Requirements as well.

Measure 1. Combination of digital certificates and digital signatures.

To ensure the identification and permission information access that are managed in blockchain by the PoSeID-on platform, a key component is combining the use of digital certificates with the digital signature in every transaction that ensures the non-repudiation. The digital certificates are directly related to the used Blockchain keys that allow recovering the user identifiers, because they help to keep them securely without being shared. These actions, along with the immutable character of the registry, allow an authenticated management of permissions and based on computational trust. The design of PoSeID-on has been made considering the distributed character of the registry too. The communication between parties to control the permissions satisfies the values of privacy, scalability, traceability, and access control needed by the Data Processors. The communication between them is done through private end-to-end encrypted messages that include mutually authenticated Transport Layer Security (mTLS) to avoid message spoofing attacks, and where the rest of the network parties are un-aware of that communication.

This measure satisfies the legal and ethics requirement identified as LER1 (Secure and reliable identification, authentication and data access).

Measure 2. Hiding complex technology implementation behind one-click button

Data subjects are allowed to withdraw consent for the access to PII in accordance to the GDPR. To achieve this, the web-based dashboard has implemented this functionality as a simple button, giving data subjects exactly this kind of control. Behind the scenes this button revokes the access permission using the Blockchain API and submits an automatic request for PII deletion to all data processors with delegated access to this information.

This measure satisfies the legal and ethics requirement identified as LER2 (withdrawing mechanism available in the platform).

Measure 3. Permission Lifecycle Model

A proper permission model has the power to avoid rogue parties and spammers. The PoSeID-on platform controls the allowance of permission requests by its Smart Contract design. The permissions can adopt different states (REQUESTED, ALLOWED, DENIED or EXPIRED), ordered in a flow that becomes the permission lifecycle. Those permissions can be updated to notify state changes. The access to information of a blocked or restricted permission requested by an unauthorised party is automatically denied by the Smart Contract, because the permission state is not ALLOWED.

This measure satisfies the legal and ethics requirement identified as LER3 (Mechanism to identify the specific data that is to be blocked or restricted).

Measure 4. Data Exchange management by design

The PoSeID-on platform offers a standardized data exchange management by design. Personal data is no longer exchanged between parties directly, but flows through the PoSeID-on platform enforcing access and security rules. This "man in the middle" functionality, however, introduces a privacy concern; whoever controls the PoSeID-on platform, can potentially access all personal information flowing through it. To prevent this from happening, the PoSeID-on platform comes with a Data Processor API Client, which is a piece of software that runs on the premises of the data processor. This application enforces end-to-end encryption among parties (both data processors and data subjects) using a custom protocol, leveraging cryptography supplied by libsodium[25] (a modern software library and fork of NaCl[26] Networking and Cryptography library). All personally identifiable information (including requests for data access permission to the data subject!) can only be read by the intended recipient.

This measure satisfies the legal and ethics requirement identified as LER4 (Extracted data are limited to the identified and authenticated person concerned and communicated securely).

Measure 5. Erasure Event and Notifications

The platform allows the data subject to erase data through the web-based dashboard, enabling the procedures for ensuring the right to be forgotten. Moreover, when this

[25] *Introduction – libsodium*, in *doc.libsodium.org,* 2020.

[26] *NaCl: Networking and Cryptography library – Introduction*, in *nacl.cr.yp.to*, 2016.

event occurs, the platform itself automatically sends a notification to the data subject, in order to transparently acknowledge receipt of the request and the enactment of erasure process.
This measure satisfies the legal and ethics requirement identified as LER5 (Appropriate information to be provided to individuals to exercise their rights and to ensure transparency).

Measure 6. Specified Events and Processes

For each specified event, the platform has defined a set of codified processes and the operations to be performed in compliance with the legal and ethics framework defined in Chapter 1, including EU data protection regulatory framework as well. These procedures include the actions to be taken inter-alia in case of permission restrictions, and in case of exercise of the right of erasure.
Specifically, for the latter, from the receipt of the request of the data subject, the data will be deleted by the platform within the period specified in the terms and conditions. Needless to point out that this means that the data can be deleted by the platform (and by all the instruments and tools connected with the platform itself), but not from databases, servers, and so on, if owned and managed by the Data Processors and their potential third parties. In other words, PoSeID-on (in its role of manager of the Platform) and the subjects which have joined the Platform, by accepting its terms and conditions, acts as independent data controller. PoSeID-on, therefore, is not in the position to delete nor to impose the deletion to these subject.
This measure satisfies the legal and ethics requirement identified as LER6 (Appropriate procedures for the governance of the system and its operations in case of exercise of the rights).

Measure 7. Contact details of Data Processors

To achieve the facilitation for the data subject of exercising the rights granted by the GDPR, PoSeID-on, once the request for the cancellation of the data has been received, automatically communicates to the applicant the contact details of the Data Processors and their potential third parties which processes his/her personal data and, in particular, the email address of these parties, and, if present, the email address (or other relevant contact information) of the data protection officer of the third parties.
This measure satisfies and enforces the legal and ethics requirement identified as LER5 (Appropriate information to be provided to individuals to exercise their rights and to ensure transparency), already satisfied by the measure 5.
Preliminarily, even if already mentioned, it is important to remark that the right of erasure and the right to be forgotten have specific limitations and that the retention of personal data, even in case of exercise of these rights, may be legitimate and allowed by the GDPR as well as by other privacy and sectorial regulations. For instance, this is the case of the retention of personal data which are connected to the performance and the execution of a contract is permitted, in the vast majority of the member States of the European Union, for ten years after the conclusion of the contract. Similarly, the storage of the data may be required by legal obligations (such as in case of many

regulations in the health sector, which demand the retention of the data for long periods) or is necessary for the performance of a task carried out in the public interest.

6. Trustworthiness, sustainability, and ethics-driven technologies

Blockchain (as well as – inter alia - Artificial Intelligence, Internet of Things, Gene Editing, Robotics, 5G) is widely recognised to be a disruptive technology, i.e. an innovation that significantly impacts the way that consumers, industries, or businesses operate. In this perspective, a blockchain-based system sweeps the traditional systems away and replaces habits.

For this reason, it is fundamental to perform a social acceptance analysis that lays the foundation for a "human first" approach in an "ethics-by-design" development process.

Now more than ever, there is a growing need for innovative technological solutions to help society achieve a sustainable future, for both current and future generations. Moreover, this need is strongly becoming a primary "ethics requirement" for the post COVID-19 emergency management.

How a technological innovation is perceived, how much it is trusted by the society and how much society is aware of the benefits deriving from its adoption, are the main questions to be understood for the social acceptance assessment of disruptive technologies.

It is not a matter of "good or bad technology", but rather, it is the approach to defining the solution, its implementation and instantiation, as well as the way to use it, that can definitely promote the innovation and sustainable scenarios for society.

The ethics-driven approach adopted for the development of the PoSeID-on platform (based on a better understanding of the technology, the respect for human rights, and willingness to use it) is definitely aiming at reducing the barriers of diffidence and mystification against blockchain, and fostering its wider and faster deployment.

7. Conclusions

This paper remarks how the ethics-by-design approach adopted by the PoSeID-on project has allowed its platform to comply with EU regulatory framework on data protection, and specifically the GDPR.

This achievement lays the foundation on the strongly cooperation among legal and technical experts of the project, while they usually work on different isolated rooms and without having the capabilities to understand each other.

PoSeID-on platform brings the blockchain technology for the management of personal permissions and, by adopting design guidelines based on legal and ethics requirements, enables the novel mechanism of "burnable pseudo-identities" in order to perform data erasure and reduce identity traceability. The underlying principle of this

mechanism, based on (i) continuous refresh and rotation of identities and (ii) giving back the PII control during its lifecycle to the Data Subject, overcomes proposals from the current state of the art applied in blockchain technology, when dealing with personal information and compliance with GDPR. Data Controller and Data Processors can access personal identifiable information if and only if Data Subject wants. When Data Subjects opt to exercise the right to be forgotten, the platform forgets the identifiers and doesn't allow in any way to retrieve and access information that can directly or indirectly refer to specific Data Subjects fallen into forgetfulness.

More than 10 legal and ethics requirements (LERs) have been identified within the PoSeID-on project and for the implementation of its platform. In this paper, focusing on the right to be forgotten, the assessment of the implemented platform has been performed based on six LERs, covering direct and indirect areas concerning the art. 17 of the GDPR. Seven measures have been adopted to comply with the six LERs. All these measures remark how PoSeID-on platform is giving back the full control of their data to the Data Subjects.

Flussi migratori e protezione dei dati personali: alla ricerca di un punto di equilibrio tra sicurezza pubblica e tutela della privacy dei migranti e dei rifugiati all'interno del territorio europeo*

Mirko Forti

Abstract

Mantenere la sicurezza dei propri confini e salvaguardare allo stesso tempo il diritto all'autonomia informativa di migranti e rifugiati; l'Unione europea è chiamata a trovare un punto di equilibrio normativo e politico tra queste due esigenze apparentemente contrapposte. La recente entrata in vigore del Regolamento (UE) 2016/679 (GDPR) propone nuovi standard giuridici a cui l'azione dell'Unione europea in materia di gestione dei flussi migratori deve adeguarsi. Il presente studio vuole offrire uno spunto di riflessione a tal proposito: partendo dalla definizione di "dato personale" fornita dal GDPR, si vuole analizzare quali diritti riconosciuti dal Regolamento all'interessato al trattamento dati possono essere rilevanti anche nel contesto migratorio. L'attenzione si sposta poi sull'effettiva legittimità delle misure messe in campo dall'Unione europea nel controllo dei propri confini con l'ausilio delle più moderne tecnologie digitali per valutarne la corrispondenza con quanto previsto dal GDPR.

Patrolling external borders and, in the meantime, securing migrants' privacy: the European Union has to find a normative and political balance between these two interests. The new EU Regulation 2016/679 (GDPR) sets out new legal standards in terms of the right to privacy: the European Union has to comply with these norms in regulating migratory fluxes. This article aims to study the relevance of GDPR rules in the migration context, starting from the new definition of "personal data". This article aims to study the relevance of GDPR rules in the migration context, starting from the

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

new definition of "personal data" to find out the legitimacy of the European Union's actions in patrolling its borders using digital technologies.

Sommario

1. Introduzione. - 2. La definizione di "dato personale" fornita dal Regolamento (UE) 2016/679 come influenza le pratiche di gestione della crisi migratoria? – 3. Quali diritti possono vantare i migranti relativamente al trattamento dei propri dati personali alla luce di quanto disposto dal Regolamento (UE) 2016/679? – 4. I "confini digitali" dell'Unione europea: l'utilizzo di sistemi tecnologici per garantire la sicurezza interna e i suoi profili giuridici. – 5. La tutela dei dati personali e la lotta al traffico di esseri umani. - 6. Conclusioni.

Keywords

immigrazione – protezione dei dati personali – privacy – GDPR – sicurezza pubblica

1. Introduzione

Il tema della corretta gestione dei flussi migratori è ormai da anni al centro del dibattito politico e giuridico europeo. 11.230 persone sono entrate nel territorio dell'Unione europea nel solo 2019, di cui ben 9.779 sono sbarcate sulle coste dei Paesi membri, dopo un pericoloso viaggio via mare[1]. Le sfide che l'amministrazione di una simile emergenza umanitaria solleva sono numerose e coinvolgono diversi ambiti: occorre difatti trovare un punto di equilibrio tra il rispetto dei diritti umani dei migranti, spesso vittime di trafficanti senza scrupoli, e le esigenze di controllo dei confini e di tutela della sicurezza e della salute pubblica fatte valere dagli Stati europei coinvolti.

L'Unione europea deve inoltre considerare che dette migrazioni si sviluppano in una società sempre più tecnologica e digitale, dove ogni individuo è costantemente connesso al *web*. Le nuove tecnologie hanno reso possibile processare e trattare una quantità sempre maggiore di dati personali, provocando rischi non trascurabili di intrusioni e ingerenze nella sfera privata dei singoli individui. Il progresso digitale si è rivelato essere ben più veloce e tempestivo della consapevolezza giuridica che avrebbe invece dovuto accompagnarlo di pari passo: le tradizionali categorie normative si stanno dimostrando inadatte a rispondere alle esigenze di una società in continuo mutamento, rendendo quindi necessaria l'individuazione di nuovi principi e valori validi sul lungo periodo, indipendentemente dai mutamenti tecnologici[2]. La continua connessione a un *network* come il *world wide web* riduce gli spazi privati di ogni singolo individuo, portando a una rivalutazione dell'idea stessa di privacy[3]. Questa non è più intesa esclu-

[1] Dati dell'Organizzazione Internazionale per le Migrazioni aggiornati al 6 marzo 2019, in *migration.com*.

[2] S. Rodotà, *Tecnologie e diritti,* Bologna, 1995, 19 ss.

[3] *Ibid.*

sivamente come *ius excludendi alios*[4], ossia come diritto a non subire ingerenze di alcun tipo nella propria sfera intima[5], ma anche come diritto all'autonomia informativa, cioè ad esprimere la propria volontà su quali dati personali condividere e per quali finalità. Al centro dell'attenzione viene posto l'individuo, che mantiene l'ultima parola sulla disponibilità delle informazioni che lo riguardano e sull'uso che ne viene fatto[6].

Il diritto alla tutela dei dati personali ha un impatto non indifferente anche nelle pratiche di amministrazione dei flussi migratori: i diversi attori impegnati nella gestione di tale emergenza, al fine di fornire un'efficace accoglienza alle migliaia di persone che ogni anno si dirigono verso i confini europei, si trovano a dover raccogliere e processare un'enorme mole di dati personali relativi ai suddetti migranti. Il trattamento di tali informazioni svolge anche una funzione preventiva di tutela della sicurezza e della salute pubblica; le autorità nazionali, analizzando i dati collezionati, possono infatti evitare l'ingresso nel proprio territorio di potenziali minacce per i propri cittadini. Si pensi ad esempio alla prevenzione del terrorismo: gli attentati terroristici dell'11 settembre 2001 hanno segnato un tragico spartiacque nella storia moderna, influenzando radicalmente numerosi aspetti della nostra vita quotidiana.

L'Unione europea ha reagito immediatamente alla minaccia terroristica affermando[7] che gli Stati membri avrebbero impedito l'accesso all'interno dei propri confini a tutti i richiedenti asilo collegati in qualsiasi modo ad associazioni con finalità sovversive, seguendo l'esempio di una precedente risoluzione ONU[8].

Questa presa di posizione ha condotto a controlli sempre più sofisticati per ogni persona intenzionata ad entrare all'interno del territorio europeo[9], giustificando anche la raccolta di informazioni al fine di individuare possibili rapporti tra questa e gruppi terroristici. Le autorità nazionali di frontiera collezionano elementi di diversa natura, come i dati biometrici, i dati relativi alle condizioni igienico-sanitarie, notizie riguardanti la provenienza geografica ed eventuali precedenti penali. L'utilizzo di sistemi di controllo biometrici segue proprio l'esigenza di garantire una maggiore sicurezza all'entrata dei confini nazionali. Si pensi a indicatori come foto digitalizzate, impronte digitali e scansioni dell'iride; la combinazione di uno o più di questi fattori serve per identificare colui che richiede l'ingresso nel Paese[10]. Tali elementi sono poi immagazzinati in *database* che possono essere consultati dalle autorità preposte ai controlli. Simili controlli sono ormai applicati quotidianamente ai confini europei: la mancata corresponsione delle impronte digitali può essere infatti considerata come un illecito[11].

---

4 S.D. Warren - L.D. Brandeis, *The right to privacy,* in *Harvard Law Review,* 4, 1890, 193 ss.

5 T.E. Frosini, *Privacy: diritto fondamentale oppure no,* in *federalismi.it*, 16, 6 agosto 2008.

6 A.F. Westin, *Privacy and freedom,* New York, 1967, 50 ss.

7 Posizione comune del Consiglio del 27 dicembre 2001 relativa alla lotta al terrorismo, 2001/930/CFSP, in *GUUE* 2001 L 344/90, art. 16.

8 Consiglio di Sicurezza delle Nazioni Unite, Risoluzione 1373, 28 settembre 2001, art. 3 (f), in *unodc.org*.

9 B. Hayes, *Migration and data protection: doing no harm in an age of mass displacement, mass surveillance and "big data",* in *International Review of the Red Cross,* 99 (1), 2017, 179 ss.

10 *Ibid.*

11 EU Fundamental Rights Agency, *Fundamental rights implications of the obligation to provide fingerprints for EURODAC,* Vienna, maggio 2015.

La raccolta di queste informazioni viene giustificata con l'esigenza di garantire l'ordine e la sicurezza pubblica dei Paesi di destinazione di tali migrazioni, ma questa necessità non deve far cadere in secondo piano il dovere di tutelare l'autonomia informativa dei migranti coinvolti. Occorre perciò trovare un punto di equilibrio alla luce delle disposizioni normative vigenti.

Il presente articolo vuole proporre una riflessione sulla tensione[12] tra questi due interessi solo apparentemente contrapposti per evidenziare come sia possibile mantenere sicuri i confini europei senza venire meno a una corretta gestione dei dati personali raccolti durante l'amministrazione dell'emergenza migratoria.

A tal proposito occorre partire da un'attenta analisi del Regolamento (UE) 2016/679[13] (d'ora in avanti anche GDPR o il Regolamento), al fine di evidenziare quali disposizioni possono avere un impatto nella gestione dei flussi migratori e dei dati personali delle persone coinvolte. Con una piena cognizione delle disposizioni normative in materia di privacy e *data protection*[14], è poi possibile riflettere sulle azioni europee di contrasto all'immigrazione illegale, al traffico di esseri umani e al crimine transfrontaliero e sulla loro compatibilità con il GDPR.

2. La definizione di "dato personale" fornita dal Regolamento (UE) 2016/679 come influenza le pratiche di gestione della crisi migratoria?

Una qualsiasi informazione che può contribuire a identificare o rendere identificabile una determinata persona: ecco come l'art. 4 del Regolamento (UE) 2016/679 inquadra la nozione di "dato personale". Il GDPR fornisce una definizione molto ampia, poiché i legislatori sono consapevoli di come il progresso tecnologico possa rapidamente portare a nuovi metodi idonei a individuare un singolo soggetto. Nella società attuale, sempre più digitale e informatizzata, elementi come dei marcatori temporanei, ossia i *cookie*, o dei segnali prodotti dai dispositivi utilizzati, come gli indirizzi IP, possono essere dei validi strumenti per identificare in maniera inequivocabile una persona.

Il Regolamento introduce tre diverse categorie di dati personali, non esplicitati chiaramente dalla previgente normativa: i dati genetici, sanitari e biometrici. I primi fanno riferimento alle caratteristiche ereditarie e genetiche dell'interessato, fornendo informazioni univoche sulla sua persona, anche attraverso l'analisi di campioni biologici. Gli elementi che indicano la condizione fisica e lo stato di salute di un individuo, comprensivi dei trattamenti medici a cui si è sottoposto, rientrano invece nella categoria

[12] Sul bilanciamento tra diritti e interessi nell'ambito cibernetico, si rimanda a T.E. Frosini-O. Pollicino-E. Apa-M. Bassini (a cura di), *Diritti e libertà in Internet,* Firenze, 2017.

[13] 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), in *GUUE* L 119, 4 maggio 2016, 1-88.

[14] Per una completa analisi dell'ordinamento normativo europeo in maniera di protezione dei dati personali, si rimanda a F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016.

dei dati sanitari. Una particolare attenzione, anche alla luce dell'ambito della presente analisi, la meritano i cd. dati biometrici. L'art. 4, par. 1, n. 14 del Regolamento indica con tale parola le caratteristiche specifiche di una persona, individuabili attraverso trattamenti automatici specifici come la scansione dell'iride o la raccolta delle impronte digitali.

I dati biometrici possono essere utilizzati per diversi scopi[15]; possono infatti svolgere una funzione di verifica. Le autorità di frontiera possono infatti controllare se colui che esibisce un determinato documento identificativo, come un passaporto o una carta di identità, ne è anche il legittimo proprietario comparando le sue caratteristiche biometriche con quelle immagazzinate nel *chip* informatico di detto documento. L'identificazione biometrica può avere un ruolo importante anche nelle procedure di autorizzazione: la registrazione delle informazioni personali nel VIS[16] (Visa Information System), in combinazione con quelle immagazzinate nei documenti identificativi elettronici, autorizza il legittimo possessore di tale documento a muoversi liberamente all'interno del territorio europeo. I dati biometrici sono inoltre un valido strumento di ricerca, utilizzato dalle forze dell'ordine nella lotta al crimine. L'investigazione forense, per avere una qualche possibilità di successo, deve però poter contare su un'enorme mole di dati.

L'utilizzo dei sistemi di identificazione biometrica può sollevare degli interrogativi sull'effettivo rispetto dei diritti del soggetto a cui tali dati si riferiscono[17]. Le autorità nazionali sono tecnicamente in grado di condurre indagini e controlli anche senza il preventivo assenso della persona coinvolta, semplicemente consultando i *database* a disposizione. Il soggetto viene informato quando le informazioni che lo riguardano vengono consultate? Può consultarle nella maniera che ritiene più opportuna? Simili interrogativi si fanno ancora più pressanti se calati nel contesto dei flussi migratori. Le autorità di frontiera raccolgono una grande quantità di dati biometrici dei migranti, al fine di fornire loro un'accoglienza adeguata e di prevenire l'ingresso nel proprio territorio di soggetti che potrebbero mettere a rischio la sicurezza e la salute pubblica. Il migrante, una volta uscito dalla situazione di emergenza e venute quindi meno le finalità che hanno legittimato la raccolta delle informazioni che lo riguardano, ha la possibilità di rientrare in possesso dei dati che aveva fornito al momento del suo ingresso, impedendone l'ulteriore diffusione? La continua profilazione dell'interessato come "immigrato" potrebbe non essere più necessaria e addirittura nociva per gli interessi dello stesso.

Tornando ad analizzare le disposizioni del Regolamento, si può notare che il testo non fornisce alcuna disciplina in merito ai cd. metadati, ossia informazioni relative ai dati. Una simile lacuna può avere importanti ripercussioni in una società digitale come quella attuale, anche nel campo della tutela dell'autonomia informativa dei migranti. Può

[15] E. Brouwer, *Digital borders and real rights. Effective remedies for third-country nationals in the Schengen Information System,* Leiden-Boston, 2008, 137 ss.

[16] Il Sistema di Informazione Visti, istituito dalla Decisione 2004/512/CE del Consiglio dell'8 giugno 2004 e disciplinato dal Regolamento (CE) 767/2008 del Parlamento europeo e del Consiglio del 9 luglio 2008, è una banca dati centrale a livello europeo a cui sono connesse le autorità nazionali dei singoli Stati membri competenti per il rilascio di visti e passaporti.

[17] E. Brouwer, *Digital borders*, cit., 151.

tornare utile un esempio a tal proposito: le persone, anche durante i loro spostamenti, sono costantemente connessi al *web* attraverso i loro *device* come telefonini e pc portatili, spesso utilizzati anche per interagire con i diversi *social media*. La tecnologia attuale a disposizione delle autorità nazionali e delle Organizzazioni Internazionali coinvolte nella gestione dei flussi migratori permette loro di raccogliere le informazioni che tali connessioni rilasciano, come la direzione del viaggio intrapreso, la localizzazione geografica da cui è avvenuta l'interazione con il *web* o anche eventuali comunicazioni con trafficanti di esseri umani che facilitano l'immigrazione irregolare. Tali informazioni svolgono un ruolo vitale nella lotta alla criminalità e nell'amministrazione delle emergenze migratorie, ma occorre anche considerare che spesso rivelano elementi relativi alla sfera privata delle persone coinvolte senza che queste ne siano consapevoli.

Per poter avere una regolamentazione del trattamento delle informazioni che ricadono nella categoria dei metadati, si deve far riferimento alla Direttiva e-Privacy[18]. La normativa in questione fornisce infatti una definizione di "dati relativi al traffico" (art. 2.b) secondo la quale con questa terminologia si indica qualsiasi dato sottoposto a trattamento al fine di permettere una comunicazione su rete elettronica. Inoltre, con la dicitura di "dati relativi all'ubicazione" (art. 2.c) vengono definite le informazioni relative alla posizione geografica dell'apparecchiatura utilizzata dall'utente per la comunicazione intrapresa.

Secondo l'art. 6 della Direttiva e-Privacy, il fornitore di una rete pubblica per siffatte comunicazioni deve cancellare o rendere anonimi i dati relativi al traffico una volta che questi hanno esaurito la loro funzione primaria. L'art. 9 specifica similmente come le informazioni relative all'ubicazione geografica diverse rispetto a quelle in merito al traffico possono essere trattate solo se appropriatamente anonimizzate o solo previo consenso dell'interessato che deve essere adeguatamente informato in merito a ogni particolarità del trattamento.

Ai fini della presente analisi, occorre comunque ricordare che l'art. 15 della direttiva in esame prevede la possibilità per gli Stati membri di apportare delle deroghe alle previsioni normative appena ricordate per finalità quali la sicurezza interna, la prevenzione e il perseguimento di attività criminali.

La gestione dei flussi migratori potrebbe quindi rientrare nelle attività sottoponibili a deroga, pur dovendo essere comunque rispettati i diritti fondamentali di migranti e rifugiati e i principi sanciti dal GDPR, quali la necessarietà, la giustizia e correttezza del trattamento dati.

[18] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in *GU* L201 del 31 luglio 2002, 37-47.

2.1. La raccolta di dati appartenenti alle categorie particolari cui all'art. 9 del Regolamento (UE) 2016/679 da parte delle autorità nazionali di frontiera può dirsi legittima?

Il trattamento di un particolare tipo di informazioni, chiamate comunemente dati sensibili, viene disciplinato in maniera specifica dal GDPR. L'art. 9 del Regolamento vieta infatti il trattamento dei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale del soggetto a cui si riferiscono o il suo orientamento sessuale. Il divieto si estende anche alle categorie esaminate nel paragrafo precedente, ossia i dati genetici, biometrici o sanitari.

Le autorità di frontiera raccolgono però quotidianamente tali dati, poiché il par. 2 del medesimo art. 9 elenca una serie di casi in cui il divieto appena esposto non trova applicazione. Il trattamento dei dati cd. "sensibili" può essere condotto se necessario per motivi di interesse pubblico sulla base del diritto dell'Unione europea e degli Stati membri. Tale trattamento deve però rispettare i principi della *data protection*, prevedere misure specifiche per la tutela dei diritti fondamentali delle persone coinvolte e deve essere proporzionato alle finalità perseguite. Il carattere di proporzionalità non può ovviamente essere preventivamente definito, ma deve essere riscontrato nel caso concreto. L'art. 8 della Convenzione europea dei diritti dell'uomo[19] afferma che ogni individuo ha il diritto a veder rispettata la propria vita privata e familiare, riconoscendo che le uniche ingerenze a tale principio possono essere giustificate solo in caso di necessità nazionale. La giurisprudenza della Corte europea dei diritti dell'uomo ha solitamente lasciato un buon margine di discrezionalità alle autorità nazionali per valutare l'effettivo bisogno di un'interferenza nel diritto alla privacy di determinati soggetti per finalità di sicurezza nazionale o di prevenzione del crimine[20]. Tale discrezionalità non può però portare a trascurare i diritti legittimamente vantati dai soggetti coinvolti. L'analisi appena svolta porta a una riflessione sull'effettiva necessità di controlli così pervasivi all'ingresso di una frontiera europea. La raccolta di dati "sensibili" come gli identificativi biometrici e il loro successivo deposito in *database* a cui il soggetto migrante ha spesso un accesso perlomeno complesso e difficoltoso, può essere considerata una misura proporzionata alle finalità di sicurezza pubblica? La Corte europea dei diritti dell'uomo ha più volte specificato che, pur riconoscendo la validità di tali finalità, il diritto alla privacy e all'autonomia informativa dei soggetti coinvolti non può venir meno.

[19] Convenzione europea dei diritti dell'uomo, firmata nell'ambito del Consiglio di Europa il 4 dicembre 1950, *ecr.coe.int.*

[20] Corte EDU, *Leander c. Svezia,* ric. 9248/81 (1987); *Klaas c. Germania*, ric. 15473/89 (1993); cfr. E. Brouwer, *Digital borders,* cit., 173 ss.

3. Quali diritti possono vantare i migranti relativamente al trattamento dei propri dati personali alla luce di quanto disposto dal Regolamento (UE) 2016/679?

L'era digitale in cui viviamo, dove ogni individuo è costantemente connesso al grande *network* comunicativo chiamato *cyberspace*, ha rivoluzionato ogni aspetto della nostra vita quotidiana e ha creato un nuovo tipo di "moneta", ossia il dato. Le moderne compagnie commerciali si servono delle informazioni che ogni persona condivide quotidianamente in rete per fornire prodotti e servizi sempre più adatti ai bisogni del singolo consumatore. L'amministrazione pubblica non fa eccezione nella valorizzazione del dato: gli Stati raccolgono imponenti quantità di informazioni riguardanti i propri cittadini per gestire in maniera efficiente la "cosa pubblica". Il dato personale ha quindi un'importanza rilevante nella società attuale ed è un elemento imprescindibile per la corretta affermazione della propria identità individuale, e per questo deve essere accuratamente tutelato. Il diritto all'autonomia informativa prevede che il soggetto interessato dal trattamento dei propri dati personali sia pienamente consapevole delle finalità per cui le informazioni che lo riguardano sono state raccolte e delle modalità con cui i suddetti dati sono effettivamente processati. L'intento è quello di evitare qualsiasi tipo di abuso da parte del titolare del trattamento, sia esso un ente pubblico o privato. Le finalità di interesse nazionale perseguite da uno Stato non possono perciò giustificare un'illimitata ingerenza nella sfera privata del singolo individuo.
Il soggetto interessato ha quindi una serie di diritti, riconosciuti dal diritto internazionale e dalla normativa europea, che può vantare nei confronti del titolare che porta avanti il trattamento dei suoi dati personali. Ai fini della presente analisi, può essere utile riflettere su quali tra questi diritti possono risultare utili per i soggetti migranti e attraverso quali modalità di tutela.

3.1. Il diritto ad accedere ai propri dati personali. I soggetti migranti possono accedere ai dati personali che li riguardano raccolti dalle autorità nazionali di frontiera?

Uno degli strumenti principali per impedire un qualsiasi abuso da autorità statali o da terze parti in merito all'utilizzo dei dati personali raccolti è il diritto ad essere informati. Questo si concretizza nel diritto del soggetto interessato a poter accedere alle informazioni che lo riguardano e nel dovere del titolare del trattamento di rendere edotto quest'ultimo delle finalità del trattamento stesso e delle modalità con cui questo viene condotto[21].
L'art. 8 della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Trattato n. 108)[22] afferma che ogni persona

[21] E. Brouwer, ivi, 201.

[22] Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, STE n. 108, firmata nell'ambito del Consiglio di Europa a Strasburgo il 28 gennaio 1981.

ha il diritto di venire a conoscenza se è in corso un trattamento automatico dei propri dati personali, le sue finalità nonché le generalità e i contatti del soggetto che sta conducendo suddetto trattamento.
Gli artt.13-15 del GDPR specificano in maniera dettagliata le informazioni che il soggetto interessato ha diritto di sapere in merito al trattamento dei dati personali che sta subendo. L'art. 15, rubricato come "Diritto di accesso dell'interessato", prevede che quest'ultimo debba essere reso edotto su questioni quali la finalità del trattamento, i soggetti con cui saranno condivise le informazioni che lo riguardano, la durata della fase di gestione dei dati nonché della possibilità di rivolgersi a un'autorità garante per far valere i propri diritti.
Considerato ciò, occorre chiedersi come la disciplina del GDPR trovi applicazione per quanto riguarda i controlli effettuati nei confronti dei migranti che chiedono di entrare nei confini europei. La Convenzione[23] per l'applicazione dell'Accordo di Schengen, che vede l'abolizione delle frontiere interne tra i Paesi firmatari, all'art. 109 specifica che ogni individuo ha il diritto di chiedere l'accesso ai propri dati secondo quanto previsto dalla normativa nazionale di ogni Stato membro. Tale diritto deve essere poi esercitato attraverso l'ausilio dell'autorità garante preposta. La Convenzione prevede però due significative limitazioni all'esercizio della prerogativa appena esposta di cui bisogna tenere conto. Qualora lo Stato verso il quale viene rivolta la richiesta di accesso non è quello che concretamente detiene i dati oggetto di domanda, questo ha la possibilità di esprimere il proprio parere sulla richiesta effettuata: un simile procedimento rischia di provocare ritardi nel rilascio delle informazioni domandate. La seconda restrizione prevede invece che il Paese richiesto possa rifiutarsi di rilasciare i dati in proprio possesso quando questi sono necessari per l'adempimento di un obbligo giuridico o servono per operazioni di sorveglianza e prevenzione del crimine. Una simile disposizione concede un ampio margine di discrezionalità al Paese detentore dei dati personali del soggetto che può facilmente portare a un abuso, qualora non ci sia un'attenta valutazione del caso concreto.

3.2. Il diritto all'oblio per i dati personali dei migranti raccolti dalle autorità statali ai confini europei

Il diritto all'oblio consiste nel diritto ad essere "dimenticato": il soggetto interessato può chiedere al titolare del trattamento che i dati che lo riguardano vengano appunto cancellati e fatti cadere nell'oblio. Non ci si limita quindi a impedirne la successiva

Ai fini di una completa trattazione, occorre segnalare il processo evolutivo a cui è stata sottoposto il documento, culminato nella sua versione emendata consultabile in *rm.coe.int*. La Convenzione cd. "modernizzata" vuole tenere il passo dell'incessante progresso tecnologico, instaurando un dialogo con altri strumenti normativi regionali quali il GDPR. La possibilità di firmare la Convenzione anche da parte di Stati non appartenenti al Consiglio di Europa fa sì che lo standard di tutela raggiunto possa essere quanto più globale e uniforme possibile.

[23] Acquis di Schengen - Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni, in *GU* L 239, 22 settembre 2000, 19-62.

diffusione, poiché dette informazioni vengono definitivamente tolte dalla disponibilità di un potenziale pubblico. Un simile diritto ha una possibile ampia applicazione nel contesto cibernetico, dove l'interessato può richiedere la rimozione di *link* e contenuti che lo riguardano e che lui ritiene potenzialmente lesivi per la sua immagine e per la sua limitazione, ma potrebbe avere una qualche rilevanza anche nel contesto dei controlli alle frontiere a cui sono sottoposti i soggetti migranti.

Il diritto all'oblio è principalmente frutto di una lunga elaborazione giurisprudenziale che vede il suo momento culminante nella famosa sentenza *Google Spain*[24]. Il Regolamento (UE) 2016/679 disciplina per la prima volta a livello europeo tale diritto, riconoscendo all'art. 17 che l'interessato ha la facoltà di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo qualora sussistano determinati requisiti. Per le finalità della presente trattazione, si vuole rivolgere l'attenzione in maniera particolare al motivo elencato all'art. 17, par. 1, lett. *a)*, ossia quando viene meno la finalità per cui i dati sono stati effettivamente raccolti. Quando può dirsi raggiunto lo scopo prefissato dalla collezione e catalogazione dei dati raccolti da parte delle autorità nazionali di frontiera nei confronti dei soggetti migranti? Come esplicitato più volte, tali dati vengono raccolti per garantire un'accoglienza più efficace e per prevenire l'ingresso nel territorio statale di potenziali rischi per la sicurezza e la salute pubblica. Ad un primo esame sembrerebbe quindi che, una volta scongiurati tali pericoli, non ci sia più necessità di mantenere nei *database* i dati raccolti. Non rilasciare suddette informazioni potrebbe condurre a un trattamento discriminatorio, dove il soggetto migrante vede "immagazzinati" senza alcun limite di tempo prefissato i dati che lo riguardano solo per il motivo di essere immigrato nel detto Paese.

L'art. 17, similmente alle altre disposizioni del GDPR prese in esame, dispone alcuni limiti all'applicazione del diritto all'oblio. Questo non trova infatti spazio qualora il titolare del trattamento collezioni e gestisca dati personali perseguendo un interesse pubblico o nell'esercizio di pubblici poteri. Le riflessioni in merito a tale disposizione sono le medesime che sono state sollevate anche nelle restrizioni previste all'esercizio del diritto di accesso; l'interesse dell'intera comunità nazionale non può condurre ad ingerenze abusive nella sfera privata del singolo soggetto.

3.3. Il diritto alla portabilità dei dati e la sua applicazione nella gestione della crisi migratoria

La tendenza a migrare, spostandosi da un luogo all'altro nel corso della sua vita, è insita nell'essere umano sin dalla notte dei tempi. La storia umana è stata caratterizzata da innumerevoli migrazioni e l'epoca attuale non fa alcuna distinzione. A differenza dei tempi passati, la società attuale si caratterizza però per una maggiore digitalizzazione, dove il dato personale diventa un complemento imprescindibile di ogni singola persona, volto a definirne l'identità. Occorre perciò riflettere se, ed eventualmente secondo quali modalità, i dati che ci riguardano ci seguono durante i nostri spostamenti e i

[24] CGUE, C-131/12, *Google Spain* (2014).

nostri viaggi.
L'art. 20 del Regolamento (UE) 2016/679 prevede il cd. diritto alla portabilità dei dati, che consente al soggetto interessato di richiedere le proprie informazioni personali fornite al responsabile del trattamento dati in un formato strutturato, di uso comune e leggibile attraverso mezzi automatici, senza che il predetto responsabile possa ostacolare o rifiutarsi di soddisfare tale richiesta. La *ratio legis* di questa disposizione è di permettere all'interessato di entrare in possesso delle informazioni condivise con il titolare del trattamento, per poterne avere effettiva contezza e piena cognizione di causa. L'interessato è così in grado di rivolgersi eventualmente a un altro fornitore di servizi, dato che le informazioni gli sono state fornite in un formato comprensibile dagli strumenti automatici e comunemente utilizzato.
Il Regolamento sembra incentivare una sorta di "interoperabilità"[25]; il diritto alla portabilità dei dati presuppone infatti la possibilità di una sorta di dialogo tra i diversi strumenti di lettura dati che devono essere infatti in grado di interpretare correttamente un formato comune, permettendo così di "portare" i dati da un operatore all'altro. Anche per quanto riguarda il diritto alla portabilità, come nei casi precedentemente esaminati, il GDPR prevede una deroga all'applicazione nel caso in cui la gestione delle informazioni sia condotta per finalità di interesse pubblico. L'amministrazione dei flussi migratori rientra ovviamente in tale casistica, facendo sì che i migranti non possano legittimamente vantare alcun diritto alla portabilità dei propri dati che sono stati collezionati al momento del loro ingresso in Europa.
È opinione di chi scrive che tale facoltà debba essere riconosciuta, seppur non attraverso un obbligo normativo, anche ai migranti. Tali persone infatti, spesso non si fermano stabilmente nel Paese di primo approdo, preferendo proseguire il proprio viaggio verso altri Stati membri dell'Unione europea. Una collaborazione tra le autorità di frontiera delle nazioni coinvolte, all'insegna dell'interoperabilità sopra auspicata, potrebbe portare a una gestione ancora più efficiente di tali flussi migratori interni. L'utilizzo di sistemi automatici di lettura dati "intercompatibili" permetterebbe inoltre ai migranti di non dover sottostare a ritardi e lungaggini burocratiche per entrare in possesso dei dati condivisi, in adempimento di quanto visto in merito al diritto di accesso.

3.4. La profilazione automatica ai confini europei e la sua legittimità alla luce delle disposizioni del GDPR

I dati riguardanti i migranti che chiedono di entrare in territorio europeo vengono raccolti e immagazzinati in diversi *database*, di cui si darà contezza nel proseguimento della trattazione, al fine di analizzare se detti individui possono creare un rischio per la sicurezza e la salute pubblica. Le informazioni collezionate consentono quindi una sorta di profilazione del migrante, ma questo è un procedimento legittimo?
L'art. 22 del Regolamento (UE) 2016/679 sancisce che l'interessato ha il diritto di non

[25] L. Scudiero, *Bringing your data everywhere: a legal reading of the right to portability,* in *European data protection Law Review,* 1, 2017, 119 ss.

essere sottoposto a una decisione che si basa esclusivamente su qualsiasi trattamento automatico, compresa per l'appunto la profilazione, che possa produrre effetti giuridici nei suoi confronti o che comunque incida in modo analogo. Il medesimo articolo specifica però che una simile decisione può essere presa qualora sia autorizzata dal diritto dell'Unione europea o dalla normativa nazionale del titolare del trattamento. Devono essere però previste delle adeguate garanzie per la tutela dei diritti fondamentali dell'interessato, che ha anche la possibilità di ricorrere in giudizio contro l'esito della decisione.

Come detto poc'anzi, la procedura di rilascio dei visti e dei permessi di soggiorno negli Stati europei si basa anche e soprattutto sui dati raccolti nel momento in cui il soggetto migrante chiede di entrare in territorio europeo. L'analisi delle caratteristiche dell'interessato attraverso l'esame, anche automatico, dei suoi dati è quindi legittimo, ma quest'ultimo deve essere reso edotto dei suoi diritti, compreso quello di far intervenire un essere umano per analizzare concretamente il caso, non lasciando quindi ogni decisione in mano alla macchina.

4. I "confini digitali" dell'Unione europea: l'utilizzo di sistemi tecnologici per garantire la sicurezza interna e i suoi profili giuridici

Le risposte politiche e normative dell'Unione europea in merito alla tutela della sicurezza interna e dei propri confini sono spesso state dettate dalla volontà di rispondere a minacce di vario tipo[26]. Ad esempio, gli attacchi terroristici contro la redazione del giornale terroristico di *Charlie Hebdo* hanno condotto all'approvazione di alcuni discussi provvedimenti normativi in merito alla sicurezza alle frontiere[27]. Le istituzioni europee fecero infatti un significativo passo in avanti[28] per l'implementazione dei codici di prenotazione (PNR) in un'ottica di prevenzione a futuri atti di terrorismo identificando i percorsi di viaggio di potenziali attentatori, seppur in contrasto con le preventive dichiarazioni a tutela della privacy dei passeggeri[29]. In questa continua ricerca di sicurezza, un ruolo fondamentale viene svolto dagli strumenti tecnologici. Le pratiche di sorveglianza digitale sono da tempo al centro del dibattito politico, poiché rischiano di causare un grave *vulnus* alla privacy degli individui coinvolti. L'impiego della tecnologia ai confini europei non ha però causato grande scalpore[30]e indignazione pubblica: la

[26] R. Bossong - H. Carrapico, *The multidimensional nature and dynamic transformation of European borders and internal security,* in R. Bossong - H. Carrapico (eds.) *Eu borders and shifting internal security. Technology externalization and accountability,* Londra, 2016, 1 ss.

[27] D. Bigo, *The EU counter-terrorism policy responses to the attacks in Paris: Towards an EU security and liberty agenda,* in *CEPS Liberty and Security in Europe,* 81, 2015, 1 ss.

[28] Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27.04.2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

[29] A. Ripoll Servent, *Institutional and policy change in the European Parliament. Deciding on Freedom, Security and Justice*, Londra, 2015, 13 ss.

[30] M. Leese, *The new profiling: Algorithms, black boxes, and the failure of antidiscriminatory safeguards in the*

maggioranza della popolazione è rimasta infatti indifferente a misure apparentemente non invasive, come l'applicazione del PNR o l'attivazione di *database* di raccolta dati come EURODAC. Consapevole di ciò, l'Unione europea sta spendendo grandi quantità di denaro per finanziare una sorveglianza digitale dei propri confini ed è quindi utile proporre una breve analisi dell'azione europea a difesa delle frontiere.

4.1. L'Unione europea e il controllo digitale dei confini marittimi: il sistema EUROSUR

Gli episodi forse più eclatanti che caratterizzano in maniera indelebile l'emergenza migratoria che l'Unione europea sta affrontando da ormai diversi anni si hanno nel mar Mediterraneo. Aumentando sempre più il numero di persone che tenta una pericolosa traversata per raggiungere le coste di Paesi come Italia o Spagna, aumenta anche il numero di vite perse in mare. A seconda del loro luogo di partenza, i migranti trascorrono da 1 fino a 4 giorni sopra piccoli vascelli, inadatti a simili viaggi e stipati fino all'inverosimile, in condizioni igieniche a dir poco precarie e spesso senza provviste. In aggiunta, devono anche subire le violenze e gli abusi dei trafficanti di esseri umani che contribuiscono a rendere un simile viaggio ancora più pericolo. Si stima che, nel solo periodo da gennaio a luglio 2015, ben 3500 persone abbiano perso la vita nel Mediterraneo tentando di raggiungere i territori europei[31].
Il controllo del confine marittimo viene portato avanti anche attraverso l'ausilio di dispositivi tecnologici, per cercare di prevenire il ripetersi di simili tragedie.
Le istituzioni europee hanno visto nel sistema di sorveglianza EUROSUR[32] il risultato delle *best practices* portate avanti dai singoli Paesi membri nell'ambito del controllo dei propri confini e il modo per raggiungere tre distinti obbiettivi.
In primis, la riduzione del numero delle persone che entrano illegalmente in territorio europeo: gli strumenti di controllo dovrebbero fornire alle autorità di frontiera informazioni affidabili e tempestive in maniera tale da contrastare il fenomeno dell'immigrazione illegale. EUROSUR dovrebbe inoltre contribuire a prevenire episodi di crimine transfrontaliero: i dati raccolti attraverso le operazioni di sorveglianza sono un valido aiuto per le forze di polizia per sventare crimini come il traffico di esseri umani, di armi e di droga. Infine, le informazioni fornite dai sistemi di sorveglianza dovrebbero aiutare a evitare ulteriori tragedie nel mar Mediterraneo. Le autorità di guardia costiera dei Paesi membri possono infatti contare su informazioni dettagliate su eventuali vascelli in difficoltà per intervenire tempestivamente in aiuto.
Per raggiungere questi ambiziosi scopi, EUROSUR deve supportare gli Stati a raggiungere una piena conoscenza della situazione di ciò che succede ai loro confini e ad

European Union, in *Security Dialogue,* 45 (5), 2014, 494 ss.; L. Verbugt, *A plea for technological activism at the European borders,* in *Science as Culture,* 21(3), 2012, 409 ss.

[31] R. Bossong - H. Carrapico, *The multidimensional nature,* cit., 12.

[32] Regolamento (UE) 1052/2013 del Parlamento europeo e del Consiglio che istituisce il sistema europeo di sorveglianza delle frontiere (EUROSUR), 22 ottobre 2013, in *GUUE* L 295/11 del 6 novembre 2013, 1-16.

aumentare la loro capacità di reazione nell'attuazione della legge[33]. In base alla "conoscenza della situazione" si misura la capacità delle autorità di scoprire i movimenti transfrontalieri e di individuare i motivi validi per applicare misure di controllo, mentre la "capacità di reazione" determina il tempo necessario per mettere sotto controllo un movimento transfrontaliero e anche il tempo e i mezzi da impiegare per reagire adeguatamente a circostanze insolite. Il funzionamento di EUROSUR sembra "tradurre" scelte prevalentemente politiche, come le azioni da intraprendere a difesa dei confini nazionali, in concetti misurabili e quantificabili[34].

Le istituzioni europee hanno previsto tre diverse fasi per l'effettiva messa in opera di un così ambizioso sistema di sorveglianza: il primo *step* consiste nella connessione e nella collaborazione tra gli enti dei Paesi coinvolti preposti al controllo dei confini. L'attenzione si sarebbe poi rivolta successivamente a un periodo di ricerca e sviluppo volto a migliorare le capacità tecniche degli operatori e le soluzioni tecnologiche impiegate. La fase finale era invece incentrata a far sì che i dati e le informazioni raccolte a ogni livello venissero analizzate in un'ottica comune, a vantaggio di tutti gli attori partecipanti a EUROSUR.

L'efficace sorveglianza di un territorio complesso come il mar Mediterraneo presenta delle sfide da non trascurare; l'Unione europea non può infatti limitarsi a tenere conto di quando un determinato soggetto ha oltrepassato la linea di un confine. L'attenzione deve essere cruciale su ogni possibile segnale di anomalia. A tal proposito, l'analisi svolta da EUROSUR è "tarata" non solo sul comportamento umano, ma anche sugli elementi artificiali. L'individuo non viene analizzato in quanto tale, ma solamente se è in gruppo con altri soggetti o su veicoli, come ad esempio una barca. La sorveglianza non si focalizza sul singolo e sulle sue caratteristiche, ma sul suo comportamento e sulla eventuale "anomalia" che questo dimostra rispetto alla statistica. Se una persona si comporta come il sistema di sorveglianza ritiene che debba fare secondo quanto esaminato in casi precedenti, non scatterà nessun allarme.

Il funzionamento di EUROSUR può prestare il fianco a diverse critiche, specialmente in merito alla tutela dei dati personali delle persone coinvolte. Il sistema di sorveglianza potrebbe andare infatti a raccogliere informazioni riguardanti persone che non sono direttamente coinvolte dalle operazioni di controllo e che nulla hanno a che fare con eventuali crimini transfrontalieri. Una raccolta dati su base quantitativa, mirata a collezione più informazioni possibili per formulare analisi statistiche atte a prevedere determinati eventi, non tiene infatti conto della tutela della privacy del singolo soggetto. Come già specificato, EUROSUR è un "sistema di sistemi di sorveglianza", ossia mette in connessione gli apparati di controllo dei vari Stati membri dell'Unione europea per portarli a un ulteriore livello di efficienza. Il suo carattere transnazionale pone però degli importanti quesiti in merito all'effettiva gestione dei dati raccolti. Le informazioni provenienti da un Paese possono essere infatti richieste dalle autorità di uno

[33] Memo/08/86, Esame della creazione di un sistema europeo di sorveglianza delle frontiere (EUROSUR).

[34] R. Bellanova - D. Duez, *The making (sense) of EUROSUR: how to control the sea borders?,*in R. Bossong -H. Carrapico (eds.), *Eu borders and shifting internal security. Technology externalization and accountability,* Londra, 2016, 23 ss.

Stato diverso, rendendo assai difficoltoso per il soggetto interessato capire chi effettivamente si sta occupando dei dati che lo riguardano e per quali finalità, a detrimento del suo diritto di accesso. Altrettanto complesso sarebbe inoltre individuare a quale giudice nazionale il suddetto interessato deve rivolgersi per far valere i propri diritti.

4.2. I database (Eurodac, Vis, Sis) e i controlli alle frontiere europee

L'abolizione dei confini interni per applicare la libertà di movimento per le persone ha portato gli Stati membri a richiedere l'applicazione di "misure compensatorie" che potessero sopperire ai controlli doganali venuti meno. La Commissione europea riconobbe, nel White Paper[35] del 1985, che la cooperazione amministrativa e giudiziaria tra le forze di polizia dei Paesi membri, che si concretizza anche nello scambio di informazioni, potesse rientrare in tale ottica. I *database* istituiti dall'Unione europea per immagazzinare i dati raccolti dai soggetti che richiedono di entrare nei confini degli Stati membri svolgono un ruolo importante per permettere la collaborazione tra le diverse autorità statali.

Il fulcro[36] di queste misure compensatorie, volte a minimizzare gli effetti dell'abolizione dei controlli doganali interni, è il sistema di informazione Schengen (SIS). Si tratta di una banca dati operativa dal 1995 che permette alle autorità nazionali facenti parte dell'area di Schengen di scambiarsi informazioni relative alle identità di specifiche persone o beni. Gli artt.95-100 della Convenzione di applicazione dell'Accordo di Schengen chiariscono che solo i dati relativi a determinate categorie di persone rientrano in tale archivio. Si fa infatti riferimento a individui su cui pende una richiesta per estradizione (art. 95), a persone provenienti da Stati terzi all'Unione europea a cui è stato rifiutato l'ingresso nel territorio europeo (art. 96), a soggetti scomparsi (art. 97) o ricercati dalle pubbliche autorità in quanto testimoni o imputati in un processo (art. 98) o a persone sospettate di pianificare crimini (art. 99).

Eurodac[37] è un perfetto esempio di come la collaborazione tra forze di polizia si svolga anche attraverso l'ausilio di strumenti tecnologici. Si tratta infatti di un archivio in cui vengono depositate le impronte digitali, quindi dati biometrici, di richiedenti asilo e migranti irregolari. Fa parte integrante del cd. "Sistema Dublino", poiché funziona

[35] Commissione europea, *Completare il Mercato Interno: White Paper dalla Commissione al Consiglio,* Milano, 28-29 giugno 1985, COM/85/0310 FINAL.

[36] B. Schattenberg, *Schengen Information System:privacy and legal protection,* in *Free movement of persons in Europe*, Dordrecht, 1993, 43 ss.

[37] Regolamento (UE) 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013 , che istituisce l'Eurodac per il confronto delle impronte digitali per l'efficace applicazione del Regolamento (UE) 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il Regolamento (UE) 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia, in *GUUE* L180, 29 giugno 2013, 78-107.

nelle aree di applicazione del Regolamento[38] Dublino III. Il principio fondamentale di detta regolamentazione si può riassumere con "chi inquina paga"[39]: lo Stato che ha "causato" l'ingresso nel territorio europeo di un migrante irregolare, ad esempio attraverso il rilascio di un visto o per una falla nei controlli di frontiera, deve poi farsi carico della procedura di asilo. La consultazione del *database* Eurodac permette quindi di individuare detto Paese.

La creazione di un unico confine europeo non può prescindere da una politica uniforme che coinvolga tutti i Paesi membri in materia di visti; la banca dati VIS ha risposto a questa esigenza. Un simile archivio si prefigge diversi scopi, come la lotta all'immigrazione illegale e alla diffusione del terrorismo e la prevenzione di pratiche di *visa shopping*, ossia di coloro che "scelgono" il Paese con la normativa più permissiva nella speranza di ricevere una risposta positiva alla propria domanda di visto.

I tre archivi che sono stati appena presentati mostrano alcune caratteristiche in comune; si parla infatti di tre distinti *database* che rispondo all'esigenza dei Paesi membri dell'Unione europea di controllare l'ingresso e la circolazione dei migranti provenienti da Stati terzi all'interno del proprio territorio. La consultazione di detti archivi da parte dei soggetti preposti è possibile a tre distinti livelli; le autorità possono accedervi non solo al momento del controllo al confine esterno dell'Unione europea, ma anche dal territorio nazionale interno e anche dalle proprie ambasciate e consolati nei Paesi terzi.

La maggiore differenza tra questi *database* è data dai criteri secondo i quali le informazioni riguardanti uno specifico individuo vengono registrate. Il SIS si attiva infatti esclusivamente nel caso in cui una determinata persona viene ritenuta "pericolosa" per la sicurezza pubblica, a differenza di Eurodac, che registra le impronte digitali di ogni richiedente asilo, e di VIS, che raccoglie le informazioni relative ai visti indipendentemente dalla "pericolosità" del loro proprietario.

Una simile differenza in termini di approccio può causare una sostanziale disparità di trattamento: la profilazione preventiva di un soggetto solo perché ritenuto suscettibile di commettere crimini può infatti ledere la sua sfera privata e la sua autonomia informativa.

5. La tutela dei dati personali e la lotta al traffico di esseri umani

La tecnologia si sta dimostrando essere un valido alleato nella lotta a fenomeni criminali come il traffico di esseri umani e il favoreggiamento dell'immigrazione illegale. Lo sviluppo di sistemi di sorveglianza sempre più accurati deve però andare di pari passo con un'attenta consapevolezza delle forze di polizia in merito alla tutela dei dati personali delle persone coinvolte in tali episodi, specialmente delle vittime.

[38] Regolamento (UE) 604/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide, in *GUUE* L180, 29 giugno 2013, 31 ss.

[39] E. Brouwer, *Digital borders,* cit., 223.

La fase di raccolta e catalogazione delle informazioni, imprescindibile nelle indagini riguardanti i crimini sopra menzionati, deve infatti avvenire in pieno rispetto della privacy delle persone coinvolte.
L'utilizzo di strumenti di geo-localizzazione può funzionare perfettamente da esempio per la presente analisi: il tracciamento della posizione dei sospetti trafficanti può infatti aiutare a prevenire il compimento di crimini transfrontalieri, ma occorre tener presente diverse questioni. La fase di rilevamento può "captare" informazioni relative a persone totalmente estranee ai sospetti traffici e che sono quindi inconsapevoli del fatto che i propri dati sono raccolti e catalogati. L'elemento transfrontaliero solleva inoltre dei dubbi relativi a chi ha effettivamente la facoltà di raccogliere le suddette informazioni ed entro quale quadro normativo. Considerato ciò, si auspica che strumenti tecnologici potenzialmente invasivi, come quelli utilizzati nelle pratiche di geo-localizzazione, vengano utilizzati esclusivamente quando necessario, informando dei propri diritti eventuali terzi coinvolti.
Riflessioni simili possono essere fatte in merito all'utilizzo di droni nelle operazioni di sorveglianza dei confini, pur considerando che il loro impiego è ancora effettivamente limitato da parte dei Paesi europei[40]. Tali velivoli possono fornire importanti informazioni alle autorità di frontiera, coadiuvando le forze di polizia nella lotta ai crimini transfrontalieri. La registrazione delle immagini attraverso un drone non è pero individuale e precisa, focalizzata su un singolo soggetto; può infatti "catturare" dati riguardanti soggetti terzi. Considerato ciò, occorre utilizzare detti strumenti con la dovuta cautela, analizzando attentamente le circostanze della realtà in cui vengono impiegati.

5.1. *Data protection* nell'ottica di prevenzione e repressione dei reati: la direttiva (UE) 2016/680

La gestione e il trattamento dei dati personali possono rappresentare degli utili strumenti per la prevenzione e la repressione di reati, come anche il traffico di esseri umani e il favoreggiamento dell'immigrazione illegale.
Le finalità di interesse pubblico e giustizia penale non possono però giustificare il mancato rispetto del diritto alla privacy e all'autonomia informativa delle persone coinvolte. La direttiva (UE) 2016/680[41] vuole trovare un punto di incontro tra queste due prospettive apparentemente contrapposte.
L'ambito di applicazione della suddetta normativa include qualsiasi trattamento dati effettuato da autorità competenti, segnatamente le autorità e gli enti pubblici incaricati

[40] L. Marin - K. Krajkova , *Deploying drones in policing European borders: constraints and challenges for data protection and human rights,* in A. Zavrinsk (ed.)*, Drones and Unmanned Aerial Systems: Legal and Social Implications for Security and Surveillance,* Londra, 2016, 12 ss; F.Merenda, *Deliberazione, giudizio e responsabilità nell'epoca degli Autonomous Weapons Systems* (AWS*): sulle sfide etiche e giuridiche poste dalla sostituzione di soldati umani con sistemi robotici*, in *Ragion Pratica*, 1, 2020, 263 ss.

[41] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in *GU* L 119 del 4 maggio 2016, 89-131.

della funzione di prevenzione e repressione dei reati,
Le fonti dalle quali tali autorità possono ricavare i dati necessari per le finalità di indagine e giustizia penale non sono tassativamente elencate, al fine di non limitare in alcun modo le modalità di azione dei soggetti coinvolti. Il considerando 3 della direttiva specifica infatti che il costante progresso tecnologico ha creato nuovi strumenti per la raccolta di dati personali che erano inimmaginabili fino a pochi anni fa. Sono ora possibili operazioni di sorveglianza molto più pervasive e penetranti, arrivando a controllare un numero astrattamente indefinito di persone che entrano anche solo casualmente in contatto digitale con il soggetto al centro delle indagini.
A tal proposito, l'art. 29 della direttiva elenca una serie di requisiti che le autorità competenti titolari del trattamento devono obbligatoriamente rispettare per salvaguardare i diritti in questione. Si fa riferimento alle tecnologie e alle strutture utilizzate, alle modalità di conservazione dei dati raccolti e al loro trasporto e alle informazioni da condividere con il soggetto interessato al trattamento.
Focalizzando l'attenzione sulle finalità del presente articolo, si può osservare che le autorità nazionali possono certamente sfruttare la raccolta di dati e informazioni per combattere fenomeni criminali come il traffico di esseri umano o lo sfruttamento dell'immigrazione illegale, ma questo deve avvenire all'interno di precisi limiti giuridici per poter salvaguardare i diritti delle persone coinvolte da queste operazioni di sorveglianza tecnologica.

6. Conclusioni

Tutela dell'identità personale dei migranti ed esigenza di mantenere sicuri i propri confini e il proprio territorio: l'azione dell'Unione europea nella gestione della crisi migratoria deve tenere conto di questi due profili apparentemente contrapposti, alla ricerca di un difficile punto di equilibrio. Il dovere dello Stato di impedire che qualsiasi minaccia possa entrare attraverso le frontiere per turbare la sicurezza pubblica non può infatti legittimare la violazione dei diritti fondamentali dei migranti controllati.
Il Regolamento (UE) 2016 dovrebbe, auspicabilmente, impedire che le autorità nazionali che hanno raccolto i dati delle persone coinvolte nei flussi migratori possano utilizzare tali informazioni in maniera abusiva. Il GDPR garantisce al soggetto interessato determinati diritti riguardanti il trattamento dei propri dati personali; la presente analisi si è soffermata in particolare su quanti tra questi potessero avere una particolare rilevanza per garantire ai migranti il pieno potere sui propri dati personali.
Il diritto all'accesso assicura di poter avere piena contezza di quali informazioni ogni persona ha condiviso, per quali finalità e con quali soggetti. Il diritto alla portabilità dei dati permette, nelle circostanze previste dalla normativa, di entrare concretamente in possesso di dette informazioni mentre il diritto all'oblio dà la possibilità all'interessato di richiedere che i propri dati vengano cancellati se non rispondono più ad alcuna funzione pubblica.
La gestione della crisi migratoria coinvolge però degli interessi nazionali di cui si deve tenere logicamente conto, anche nel trattamento dei dati personali; il GDPR specifica

quindi delle deroghe ai diritti summenzionati quando i dati vengono raccolti nell'esercizio di pubblici poteri per finalità di interesse pubblico.
Non è possibile individuare aprioristicamente e preventivamente le circostanze in cui il diritto alla privacy e all'autonomia informativa personale può essere "compresso" a favore di un beneficio per l'intera comunità dei cittadini; una simile valutazione deve essere giocoforza lasciata alle autorità nazionali preposte ed eventualmente esaminata in sede giurisdizionale. L'art. 8 della Convenzione europea sui diritti dell'uomo specifica che ogni ingerenza alla vita privata di un individuo deve essere giustificata dalla necessità di perseguire un interesse di rilevanza pubblica; è spesso arduo affermare che una specifica limitazione era indispensabile e che non vi erano altre strade percorribili per raggiungere l'obbiettivo prefissato, che spesso coincide con il mantenimento della sicurezza pubblica.
La raccolta dei dati personali dei migranti e la loro analisi vuole infatti impedire che soggetti suscettibili di arrecare una minaccia alla comunità nazionale oltrepassino i confini di uno Stato. L'Unione europea ha implementato a tal scopo diversi *database* che sono accessibili dalle forze di polizia in un'ottica di coordinazione degli interventi di controllo. L'utilizzo di simili archivi, pur giustificato da interessi pubblici, può però sollevare diversi quesiti. Il migrante non viene spesso reso edotto del fatto che i dati personali che lo riguardano vengono raccolti e catalogati, né ha contezza di quali soggetti sono effettivamente in grado di consultarli. Un'ulteriore riflessione ha come oggetto la finalità di detti archivi: quando può dirsi garantita la sicurezza del territorio statale dopo l'ingresso del migrante? Per quanto tempo quindi i dati che lo riguardano possono essere legittimamente conservati nei *database?* Un'effettiva accoglienza e integrazione del migrante nel tessuto nazionale non può dirsi raggiunta se questo viene catalogato e profilato *ad libitum* come tale.
In conclusione, il mantenimento della sicurezza interna e della salute pubblica non può giustificare un completo venir meno delle più elementari e basilari salvaguardie a tutela del diritto alla privacy e all'autonomia informativa dei migranti. Si auspica quindi un corretto intervento degli enti, sia pubblici che privati, impegnati quotidianamente nella gestione della crisi migratoria a far sì che i migranti siano correttamente informati dei diritti da loro vantati in merito dei propri dati personali e siano dotati dei mezzi necessari per farli valere. Gli archivi devono essere inoltre organizzati nella maniera più trasparente possibile, facendo in modo che ogni consultazione sia completamente tracciabile e identificabile in ogni suo elemento, dal soggetto che l'ha materialmente eseguita alle effettive finalità perseguite.

Processo penale "a distanza" e diritto alla privacy: possibili profili di contrasto*

Pietro Insolera - Stella Romano

Abstract

L'articolo analizza le novità normative emergenziali introdotte dal d.l. 17 aprile 2020, n. 18, convertito nella legge n. 27 del 24 aprile 2020, come modificato dal d.l. 30 aprile 2020, n. 28, inerenti alla disciplina del c.d. processo penale a distanza. Ci si sofferma sui potenziali profili di frizione con il diritto alla privacy, che, com'è noto, gode di un robusto statuto di garanzia tanto a livello costituzionale interno, quanto a livello eurounitario e convenzionale. Si svolge in particolare una critica dell'individuazione, a mezzo provvedimento amministrativo del DGSIA del Ministero della Giustizia, degli applicativi Teams e Skype for Business, che determina l'applicabilità del *Cloud Act* statunitense, con importanti conseguenze negative per il trattamento dei dati giudiziari. Si conclude sottolineando l'insufficienza delle modifiche da ultimo apportate con il provvedimento del DGSIA del 21 maggio 2020 a garantire il rispetto dei fondamentali principi posti a presidio della privacy nel sistema interno e sovranazionale.

The article analyzes the new emergency regulations introduced by Decree Law no. 18 of 17 April 2020, converted into Law no. 27 of 24 April 2020, as modified by Decree Law no. 28 of 30 April 2020, relating to the regulation of the so-called remote criminal trial. Focus is given to the potential violations of the right to privacy, which enjoys strong protection both under domestic constitutional principles, as well as under CFREU and ECHR provisions. In particular, it is developed a critical assessment of the identification, by means of an administrative provision of the DGSIA of the Ministry of Justice, of the Teams and Skype for Business applications, which determines the applicability of the US Cloud Act, with important negative consequences for the treatment of judicial data. The article ends by highlighting the insufficiency of the changes recently adopted with the DGSIA provision of 21 May 2020 to comply with the fundamental principles of privacy protection in the internal and supranational legal systems.

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

Sommario

1. Premessa. – 2. Il processo "a distanza" al vaglio del diritto costituzionale alla riservatezza. – 3. (*segue*) Spunti di diritto eurounitario sulla protezione dei dati personali. – 4. Il processo "a distanza" nel *focus* del diritto convenzionale. – 5. Conclusioni.

Keywords

pandemia - processo penale da remoto – privacy – Carta di Nizza – CEDU

1. Premessa

Diversi contributi si sono già concentrati sui molteplici profili di incostituzionalità che paiono inficiare le disposizioni di matrice emergenziale sul cd. processo penale a distanza[1], relativi in particolare al *vulnus* del diritto di difesa, del giusto processo e del diritto di riservatezza[2] .

Obiettivo di questo breve articolo è riprendere e approfondire alcune di quelle considerazioni, soffermandosi specialmente sulle potenziali frizioni con il diritto di privacy,

[1] La disciplina è costituita dall'art. 83, c. 12, 12-*bis*, 12-*ter*, 12-*quater*, 12-*quater.1*, 12-*quater.2* e 12-*quinquies*, del d.l. 18/2020, convertito nella l. 27/2020, come modificato dal d.l. 28/2020. In particolare, il Governo con l'art. 2, c. 7 del d.l. 11/2020, reiterato con d.l. 18/2020, all'art. 83, c. 12, ha esteso le limitate ipotesi di collegamento da remoto previste dall'art. 146 bis disp. att. c.p.p., e sino al 31 maggio p.v., a qualsiasi udienza, per tutte le persone detenute, internate o in stato di custodia cautelare con modalità da individuarsi tramite provvedimento del Direttore generale dei sistemi informativi e automatizzati del Ministero della giustizia. Con provvedimento del 10 marzo 2020 il DGSIA ha dato sintetica attuazione alla delega, prescrivendo per le udienze penali l'utilizzo degli strumenti già adottati per i collegamenti di cui all'art. 146 bis disp. att. c.p.p. a disposizione degli istituti penitenziari e degli uffici giudiziari; o, in alternativa, i programmi attualmente a disposizione dell'Amministrazione - cioè *Skype for Business* e *Teams* - previsti per il settore civile all'art. 2 del medesimo provvedimento. In seguito, il Governo ha posto al Senato la questione di fiducia sul proprio maxiemendamento al disegno di legge di conversione del d.l. 18/2020 in data 9 aprile 2020 alla Camera ed in data 22 aprile 2020 al Senato. In tal modo, con la conversione nella l. 27/2020 sono stati inseriti, dopo il c. 12, ulteriori commi volti ad estendere il sistema dei collegamenti da remoto ben oltre le originarie previsioni di cui ai due decreti legge citati, ovvero alla generalità dei casi, "normalizzando temporaneamente", per così dire, il processo da remoto, che diviene il regime processuale ordinario a prescindere dallo stato di detenzione dell'imputato sino al 30 giugno 2020 (c. 12-*bis*). Il collegamento da remoto resta comunque "possibile" anche nella fase delle indagini preliminari (c. 12-*quater*) per il compimento di specifiche attività; nonché come modalità per le deliberazioni collegiali in camera di consiglio di tutti gli organi giurisdizionali, Corte di Assise compresa (c. 12-*quinquies*) e della Corte di Cassazione (c. 12-*ter* che richiama il c 12-*quinquies*). Infine, si è previsto con d.l. 28/2020 che il giudice, nei casi di cui sopra, debba comunque trovarsi nell'ufficio giudiziario e che il consenso delle parti al processo da remoto è necessario per le "udienze di discussione finale, in pubblica udienza o in camera di consiglio e a quelle nelle quali devono essere esaminati testimoni, parti, consulenti o periti" (art. 3, c. 1, lett. *c)* e lett. *d)*). Insiste, inoltre, un pericolo di normalizzazione del processo da remoto, in quanto con un emendamento all'art. 83 proposto dal Governo, si vuole introdurre la possibilità, previo accordo tra le parti, che i processi da remoto sia nel penale che nel civile possano tenersi fino al 31 dicembre 2021.

[2] Cfr. *Appunti sulle possibili eccezioni di illegittimità costituzionale in ordine alla disciplina del processo da remoto*, con il contributo degli avv.ti Federico Baffi, Gaia Caneschi, Federico Febbo, Francesco Fratini, Ettore Grenci, Pietro Insolera, Ladislao Massari e Stella Romano; coordinamento a cura di V. Manes - I. Pellizzone, consultabile in *camerepenali.it*; v. anche, per tutti questi profili, le analoghe considerazioni sviluppate da V. Manes - L. Petrillo - G. Sacconi, *Processo penale da remoto: prime riflessioni sulla violazione dei principi di legalità costituzionale e convenzionale*, in *dirittodidifesa.eu*, 6 maggio 2020.

che – come noto – gode di robusta protezione tanto nel sistema costituzionale interno, quanto in quello sovranazionale (eurounitario e convenzionale)[3].

A tale scopo, occorre in primo luogo ripercorrere sinteticamente il contenuto delle disposizioni rilevanti del d.l. 18/2020, convertito nella l. 27/2020.

La disposizione di cui al comma 12-*bis* dell'art. 83 permette il collegamento da remoto, da individuarsi e regolarsi con provvedimento del direttore generale dei sistemi informativi e automatizzati del Ministero della Giustizia (d'ora innanzi: DGSIA), per lo svolgimento delle udienze penali, con l'eccezione delle udienze di discussione finale o delle udienze istruttorie.

La disposizione di cui al comma 12-*quater* dell'art. 83 autorizza il giudice o il pubblico ministero in fase di indagini preliminari ad avvalersi del collegamento da remoto, da individuarsi e regolarsi con provvedimento del DGSIA, per il compimento di atti di indagini preliminari, che richiedono la partecipazione della persona sottoposta alle indagini, della persona offesa, del difensore, di consulenti, di esperti o di altre persone, nei casi in cui la presenza fisica di costoro non può essere assicurata senza mettere a rischio le esigenze di contenimento della diffusione del virus Covid 19.

Il DGSIA ha dato sintetica attuazione alla delega ed all'art. 3 si prescrive per le udienze penali l'utilizzo degli strumenti già adottati per i collegamenti di cui all'art. 146 *bis* disp. att. c.p.p. a disposizione degli istituti penitenziari e degli uffici giudiziari; o, in alternativa, i programmi attualmente a disposizione dell'Amministrazione – cioè *Skype for Business* e *Teams* – previsti per il settore civile all'art. 2 del medesimo provvedimento.

Tali disposizioni paiono porsi in contrasto con i principi costituzionali ed europei in materia di diritto alla riservatezza e di protezione dei dati personali, nella parte in cui introducono il collegamento da remoto per lo svolgimento delle udienze penali, rimettendone il vaglio all'autorità procedente da remoto laddove, con riferimento alla fase delle indagini preliminari, l'individuazione dell'opportunità del collegamento da remoto viene affidata alla valutazione dell'autorità giudiziaria al ricorrere dell'unica ed esclusiva condizione che la presenza fisica non possa essere assicurata per le esigenze di contenimento della diffusione del virus COVID – 19, senza che entrambe le disposizioni contengano alcuna precisa e chiara specificazione in merito al trattamento dei dati personali, oggetto della trasmissione attraverso il collegamento virtuale.

Ciò appare di maggior rilievo, laddove i dati oggetto di trattamento dal sistema informatico utilizzato nel collegamento da remoto appartengono al possibile *status* di "indagato" o "imputato" nel procedimento penale (cd. dati giudiziari). D'altronde, il d.lgs. 51/ 2018[4] – completamente ignorato dal legislatore dell'emergenza – ha disposto la piena applicabilità della disciplina di protezione dati, anche ai trattamenti di dati svolti nell'esercizio della funzione giurisdizionale.

Con riguardo al costituzionalmente problematico utilizzo di provvedimenti amministrativi del DGSIA, occorre preliminarmente richiamare i profili di criticità sollevati

[3] Cfr. *Appunti sulle possibili eccezioni di illegittimità costituzionale*, cit., 6-10.

[4] Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (18G00080).

dai 21 quesiti di cui alla nota dell'Unione Camere Penali Italiane indirizzata al Garante per la protezione dei dati personali in data 14 aprile 2020[5], relativi ai plurimi punti di frizione dell'art. 83, c. 12-*bis* e 12-*quater*, d.l. 18/2020 con il d.lgs. 51/2018, in particolare laddove individuano i programmi commerciali *Skype for Business* e *Teams*, della società statunitense Microsoft Corporation, quali piattaforme per lo svolgimento del processo penale da remoto.

Come rilevato nella successiva lettera del Presidente del Garante per la protezione dei dati personali al Ministro della Giustizia il 16 aprile 2020[6], il trattamento dei dati personali pone seri problemi di compatibilità con la disciplina *ex* d.lgs. 51/2018, stante l'applicabilità del *Cloud Act* statunitense[7], che attribuisce alle autorità americane di contrasto un ampio potere acquisitivo di dati e informazioni.

Il Garante ha poi condiviso le ulteriori perplessità espresse dall'UCPI in merito alla «tipologia di dati eventualmente memorizzati da Microsoft Corporation per finalità proprie, del servizio o commerciali; sui soggetti legittimati all'accesso ai metadati delle sessioni e, in particolare, sull'eventualità che Microsoft Corporation o un amministratore di sistema possa desumere, dai metadati nella sua disponibilità, alcuni dati "giudiziari" particolarmente delicati quali, ad esempio, la condizione di soggetto sottoposto alle indagini o di imputato, magari *in vinculis*».

Il Garante ha osservato altresì che si tratta di temi sicuramente rilevantissimi e degni, pur nella condizione emergenziale che stiamo vivendo, della massima attenzione, al fine di coniugare esigenze di giustizia, tutela della salute e protezione dati.

Infine, il Garante ha rilevato criticamente che il Governo ha omesso di consultarsi preventivamente con la Sua Autorità, «passaggio tutt'altro che formale» per stabilire le adeguate opzioni di disciplina, tramite ragionevole contemperamento dei diversi interessi in gioco, in un settore così delicato.

2. Il processo "a distanza" al vaglio del diritto costituzionale alla riservatezza

Le disposizioni di cui all'art. 83, c. 12-*bis* e 12-*quater*, d.l. 18/2020 hanno l'obiettivo di consentire la prosecuzione dell'attività giudiziaria penale, volta ad accertare fatti di reato e responsabilità individuali per punire i responsabili secondo la legge e proteggere la sicurezza pubblica, garantendo al contempo adeguatamente, nel contesto di un'eccezionale crisi sanitaria causata dalla pandemia da Covid 19, la salute individuale degli operatori del diritto e la salute collettiva.

Appurato che si tratta di scopi legittimi, occorre verificare se il sacrificio dei diritti individuali – e, segnatamente, per quel che rileva, il diritto alla privacy, in specifica

[5] *Processo penale da remoto e protezione dei dati personali. L'Unione scrive al Garante*, 14 aprile 2021, consultabile in *camerepenali.it*.

[6] *Processo penale da remoto: lettera del Presidente del Garante per la protezione dei dati personali, Antonello Soro, al Ministro della Giustizia, Alfonso Bonafede*, 17 aprile 2021, doc. web n. 9316889, consultabile in *garanteprivacy.it*.

[7] The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943)

relazione alla raccolta, alla conservazione e al trattamento di alcuni dati "giudiziari" particolarmente delicati quali, ad esempio, la condizione di soggetto sottoposto alle indagini o di imputato, magari *in vinculis*, implicato dallo strumento normativo utilizzato – possa dirsi necessario e dunque proporzionato agli obiettivi, stante l'indisponibilità di misure meno invasive, ma egualmente adeguate allo scopo.

Con specifico riguardo all'individuazione del parametro costituzionale, si tratta del diritto alla riservatezza dell'individuo, che svolge la propria personalità anche in quel luogo virtuale rappresentato dal sistema informatico.

In tale prospettiva, la portata della "riservatezza informatica", da un lato, appare più estesa della dimensione originaria della privacy, e, da un altro lato, è espressione del riconoscimento dei diritti dell'individuo in quanto partecipe della comunità virtuale[8].

Sul piano del fondamento costituzionale, il diritto alla riservatezza dei dati personali è manifestazione del diritto fondamentale all'intangibilità della sfera privata (Corte cost., 23 luglio 1991, n. 366), che attiene alla tutela della vita degli individui nei suoi molteplici aspetti. Un diritto che trova riferimenti nella Costituzione italiana, già riconosciuto, in relazione a molteplici ambiti di disciplina, nella giurisprudenza della Corte costituzionale (Corte cost., 21 febbraio 2019, n. 20; 11 giugno 2009, n. 173; 14 novembre 2006, n. 372; 24 aprile 2002, n. 135; 11 marzo 1993, n. 81; 23 luglio 1991, n. 366;26 giugno 1969, n. 104; 26 giugno 1970, n. 112; 6 aprile 1973, n. 34; 12 aprile 1973, n. 38; 5 febbraio 1975, n. 20)[9].

Dato costante nella giurisprudenza costituzionale sopra richiamata è, inoltre, l'esigenza che la riservatezza, in tutte le sue specifiche declinazioni e variegati contenuti di protezione, sia oggetto di un ragionevole bilanciamento complessivo in sede legislativa con gli altri valori e interessi rilevanti (v. spec. Corte cost., 24 febbraio 1994, n. 63; 14 novembre 2006, n. 372, *mutatis mutandis* v. soprattutto la nota Corte cost., 9 maggio 2013, n. 85[10]), ed in particolare con l'istanza di repressione dei fenomeni criminosi.

Invero, se con riferimento alla conservazione tradizionale dei dati giudiziari, la Corte costituzionale nella sentenza n. 173/2009*,* qualificando come fondamentale il diritto

---

[8] V. De Rosa, *La formazione di regole giuridiche per il* cyberspazio, in *Il diritto dell'informazione e dell'informatica*, 2003, 2, 377.

[9] Cfr. l'ampia disamina dell'evoluzione giurisprudenziale e dottrinaria di M. Luciani, *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato*, in astrid-online.it , 4 ottobre 2018.

[10] «Tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile pertanto individuare uno di essi che abbia la prevalenza assoluta sugli altri. La tutela deve essere sempre «sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro» (sentenza n. 264/2012). Se così non fosse, si verificherebbe l'illimitata espansione di uno dei diritti, che diverrebbe "tiranno" nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della persona. […] «La Costituzione italiana, come le altre Costituzioni democratiche e pluraliste contemporanee, richiede un continuo e vicendevole bilanciamento tra princìpi e diritti fondamentali, senza pretese di assolutezza per nessuno di essi. La qualificazione come "primari" dei valori dell'ambiente e della salute significa pertanto che gli stessi non possono essere sacrificati ad altri interessi, ancorché costituzionalmente tutelati, non già che gli stessi siano posti alla sommità di un ordine gerarchico assoluto. Il punto di equilibrio, proprio perché dinamico e non prefissato in anticipo, deve essere valutato – dal legislatore nella statuizione delle norme e dal giudice delle leggi in sede di controllo – secondo criteri di proporzionalità e di ragionevolezza, tali da non consentire un sacrificio del loro nucleo essenziale». Cfr. in dottrina: M. Cartabia, *Ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, in A. Giorgis - E. Grosso – J. Luther, *Il costituzionalista riluttante. Scritti per Gustavo Zagrebelsky*, Torino, 2016, 463 ss.

alla riservatezza e riconoscendogli altresì pari dignità di tutela rispetto al diritto inviolabile alla riservatezza della corrispondenza, aveva affermato che «non è garantita, nelle condizioni normative ed organizzative attuali, una adeguata tenuta della segretezza degli atti custoditi negli uffici giudiziari, come purtroppo dimostrano le frequenti 'fughe' di notizie e documenti», la presente normativa presenta un importante *vulnus* nella misura in cui non specifica precise modalità atte a garantire la riservatezza e l'integrità dei sistemi di collegamento da remoto e rinviando alla fonte amministrativa per la loro concreta operatività.
Il legislatore, nelle disposizioni censurate, ha infatti fatto prevalere irragionevolmente le esigenze di tutela della salute e di repressione dei reati a discapito della riservatezza degli indagati/imputati.
Ciò è manifestato plasticamente dal fatto che si sia delegato a una fonte amministrativa, il provvedimento della DGSIA, il compito di "individuare e regolamentare i collegamenti" necessari a consentire lo svolgimento delle udienze da remoto in modo da «garantire il contraddittorio e l'effettiva partecipazione delle parti» (12-*bis*), o, in fase di indagini preliminari, affidandone la valutazione all'autorità procedente nei casi in cui la presenza fisica «non può essere assicurata senza mettere a rischio le esigenze di contenimento della diffusione del virus COVID-19» (12-*quater*), omettendosi ogni previo confronto con il Garante per la protezione dei dati personali, in una materia di sua esclusiva competenza.
Emergono dunque dall'*iter legis* una insufficiente ponderazione degli interessi in gioco e una mancata valutazione – anche attraverso indagini empiriche, approfondimenti tecnici, valutazioni di impatto – di strumenti alternativi meno invasivi per i diritti individuali ma comunque idonei a perseguire lo scopo, tali da risolversi in un eccessivo sacrificio dei diritti di riservatezza.

3. (*segue*) Spunti di diritto eurounitario sulla protezione dei dati personali

Il diritto alla protezione dei dati personali è attratto al livello dell'ordinamento dell'Ue, dove non solo riceve un articolato riconoscimento nel catalogo dei diritti fondamentali (art. 8 Carta di Nizza) e nelle fonti di diritto primario (art. 16 TFUE), ma trova anche compiuta disciplina mediante una fonte secondaria idonea a realizzare il livello massimo di armonizzazione della legislazione degli Stati membri, di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016.
Peraltro, proprio in materia di diritto alla protezione dei dati personali, la Corte costituzionale con sentenza n. 20/2019 ha stabilito che «i principi e i diritti enunciati nella CDFUE intersecano in larga misura i principi e i diritti garantiti dalla Costituzione italiana (e dalle altre Costituzioni nazionali degli Stati membri), e che la prima costituisce pertanto 'parte del diritto dell'Unione dotata di caratteri peculiari in ragione del suo contenuto di impronta tipicamente costituzionale'», derivandone che «va preservata l'opportunità di un intervento con effetti erga omnes di questa Corte, in virtù del principio che situa il sindacato accentrato di legittimità costituzionale a fondamento

dell'architettura costituzionale (art. 134 Cost.), precisando che, in tali fattispecie, la Corte costituzionale giudicherà alla luce dei parametri costituzionali interni, ed eventualmente anche di quelli europei (*ex* artt. 11 e 117, primo comma, Cost.), comunque secondo l'ordine che di volta in volta risulti maggiormente appropriato».

I principi che devono governare il trattamento sono sanciti nell'art. 5, c. 1, del citato regolamento e, tra di essi, assumono particolare rilievo quelli che consistono: nella limitazione della finalità del trattamento (lettera b) e nella "minimizzazione dei dati", che si traduce nella necessità di acquisizione di dati adeguati, pertinenti e limitati a quanto strettamente necessario alla finalità del trattamento (lettera c).

Ancora, un riferimento al necessario bilanciamento tra diritti si trova nelle premesse al regolamento 2016/679/UE (considerando 4), ove si legge che «[i]l diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità». Tale corollario normativo non rappresenta altro che il precipitato dell'art. 52, par. 1, della Carta di Nizza, che riconosce, pertanto, che possono essere apportate limitazioni all'esercizio di diritti come quelli sanciti dagli artt. 7 e 8 della medesima, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e libertà, nel rispetto del principio di proporzionalità.

In definitiva, la disciplina europea, pur riconoscendo un ampio margine di regolazione autonoma e di dettaglio agli Stati membri con riguardo a certe tipologie di trattamento (in specie con riferimento alla tutela della salute pubblica: art. 32 Cost. ed art. 35 della Carta di Nizza), impone loro il principio di proporzionalità del trattamento che, rappresenta il fulcro della giurisprudenza della Corte di giustizia dell'Unione europea in materia[11].

In particolare, occorre rimarcare le criticità poste dalla normativa applicabile alle piattaforme individuate, su delega dell'art. 83, d.l. 18/2020, con provvedimenti amministrativi della DSGIA, *Microsoft Teams* e *Skype for Business*, il *Cloud Act*, che consente alle autorità statunitensi, forze dell'ordine e agenzie di *intelligence*, di acquisire dati informatici dagli operatori di servizi di *cloud computing* «*regardless of whether such communications, record or other informations is located within or outside of USA*», ossia indipendentemente dal fatto che tali comunicazioni, registrazioni o altre informazioni si trovino all'interno o all'esterno degli Stati Uniti.

Gli *Internet Service Provider*, interessati dalla misura, sono le compagnie private sottoposte alla giurisdizione degli Stati Uniti ovvero le società costituite negli Stati Uniti e le loro filiali all'estero (per quel che qui rileva, la Microsoft Corporation), ma anche le società europee che hanno una filiale negli Stati Uniti o che operano nel mercato americano. Per quanto riguarda i dati richiesti e la natura della misura, quest'ultima è considerata una misura nazionale e le autorità statunitensi devono rispettare rigorosamente le tutele legislative e costituzionali proprie degli Stati Uniti: a seconda dei casi mandato, ordinanza o ordine di esibizione amministrativo[12].

---

[11] CGUE, cause riunite C-465/00, C-138/01 e C-139/01, *Österreichischer Rundfunk e altri* (2003) e cause riunite C-92/09 e 93/09, *Volker und Markus Schecke e Eifert* (2010).

[12] Cfr. B. Calderini, *Cloud act, la norma USA che fa a pugni con la privacy europea: i nodi*, all'URL, in

La disciplina statunitense relativa al trattamento dei dati personali applicabile alle piattaforme individuate dal DGSIA *Microsoft Teams* e *Skype for Business* è stata criticata in questi termini dal Consiglio degli Ordini Forensi d'Europa: «La legge CLOUD è in conflitto con i diritti umani fondamentali, poiché non fornisce gli standard minimi stabiliti dalle corti europee per limitare la sorveglianza elettronica da parte del governo. Secondo la giurisprudenza della Corte europea dei diritti dell'uomo e della Corte di giustizia europea, qualsiasi interferenza con il diritto alla privacy deve essere conforme alla legge, per uno scopo legittimo e limitato a ciò che è necessario in una società democratica»[13].

Si porrebbero, dunque, profili rilevanti di limitazione del nucleo essenziale del diritto alla riservatezza, con riferimento al trattamento dei dati giudiziari all'interno di circuiti, posti al di fuori dal controllo di soggetti terzi ed indipendenti, come, invece, richiesto dalla normativa derivata europea[14], passibili altresì di accessi occulti ed in maniera generalizzata, oltre il limite della stretta necessità, pregiudicando l'integrità e la sicurezza dei dati stessi.

In conclusione, può affermarsi che, alla luce di questi principi, le disposizioni di cui all'art. 83, c. 12-*bis* e 12-*quater,* laddove individuano tramite delega alla DSGIA gli applicativi della Microsoft Corporations *Microsoft Teams* e *Skype for Business*, assoggettati all'applicazione del *Cloud Act*, espongono ad un pericolo di lesione eccessivo i cd. dati giudiziari di indagati ed imputati, senza rispettare – come visto sopra – gli standard di protezione minima garantiti dalle disposizioni interne ed europee.

L'ampio potere di acquisizione, archiviazione, trattamento delle autorità governative statunitensi può comportare peraltro – osserviamo infine – ulteriori pregiudizi. Si pensi, ad esempio, al soggetto sottoposto a procedimento penale celebrato da remoto, conclusosi con pronuncia di proscioglimento, che si veda poi rigettata la domanda per ottenere il visto di lavoro o di studio negli USA, a causa di dati giudiziari illegittimamente acquisiti e magari conservati oltre un certo limite temporale, in violazione del diritto all'oblio[15].

Parimenti dubbia la compatibilità con l'art. 48 del Regolamento Generale sulla Protezione dei Dati (regolamento (UE) 2016/679) sul trasferimento di dati personali verso

agendadigitale.eu, 11 giugno 2019. La normativa, emanata per semplificare le attività di indagine penali transfrontaliere superando il precedente sistema MLAT, è stata sottoposta a numerose critiche anche negli USA: cfr. ad es. N.S. Giuliani, *The Cloud Act is a Dangerous Piece of Legislation*, in *aclu.org*, 13 marzo 2018; in dottrina, v. ad es. S. Biligic, *Something Old, Something New, and Something Moot: The Privacy Crisis Under the Cloud Act*, in *Harvard Journal of Law & Technology*, 32(1), 2018, 321 ss., spec. 347 ss.

[13] Cfr. *CCBE Assessment of the U.S. Cloud Act,* 28 febbraio 2019, consultabile in *ccbe.eu*. Per una valutazione meno critica, cfr. O. Pollicino - M. Bassini, *La proposta di Regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, in *medialaws.eu*, 26 ottobre 2018, spec. § 2.

[14] L'art. 10 del GDPR prevede che «il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica».

[15] In tale situazione, potrebbero prospettarsi ulteriori profili di contrasto con l'art. 117, c. 1, Cost., in relazione agli artt. 14 e 2, Prot. n. 4, CEDU.

Paesi terzi[16].

A tale riguardo, viene in rilievo quanto statuito dalla Corte di giustizia dell'Unione europea nella causa *Schrems* del 6 ottobre 2015[17] che riguardava la tutela delle persone fisiche con riguardo al trasferimento dei loro dati personali verso paesi terzi, nella fattispecie, gli Stati Uniti.

I trasferimenti di dati verso gli Stati Uniti si basavano su una decisione di adeguatezza adottata dalla Commissione nel 2000, che all'epoca consentiva trasferimenti verso le società statunitensi che autocertificavano la protezione da parte loro dei dati personali trasferiti dall'UE e il rispetto dei cosiddetti "principi di approdo sicuro" (c.d. *Safe Harbour*). Quando la causa è stata portata dinanzi alla CGUE, quest'ultima ha esaminato la validità della decisione della Commissione alla luce della Carta ricordando che la protezione dei diritti fondamentali nell'UE richiede che le deroghe e le restrizioni a tali diritti operino solo entro i limiti dello stretto necessario. La CGUE ha ritenuto che una normativa che consenta alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche «pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta».

Il diritto sarebbe svuotato di significato qualora i pubblici poteri statunitensi fossero autorizzati ad accedere alle comunicazioni su base casuale, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente individuati.

Da ultimo occorre sinteticamente rilevare che, sebbene la nuova Decisione della Commissione europea di adeguatezza riguardo al trasferimento dei dati dall'UE agli U.S.A. del 12 luglio 2016, c.d. *Privacy Shield*[18], abbia in parte sanato alcune delle gravi carenze censurate dalla Corte di giustizia nella sentenza *Schrems*, allo stato permangono diversi profili di dubbia compatibilità, in relazione al potere ancora molto invasivo delle autorità statunitensi, difficilmente in grado di assicurare un livello di protezione dei dati adeguato e sostanzialmente equivalente a quello predisposto dal sistema normativo dell'UE[19].

---

[16] Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.

[17] CGUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* [GC] (2015).

[18] Cfr. la scheda "Privacy Shield" del Garante privacy, 26 luglio 2016, doc. web n. 5306161, al sito *garanteprivacy.it*

[19] Per considerazioni più diffuse sul punto, cfr. senza pretesa di completezza: S. Crespi, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, 3, 2016, 687 ss., spec. 710 ss.; R. Ferraro, *Lo EU-U.S.* Privacy Shield. *Una risposta insufficiente alle richieste della Corte di giustizia dell'Unione europea nella sentenza* Safe Harbour*?*, in *Diritto del commercio internazionale*, 3, 2017, 635 ss.

4. Il processo "a distanza" nel *focus* del diritto convenzionale

Il diritto alla riservatezza trova tutela nell'art. 8 della Convenzione europea dei diritti dell'uomo che dispone: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».
Ai sensi del paragrafo 2 le ingerenze dell'autorità sono legittime in presenza di tre requisiti: 1) una previsione legislativa, rispetto alla quale la giurisprudenza europea accentua il riferimento all'accessibilità e alla conoscibilità delle fonti normative e della giurisprudenza, essendo necessario che il cittadino possa ragionevolmente prevedere le conseguenze delle proprie azioni; 2) il perseguimento di una delle finalità legittime previste tassativamente dalla norma con riferimento sia a molteplici interessi dello Stato e della collettività, sia alla tutela dei diritti e delle libertà altrui; 3) la necessità della misura in una società democratica per il conseguimento degli obiettivi sopra indicati. In questa ultima prospettiva della "necessità" si inserisce il criterio della proporzionalità tra ingerenza e finalità legittima perseguita.
Le considerazioni dianzi svolte consentono di apprezzare un primo profilo di possibile contrasto dell'art. 83, c. 12-*bis* e 12-*quater*, cit. con l'art. 117, c. 1, Cost., in relazione all'art. 8 CEDU. L'art. 8, par. 2, Convenzione EDU, dispone che non può esservi ingerenza di una autorità pubblica nell'esercizio del diritto alla vita privata a meno che tale ingerenza sia prevista dalla legge.
La Corte di Strasburgo[20] ha statuito che tale previsione non si limita a richiedere la conformità con la normativa nazionale – più che dubbia, come si è visto, nel caso di specie – ma riguarda anche la qualità della legge, richiedendo che sia compatibile con la *rule of law*. Si è così affermato che la disposizione nazionale deve essere chiara, prevedibile e adeguatamente accessibile[21]. Essa dev'essere sufficientemente prevedibile, così da mettere nelle condizioni gli individui di agire in conformità alla legge[22], e deve tracciare chiaramente i confini della portata della discrezionalità di cui godono le pubbliche autorità. Per esempio, come la Corte ha illustrato nel contesto della sorveglianza, la legge deve essere sufficientemente chiara nella sua formulazione testuale da fornire ai cittadini una indicazione adeguata circa le condizioni e circostanze in cui le autorità hanno il potere di ricorrere a qualsivoglia misura di sorveglianza segreta e

[20] I riferimenti del *case law* convenzionale d'ora innanzi citati sono traduzioni di passaggi tratti dai *Reports: Guide on Article 8 of the European Convention on Human Rights* e *Factsheet – Personal data protection*, entrambi disponibili all'URL *echr.coe.int*.

[21] CEDU, *Amann c. Svizzera* [GC], ric. 27798/95 (2000), § 56; cfr. anche *Malone c. Regno Unito*, ric. 8691/79 (1984), § 66; *Silver e a. c. Regno Unito*, ricc. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75(1983), § 88).

[22] CEDU, *Amann c. Svizzera,* cit., § 50; cfr. anche *Kopp c. Svizzera*, ric. 23224/94 (1998).

raccolta di dati personali[23]. Si è altresì statuito che il requisito della chiarezza si applica alla portata della discrezionalità esercitata dalle pubbliche autorità. La norma nazionale deve indicare con ragionevole chiarezza la portata e il modo dell'esercizio della discrezionalità rilevante conferita alle pubbliche autorità, in modo tale da assicurare agli individui un grado minimo di protezione al quale loro hanno il diritto in forza della *rule of law* in una società democratica[24].

Per quanto attiene al diritto alla protezione dei dati, nella causa *Rotaru c. Romania*, la Corte EDU ha rilevato che la legge nazionale autorizzava la raccolta, la registrazione e l'archiviazione in fascicoli segreti di informazioni rilevanti per la sicurezza nazionale, ma non stabiliva limiti all'esercizio di tali poteri, che rimanevano *a discrezione delle autorità*. Il diritto nazionale non definiva, per esempio, il tipo d'informazioni che avrebbero potuto essere trattate, le categorie di persone nei cui confronti si sarebbero potute adottare misure di sorveglianza, le circostanze in cui tali misure si sarebbero potute prendere o la procedura da seguire. La Corte di Strasburgo ha pertanto concluso che il diritto nazionale non rispettava il requisito di prevedibilità ai sensi dell'art. 8 della CEDU[25].

Ancora, la causa *Vukota-Bojić c. Svizzera* riguardava la sorveglianza segreta di una richiedente un'assicurazione sociale, da parte di *investigatori privati commissionati* dalla sua compagnia di assicurazione. La Corte EDU ha ritenuto che, sebbene la misura di sorveglianza oggetto del ricorso fosse stata ordinata da una compagnia di assicurazione privata, a tale società era stato riconosciuto dallo Stato il diritto di erogare prestazioni rientranti nell'assicurazione medica obbligatoria e di riscuotere premi assicurativi. I giudici di Strasburgo hanno, in particolar modo, statuito che uno Stato non può esonerare sé stesso dalle responsabilità previste dalla Convenzione, delegando i propri obblighi a enti privati o persone fisiche. Affinché l'ingerenza potesse essere "conforme alla legge", il diritto nazionale avrebbe dovuto fornire garanzie sufficienti contro l'abuso per ingerenza nei diritti di cui all'articolo 8 della CEDU. Nel caso in esame, la Corte EDU ha concluso che vi era stata violazione dell'articolo 8 della CEDU, in quanto il diritto nazionale non aveva indicato con sufficiente chiarezza la portata e le modalità dell'esercizio del potere discrezionale di esercitare una sorveglianza segreta su una persona assicurata, accordato a compagnie di assicurazione che agiscono in qualità di autorità pubbliche nelle controversie in materia[26].

Ebbene, se il requisito di *lawfulness* è ricostruito in termini così stringenti nella giurisprudenza convenzionale, che richiede vi siano salvaguardie idonee ad assicurare i diritti individuali protetti dall'art. 8, non può che escludersi che la norma censurata sia in grado di soddisfare tale standard di garanzia.

Come si è già detto, infatti, il contrasto con il principio di legalità processuale è aggra-

[23] CEDU, *Shimovolos c. Russia*, ric. 30194/09 (2011), § 68.

[24] CEDU, *Piechowicz c. Polonia,* ric. 20071/07 (2012), § 212.

[25] CEDU, *Rotaru c. Romania* [GC], ric. 28341/95 (2000), § 57; cfr. anche *Association for European Integration and Human Rights e Ekimdzhiev c. Bulgaria*, ric. 62540/00 (2007); *Shimovolos c. Russia*, ric. 30194/09 (2011); e *Vetter c. Francia*, ric. 59842/00 (2005).

[26] CEDU, *Taylor-Sabori c. Regno Unito*, ric. 47114/99 (2002) § 48; *Vukota-Bojić c. Svizzera*, ric. 61838/10 (2016), § 77.

vato dall'ampiezza del margine di intervento concesso al menzionato provvedimento del DSGIA, per la disciplina dei collegamenti da remoto; consegnando parallelamente al giudice un compito altrettanto generico ed indeterminato, ossia quello di assicurare che lo svolgimento dell'udienza avvenga «con modalità idonee a salvaguardare il contraddittorio e l'effettiva partecipazione delle parti»: così rimettendo alla discrezionale ed insindacabile valutazione del giudice (il gravoso onere di garantire) aspetti essenziali e fondamentali delle garanzie previste dagli artt. 24 e 111 Cost., con una latitudine valutativa difficilmente compatibile con quando la stessa Corte costituzionale ha stabilito ripudiando apertamente – nell'ordinanza n. 24/2017 – l'idea del "giudice di scopo", ritenuta incompatibile con la stessa soggezione del giudice alla legge (art. 101, c. 2, Cost.).

Siffatto *vulnus* al principio di legalità, sotto il profilo dell'eccesso di discrezionalità, tale da sfociare in arbitrio, compromette anche il requisito di *lawfulness* della misura che interferisce sul diritto alla riservatezza, per quanto concerne il trattamento dei dati personali, affidato, attraverso un provvedimento amministrativo, a una società commerciale di diritto statunitense assoggettata all'applicabilità di una normativa, il *Cloud Act* statunitense, sulla cui effettiva idoneità a preservare la riservatezza dei dati giudiziari è ragionevole nutrire più di un dubbio.

Se si ritenesse l'art. 83, c. 12-*bis* e 12-*quater*, d.l. 18/2020 conforme al requisito di *lawfulness*, occorrerebbe comunque verificarne la legittimità costituzionale rispetto all'art. 117, c. 1, Cost. in rapporto all'art. 8, c. 2, CEDU, ove impone che la misura che interferisce sul diritto alla vita privata, in una società democratica, sia necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Sotto questo profilo, non vi è dubbio che gli scopi perseguiti dalla disposizione censurata, che intende consentire la prosecuzione dell'attività giudiziaria penale in condizioni di sicurezza durante una grave emergenza sanitaria pandemica (e dunque: pubblica sicurezza, difesa dell'ordine e prevenzione dei reati, protezione della salute, protezione dei diritti e delle libertà altrui, tutti da ritenersi "*pressing social needs*"), siano legittimi.

Occorre però valutare se la misura adottata risulti proporzionata rispetto ai suddetti scopi.

In particolare, è necessario stabilire se il significativo sacrificio dei cd. dati giudiziari determinato dall'individuazione delle piattaforme *Microsoft Teams* e *Skype for Business* con provvedimento amministrativo da parte della DSGIA e dalla conseguente applicabilità del *Cloud Act* è necessario, ovvero se, al contrario, era possibile perseguire l'obiettivo di assicurare la prosecuzione dell'attività giudiziaria penale in condizioni di sicurezza durante una grave emergenza sanitaria pandemica con la stessa efficacia attraverso strumenti meno afflittivi per il diritto di riservatezza, sotto il peculiare profilo della conservazione e del trattamento dei dati giudiziari dell'indagato/imputato.

A tale proposito, le stesse caratteristiche della procedura legislativa d'urgenza e l'omessa consultazione del Garante per la protezione dei dati personali indicano come non siano state valutate con sufficiente ponderazione/attenzione modalità alternative più adeguate a salvaguardare i dati giudiziari, inevitabilmente disvelati nell'ambito dell'at-

tività processuale penale.

Una più approfondita analisi tecnica, empirica e di impatto, pur nei limiti delle possibilità concesse da un assai complicato contesto emergenziale, avrebbe permesso al legislatore di selezionare più ragionevolmente piattaforme per lo svolgimento delle udienze penali meno rischiose per la privacy[27].

Insomma, l'*iter legis* conferma un inadeguato e irrazionale bilanciamento tra i valori in gioco, a tutto detrimento della protezione dei cd. dati giudiziari, tale da produrre una misura che interferisce sul piano sostanziale eccessivamente nel diritto alla vita privata.

D'altra parte, nel *case law* della Corte EDU emerge che, per determinare la proporzionalità generale di una misura, la Corte valuta in primo luogo le scelte legislative che ne stanno alla base. La qualità del controllo parlamentare sulla effettiva necessità della misura è di particolare importanza sotto questo profilo[28].

Ed invero, la Corte europea, proprio nel settore di nostro interesse, inerente al c.d. "*storage and use of personal data*" nell'amministrazione della giustizia penale, è intervenuta a più riprese accertando la violazione dell'art. 8 da parte di misure statuali viziate da sproporzione rispetto a scopi legittimi.

Nella sentenza *S. and Marper c. Regno Unito*[29], la Corte afferma in termini generali che «La protezione dei dati personali è di fondamentale importanza affinché la persona possa godere del suo diritto al rispetto della vita privata e familiare, garantito dall'articolo 8. Il diritto nazionale deve accordare salvaguardie appropriate per impedire qualsivoglia uso dei dati personali che possa essere incoerente con le garanzie di questo articolo […] la necessità di tali garanzie è ancora più forte laddove è in gioco la protezione di dati personali sottoposti a procedure di trattamento automatico, non ultimo quando tali dati sono utilizzati per scopi di polizia. La normativa interna dovrebbe specialmente assicurare che tali dati siano rilevanti e non eccessivi in rapporto agli scopi per cui sono archiviati; e conservati in una forma che permetta l'identificazione dei titolari dei dati non oltre il tempo necessario rispetto allo scopo per il quale i dati sono archiviati [...] Essa deve accordare anche adeguate garanzie sul fatto che i dati conservati sono stati efficacemente protetti da un utilizzo erroneo e dall'abuso»[30].

---

[27] Si sarebbe potuto trarre spunto, ad esempio, dall'esperienza del cd. Processo Civile Telematico, oppure collocare i collegamenti da remoto per lo svolgimento delle udienze penali nella Rete Unica Giustizia (c.d. R.U.G.), e non nella rete internet pubblica, ove i dati giudiziari sono ben più facilmente intercettabili; ovvero, infine, si sarebbero potute scegliere altre piattaforme gestite da *software* italiani, come *iorestoacasa.work*, consorzio che fornisce attualmente la dorsale internet al CNR e alle Università italiane, in grado di garantire standard di protezione ben più elevati. Cfr. ad es. P. Dimalio, *I processi targati Microsoft: arriva la spia in tribunale?*, in *Il Fatto Quotidiano*, 27 aprile 2020.

[28] Cfr. CEDU, *Animal Defenders International c. Regno Unito* [GC], ric. 48876/08 (2013) § 108.

[29] CEDU, ric. 30562/04 (2008), § 103.

[30] Il caso *S. and Marper* riguardava la conservazione a tempo indefinito in un archivio delle impronte digitali, dei campioni cellulari e dei profili di DNA dei ricorrenti dopo che un procedimento penale nei loro confronti era terminato con una assoluzione in un caso e sospeso nell'altro. La Corte ha accertato una violazione dell'art. 8, ritenendo che la conservazione in questione aveva integrato un'interferenza sproporzionata nell'esercizio del diritto dei ricorrenti al rispetto della vita privata e non poteva essere considerata necessaria in una società democratica. La Corte ha ritenuto in particolare che l'utilizzo di moderne tecniche scientifiche nel sistema di giustizia penale non poteva essere consentito ad ogni costo e senza bilanciare accuratamente i potenziali benefici dell'uso estensivo di tali tecniche a fronte di importanti interessi riconducibili alla riservatezza. Ogni Stato Contraente che rivendica un ruolo

Nel caso *M.M. c. Regno Unito* del 13 novembre 2012[31], la Corte ha dichiarato che vi era stata una violazione dell'articolo 8 della Convenzione, in quanto non erano state approntate sufficienti garanzie nel sistema per la conservazione e la rivelazione dei dati del casellario giudiziario al fine di garantire che i dati relativi alla vita privata del richiedente non fossero divulgati in violazione del suo diritto al rispetto della vita privata. La Corte ha osservato in particolare che, sebbene i dati contenuti nel casellario giudiziale fossero, in un certo senso, informazioni pubbliche, la loro sistematica memorizzazione nei registri centrali significava che erano disponibili per la rivelazione molto tempo dopo l'evento quando probabilmente tutti gli altri, tranne la persona interessata, se ne sarebbero dimenticati, specialmente laddove, come nel caso del richiedente, l'ammonimento si era verificata in privato.

Nel caso *Brunet c. Francia* del 18 settembre 2014[32]**,** il ricorrente si è lamentato in particolare di un'interferenza con la sua vita privata a seguito dell'aggiunta al database di polizia STIC (sistema per l'elaborazione dei reati registrati) - contenente informazioni da rapporti di indagine, elencando le persone coinvolte e le vittime - dopo l'interruzione del procedimento penale a suo carico. La Corte ha ritenuto che vi fosse stata una violazione dell'articolo 8 della Convenzione, rilevando che lo Stato francese aveva oltrepassato il suo potere discrezionale di decidere ("margine di apprezzamento") su tali questioni: la conservazione poteva essere considerata una violazione sproporzionata del diritto della ricorrente al rispetto della sua vita privata. La Corte ha ritenuto in particolare che il ricorrente non avesse avuto una reale possibilità di chiedere la cancellazione dalla banca dati delle informazioni che lo riguardavano e che la durata della conservazione di tali dati, 20 anni, potesse essere assimilata, se non alla conservazione a tempo indefinito, a quanto avveniva di regola piuttosto che a un limite massimo.

Infine, nel caso *Gaughran c. Regno Unito* del 13 febbraio 2020[33], riguardante una denuncia della conservazione indefinita di dati personali (profilo del DNA, impronte digitali e fotografie), la Corte ha ritenuto che vi fosse stata una violazione dell'articolo 8 della Convenzione, constatando che il Regno Unito aveva superato il margine di apprezzamento accettabile e che la conservazione in questione costituiva un'interferenza sproporzionata con il diritto del richiedente al rispetto della vita privata, che non poteva essere considerato necessario in una società democratica.

---

di pioniere nello sviluppo di nuove tecnologie ha una speciale responsabilità di "trovare il giusto compromesso". La Corte ha concluso che la natura totale e indiscriminata dei poteri di conservazione delle impronte digitali, dei campioni cellulari e dei profili di DNA di persone sospettate ma non condannate per i reati, così come applicata nel caso di specie, non era riuscita a bilanciare adeguatamente gli interessi pubblici e privati contrapposti.

[31] CEDU, ric. 24029/07 (2012). Nel 2000 la ricorrente era stata arrestata dalla polizia dopo essere scomparsa per un giorno con suo nipote nel tentativo di impedire la sua partenza in Australia a seguito della rottura del matrimonio di suo figlio. Le autorità hanno deciso di non procedere penalmente e lei è stata invece ammonita per rapimento di minori. La misura di ammonimento inizialmente era destinata a rimanere nel suo registro per cinque anni, ma a causa di un cambio di politica nei casi in cui la parte lesa fosse una bambina, quel periodo è stato successivamente esteso alla vita. La ricorrente si è lamentata della conservazione a tempo indeterminato e della divulgazione del suo ammonimento e dell'impatto di ciò sulle sue prospettive di impiego.

[32] CEDU, ric. 21010/10.

[33] CEDU, ric. 45245/15.

La Corte ha sottolineato in particolare che non era stata la durata della conservazione dei dati a essere stata determinante, ma l'assenza di alcune garanzie. Nel caso del richiedente, i suoi dati personali erano stati conservati a tempo indeterminato senza tener conto della gravità del suo reato, della necessità di una conservazione indefinita e senza alcuna reale possibilità di revisione. Notando anche che la tecnologia utilizzata si è dimostrata più sofisticata di quella considerata dai tribunali nazionali in questo caso, in particolare per quanto riguarda la conservazione e l'analisi delle fotografie, la Corte ha ritenuto che la conservazione dei dati del richiedente non fosse riuscita a trovare un giusto equilibrio tra gli interessi pubblici e privati concorrenti.
Pur con le dovute differenze, può ricavarsi un principio comune e unificante da queste pronunce: esse impongono un rapporto di ragionevole proporzionalità tra la misura della pubblica autorità di conservazione e trattamento dei dati giudiziari, l'impatto che essa determina sulla ampia sfera di vita privata della persona, e gli scopi legittimi perseguiti.

5. Conclusioni

In ultima analisi, si può affermare come il diritto alla riservatezza sia riconosciuto e tutelato dagli artt. 2, 14, 15 Cost., 8 CEDU, 7 e 8 e 52 CDFUE, dai quali si trae un modello di garanzie pari a quello delineato dallo statuto costituzionale interno con riferimento ai diritti di libertà classici: i diritti fondamentali possono essere limitati soltanto nel rispetto di una riserva di legge chiara ed accessibile e di un atto motivato dell'autorità giudiziaria, alla luce del principio di proporzionalità.
Ognuno vede come la normativa in esame, per tutte le ragioni sopra ampiamente svolte, non preveda le garanzie richieste dalla normativa costituzionale ed europea: ossia regole chiare e dettagliate, non dotate peraltro dei requisiti di sufficiente accessibilità e precisione in ordine al trattamento dei dati giudiziari oggetto del collegamento da remoto, affidando di volta in volta all'autorità procedente la scelta di procedere da remoto.
Inoltre, la normativa in esame, dettata sull'onda dell'emergenza, non ha previsto alcuna altra specificazione in ordine alle procedure da seguire per la conservazione dell'integrità del dato giudiziario, l'accesso, l'esame, l'uso, la comunicazione e la cancellazione dei dati giudiziari oggetto di trasmissione telematica entro i tempi di stretta necessità dell'emergenza, in modo da realizzare la cosiddetta minimizzazione dei dati.
In definitiva, risulterebbe assente uno statuto di questo trattamento speciale di dati operato con modalità automatizzate, avendo obliterato altresì il legislatore una valutazione dei rischi aggiuntivi che tale modalità pone rispetto all'ordinario trattamento di dati che avviene in sede processuale.
Non ci pare, infine, che i più recenti sviluppi in materia, e in particolare il parere positivo espresso dal Garante per la protezione dei dati personali in merito al cd. processo amministrativo da remoto[34], possano considerarsi idonei a ridimensionare o finanche

[34] Cfr. S. Musco, *Processo da remoto, arriva il via libera del Garante della privacy*, in *Il Dubbio*, 22 maggio 2020; R. Berti - F. Zumerle, *Giustizia digitale, gli aspetti privacy delle udienze da remoto: ecco le regole*, in *agendadigitale.*

a risolvere i molteplici profili problematici sopra enucleati. Non foss'altro perché la natura dei cd. dati giudiziari specificamente afferenti al processo penale, caratterizzata come è da un effetto potenzialmente assai pregiudizievole e stigmatizzante nelle più varie sfere esistenziali della persona[35], impone di confrontarsi con preoccupazioni eccezionali, non comuni a nessun altro ramo dell'ordinamento giuridico.

Conclusivamente, si può dire, che tali preoccupazioni soltanto in parte possano dirsi superate in ragione dell'ultimo intervento del DGSIA che, sebbene non abbia fatto precedere l'emanazione del provvedimento direttoriale da un parere del Garante come invece è stato fatto nel processo amministrativo, ha corretto il tiro emanando in data 21 maggio un nuovo provvedimento con cui riconferma l'utilizzo degli strumenti già individuati nei provvedimenti del 10 e 20 marzo, ma ne precisa il funzionamento e gli aspetti privacy. In particolare si precisa che mentre i dati delle videoudienze attraverso *Microsoft Teams* sono ospitati su server di Microsoft in Irlanda e nei Paesi Bassi (data center che però sono "amministrati dalla D.G.S.I.A."), i dati relativi alle videoudienze tramite *Skype for Business* sono ospitati direttamente in data center dell'Amministrazione. Rispetto alle istanze di protezione della riservatezza si precisa che tutti i servizi vengono forniti attraverso un canale di comunicazione criptato. Il Ministero ha puntualizzato, infine, che per quanto riguarda *Teams* e *Skype for Business*, vengono conservati (da Microsoft e su server di Microsoft in Europa, nel caso di *Teams*, o su server del Ministero, nel caso di *Skype*) unicamente i dati tecnici di sessione, quali: orario di inizio e fine sessione, identificativo utente, durata, sistema operativo del dispositivo utilizzato, indirizzo IP[36]. Orbene, permangono distinte perplessità che riguardano comunque il potenziale accesso da parte di Microsoft Corporation ai dati relativi a chat, ai file scambiati nonché ai metadati relativi allo streaming video. Questa problematica è aggravata dal nodo del "*Clarifying Lawful Overseas Use of Data (CLOUD) Act*", che può essere opposto solo in caso di sottoscrizione di appositi *executive agreements* con "*qualifying foreign States*", dal momento che il c.d. "Privacy Shield" tra U.E. e Stati Uniti non sembrerebbe rientrare nel novero di tali *executive agreements*. In altri termini, come già ampiamente esposto, dati particolarmente delicati, attinenti alle vicende giudiziarie di individui incappati negli ingranaggi della macchina processuale, seppur da remoto, verrebbero a subire un trattamento al di fuori dell'alea di controllo di soggetti terzi ed indipendenti, come, invece, richiesto dalla normativa europea, e sarebbero altresì passibili di accessi occulti ed in maniera generalizzata, oltre il limite della stretta necessità, pregiudicando l'integrità e la sicurezza dei dati stessi.

---

eu, 22 maggio 2020; A. Polito, *Vita pubblica, chi detiene il software?*, in *Corriere della Sera*, 24 maggio 2020.

[35] Cfr. ad es., Cass. pen., sez. II, ord. 25 giugno 2018, n. 29248, nell'interpretare la disposizione di cui all'art. 52, d.lgs. 196/2003, relativo alle condizioni per l'oscuramento dei dati personali nei provvedimenti giurisdizionali penali: «Mentre i «dati sensibili» sono individuati dalla legge [...], lo stesso non può dirsi quanto alla «delicatezza» della vicenda processuale, nozione che necessita di essere riempita di contenuti concreti, sintomatici della peculiarità del caso e della capacità, insita nella diffusione dei dati relativi, di riverberare – come osserva lo stesso Garante – «negative conseguenze sui vari aspetti della vita sociale e di relazione dell'interessato (ad esempio, in ambito familiare o lavorativo)», così andando ad incidere pesantemente sul diritto alla riservatezza del singolo". Conseguentemente non basta, per ottenere l'oscuramento, il "danno alla reputazione", perché, altrimenti, "ogni processo penale dovrebbe comportare l'oscuramento dei dati personali».

[36] Cfr. *amplius* in proposito, R. Berti - F. Zumerle, *Giustizia digitale, gli aspetti privacy*, cit.

Verso l'attuazione della direttiva (UE) 2019/1024 sul riutilizzo degli open data della PA: nuove opportunità per le imprese*

Sara Gobbato

Abstract

Entro il 17 luglio 2021 gli Stati membri dell'UE devono attuare la direttiva (UE) 2019/1024, che abroga la vigente direttiva 2003/98/CE apportando significative novità in tema di riutilizzo dei dati aperti della PA. L'approssimarsi del termine obbligatorio di recepimento costituisce un'importante occasione per l'Italia, per diffondere la cultura degli open data così aggregando la domanda dei dati aperti della PA da parte dei soggetti che più potrebbero trarre beneficio dalle novità in arrivo, ossia le PMI e le start-up innovative. La nuova direttiva (UE) 2019/1024 accresce infatti la rilevanza economica del riutilizzo degli open data andando ad estenderne il campo di applicazione alle attività di interesse economico generale, ai "dati dinamici" e "di elevato valore" nonché ai dati prodotti nell'ambito della ricerca scientifica. In quanto atto di armonizzazione minima, la direttiva lascia al Legislatore nazionale il compito di sciogliere, in sede di trasposizione, importanti nodi applicativi quanto al rapporto tra riutilizzo ed accesso documentale/civico, alle licenze ed alla limitazione dei diritti esclusivi, alla previsione di tariffe ed alle opportune misura di tutela dei dati personali e dei segreti commerciali.

By July 17, 2021, EU Member States shall implement Directive (EU) 2019/1024 repealing with relevant amendments Directive 2003/98/EC on open data and the reuse of public sector information. The forthcoming mandatory deadline brings the opportunity to spread the open government data culture among in particular Italian SMEs and innovative start-ups, which may benefit the most from the new provisions on open data reuse. Directive (EU) 2019/1024 enhances the economic impact of reuse by extending its scope to the services of general economic interest, to "dynamic"

*Il presente contributo corrisponde al testo aggiornato dell'intervento svolto nel panel dedicato a "Nuove tecnologie per la PA e le imprese: problemi e prospettive", in occasione della seconda conferenza annuale di ICON-S Italian Chapter, "Le nuove tecnologie ed il futuro del diritto pubblico", tenutasi a Firenze il 22 novembre 2019. Su determinazione della direzione, l'articolo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista.

and "high-value" datasets as well as to research data. As minimum harmonisation act, the Directive requires national lawmakers to deal with relevant issues regarding the relationship between reuse and access to public documents, the implementation of licences, exclusive rights and tariffs, the protection of personal data and trade secrets.

Sommario

1. Un tesoro da scoprire (…entro il 17 luglio 2021): i dati aperti della PA. - 2. Notazioni preliminari sulla "clausola di salvaguardia": cogliamo l'occasione per chiarire i rapporti tra accesso vs riuso nella nuova direttiva (UE) 2019/1024. - 3. Ambito di applicazione soggettivo del riutilizzo: l'ampliamento ai SIEG. - 4. I dati dinamici e di elevato valore. - 5. Dati della ricerca scientifica. - 6. Licenze e limitazione ai diritti esclusivi. - 7. Gratuità e tariffazione. - 8. Tutela dei dati personali e dei segreti commerciali. - 9. Conclusione.

Keywords

open data – eGovernment – big data – dati personali – Direttiva PSI

1. Un tesoro da scoprire (...entro il 17 luglio 2021): i dati aperti della PA

Se i dati sono unanimemente indicati come una delle risorse più preziose nell'attuale fase della *digital economy* a livello globale, c'è tuttavia un tesoro che giace parzialmente negletto sotto gli occhi degli operatori economici: si tratta dei big data[1] raccolti dagli enti pubblici nell'ampio raggio di attività svolte nell'esercizio dei loro compiti di interesse generale.

Sull'onda del movimento internazionale "open data"[2], dal 2003 l'Unione europea si

[1] Per big data si intendono gli insiemi di dati digitali caratterizzati da alcune proprietà comuni sintetizzabili in (almeno) quattro "V": il Volume dei dati raccolti, la Velocità con i quali sono trattati, la loro Varietà ed infine il Valore economico da essi generato quale causa e conseguenza dell'incremento progressivo delle tre V precedenti. I big data sono dunque il campo di applicazione dei big data analytics e dell'intelligenza artificiale. In proposito A. De Mauro - M. Greco - M. Grimaldi, *A Formal Definition of Big Data Based on its Essential Features*, in *Library Review*, 65(3), 2016, 122 ss; Organization for Economic Co-operation and Development (OECD), *Big Data: bringing competition policy to the digital era*, DAF/COMP(2016)14, 29-30 novembre 2016, 5; Autorité de la Concurrence - Bundeskartellamt, *Competition Law and Data*, 10 maggio 2016, 8; M.E. Stucke - A.P. Grunes, *Big Data and Competition Policy*, Oxford, 2016; M. Maggiolino, *I big data e il diritto antitrust*, Milano, 2018; Autorità Garante della Concorrenza e del Mercato - Autorità per le Garanzie nelle Comunicazioni - Garante per la protezione dei dati personali, *Indagine Conoscitiva sui Big Data - IC53*, in Boll. AGCM n. 9/2020. Per ulteriori riferimenti bibliografici sia consentito un rinvio a S. Gobbato, *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in *questa Rivista*, 3, 2019, 148 ss.

[2] In proposito F. Sciacchitano, *Disciplina e utilizzo degli Open Data in Italia*, in *questa Rivista*, 1, 2018, 281 ss.; F. Martines, *La digitalizzazione della pubblica amministrazione*, ivi, 2, 2018, 146 ss.; M. Bisogno - S. Santis - G. Vaia - G. Cogo, *Toward a Quality Open Government Data Ecosystem: Actors and practices*, 2020 in *opendataveneto.regione.veneto.it*; E. Belisario - G. Cogo - S. Epifan - C. Forghieri (a cura di), *Come si fa Open Data? Istruzioni per l'uso per Enti e Amministrazioni Pubbliche (Versione 2.0)*, in *egovnews.it*, 2011, ove a p. 7

è dotata di una direttiva (la 2003/98/CE[3], c.d. *Public Service Information Directive* o "Direttiva PSI") che – mediante norme di armonizzazione minima – ha chiesto agli enti pubblici nazionali dapprima di agevolare il riutilizzo e, quindi, di mettere obbligatoriamente[4] a disposizione i "dati aperti" della PA, rendendoli riutilizzabili dai soggetti privati (ricercatori, sviluppatori, imprese, semplici cittadini) che ne facciano richiesta per finalità commerciali e non commerciali.

Attuata dall'Italia con il d.lgs. 36/2006 e parzialmente aggiornata nel 2013[5], la direttiva 2003/98/CE verrà integralmente abrogata mediante rifusione nella nuova direttiva (UE) 2019/1024[6], che dovrà essere recepita dai Paesi membri dell'Unione europea entro il 17 luglio 2021.

L'approssimarsi del termine obbligatorio di recepimento costituisce un'importante occasione per il nostro Paese per diffondere la cultura degli "open data della PA" nell'accezione codificata dall'art. 1 del Codice dell'Amministrazione Digitale (CAD)[7], consentendo agli operatori economici di sfruttare quest'*asset* strategico per creare processi, prodotti e servizi innovativi. Gli indici annualmente elaborati[8] ci dicono, infatti, che l'Italia – pur in posizioni avanzate nei *ranking* di *Open Data Maturity* – non esprime appieno il proprio potenziale in quanto non riesce ad aggregare la domanda di dati aperti da parte dei soggetti che più potrebbero trarne vantaggio, ossia le PMI e le start-up innovative. Il disallineamento tra domanda ed offerta, a livello nazionale, de-

si definisce l'Open Government come «un nuovo concetto di Governance a livello centrale e locale, basato su modelli, strumenti e tecnologie che consentono alle amministrazioni di essere "aperte" e "trasparenti" nei confronti dei cittadini».

[3] Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico, in *GUCE* L 345 del 31.12.2003, 90-96.

[4] Sul punto si veda R. Sanna, *Dalla trasparenza amministrativa ai dati aperti. Opportunità e rischi delle autostrade informatiche*, Torino, 2018, spec. 251 ove si precisa che, con l'emanazione della direttiva 2013/37/CE, di modifica dell'originaria direttiva 2003/98/CE, «l'indirizzo viene capovolto e si stabilisce l'obbligo generale, per i singoli Stati Membri, di consentire il riutilizzo di tutti i documenti generati dagli enti pubblici».

[5] Direttiva 2013/37/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico, in *GUUE* L 175 del 27.6.2013, 1-8.

[6] 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, in *GUUE* L 172 del 26.6.2019, 56-83.

[7] Ai sensi dell'art. 1 del d.lgs. 82/2005 ("Codice dell'Amministrazione Digitale", o CAD) per dati aperti si intendono: «i dati che presentano le seguenti caratteristiche: 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato; 2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera l-bis), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati; 3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione salvo quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36». I dati aperti si caratterizzano, dunque, per la presenza cumulativa necessaria dei tre citati requisiti di ordine rispettivamente "giuridico", "tecnico" ed "economico". In proposito, M. Bassi, *Open Data: cosa sono, come sfruttarli e stato dell'arte in Italia*, in *Forum PA*, 12 dicembre 2019.

[8] Commissione europea, *Open Data Maturity Report 2019*, in *europeandataportal.eu*.

riva dalla insufficiente conoscenza e dalle conseguenti difficoltà nell'implementazione delle disposizioni armonizzate per il riutilizzo dei dati aperti ai sensi del vigente d.lgs. 36/2006.
Per portare il nostro Paese a cogliere appieno i benefici che deriveranno dalle novità oggetto di implementazione entro l'anno prossimo, è dunque in questa fase cruciale richiamare l'attenzione degli operatori economici sul processo di recepimento della nuova direttiva (UE) 2019/1024. Vediamo quindi insieme le principali novità in arrivo.

2. Notazioni preliminari sulla "clausola di salvaguardia": cogliamo l'occasione per chiarire i rapporti tra accesso *vs* riuso nella nuova direttiva (UE) 2019/1024

Il passaggio dalla "vecchia Direttiva PSI" alla nuova direttiva (UE) 2019/1024 non ha alterato, nella sostanza, la "clausola di salvaguardia" ai sensi della quale le disposizioni armonizzate sul riutilizzo dei dati non pregiudicano i regimi di accesso vigenti nei Paesi membri dell'UE[9]. Si conferma, in tal modo, che non sono oggetto di riutilizzo i documenti, le informazioni e i dati della PA sottratti al diritto di accesso in virtù delle disposizioni applicabili in ciascuno Stato Membro[10].
Sul punto va tuttavia tenuto presente che proprio la citata clausola di salvaguardia ha posto in passato delle tensioni, in sede di applicazione del riuso a livello nazionale, rispetto agli altri istituti previsti dall'ordinamento in materia di accesso e trasparenza della PA. Quanto all'Italia è stato evidenziato, infatti, che nell'ordinamento interno non si è per il passato adeguatamente esplicitato «quale debba essere il corretto rapporto e il giusto punto di equilibrio tra l'utilizzazione dei dati, documenti e informazioni resi pubblici dalla PA per finalità di trasparenza o per scopo di riuso»[11].
Sotto questo profilo, il recepimento della direttiva (UE) 2019/1024 potrebbe dunque costituire l'occasione per chiarire in via normativa il raccordo esistente tra accesso ai documenti/informazioni/dati della PA ed il loro riutilizzo, così supportando i pubblici funzionari che – dall'anno prossimo – saranno chiamati a esaminare le istanze dei privati fornendo una risposta congrua in termini di legge.
Così come suggerito dalla giurisprudenza circa i rapporti fra i vigenti istituti dell'accesso documentale ai sensi della l. 241/1990 *vs.* l'accesso civico ai sensi del d.lgs. 33/2013[12], la formulazione di una previsione di raccordo espresso – in sede di rece-

[9] Cfr. art. 1, par. 3, della direttiva (UE) 2019/1024: «La presente direttiva si basa, senza pregiudicarli, sui regimi di accesso dell'Unione e nazionali».

[10] In proposito, si veda anche R. Sanna, *Dalla trasparenza amministrativa ai dati aperti*, cit., spec. 258.

[11] In tal senso F. Pizzetti, *Sentenza n. 20/2019 della Consulta e riordino degli obblighi di pubblicità, trasparenza e diffusione delle informazioni della PA: il legislatore non trascuri il "riuso" delle fonti pubbliche,* in *questa Rivista,* 2, 2019, 11 ss..

[12] Si veda ad esempio Tar Toscana, sez. II, 20 dicembre 2019, n. 1748, ove si è chiarito che: «L'accesso ai documenti amministrativi è oggi regolamentato da tre sistemi generali, ognuno caratterizzato da propri limiti e presupposti […]. Si tratta di istituti a carattere generale ma ognuno con oggetto diverso, e sono applicabili ognuno a diverse e specifiche fattispecie: ne segue che ognuno di essi opera nel proprio ambito di azione senza assorbimento della fattispecie in un'altra, e senza abrogazione tacita o implicita ad opera della disposizione successiva poiché diverso è l'ambito di applicazione di ciascuno di

pimento della direttiva (UE) 2019/1024 – potrebbe essere utile a ridurre le remore al riutilizzo, tenendo conto delle diverse basi giuridiche, delle connesse finalità e dei rispettivi campi di esclusione di ciascuno dei seguenti strumenti:
(i) l'accesso ai documenti della PA ai sensi degli artt. 22 e ss. l. 241/1990. Si tratta come noto di mezzo non azionabile da chiunque. È infatti strumentale alla tutela degli interessi del soggetto privato che, in quanto possa affermare con richiesta motivata di essere in una posizione differenziata, ha il diritto di prendere visione ed estrarre copia di un particolare documento già detenuto dalla PA[13]. L'accesso è escluso, oltre che per finalità di controllo generalizzato dell'attività della PA, nelle fattispecie previste dall'art. 24 l. 241/1990;
(ii) l'accesso civico semplice ai sensi dell'art. 5, c. 1, del d.lgs. 33/2013 ha ad oggetto i particolari «documenti, informazioni o dati» che, per obbligo di legge, devono essere pubblicati dalla PA. Nei casi in cui l'obbligo non sia stato assolto, ciascun individuo ha il diritto di richiedere alla PA la pubblicazione senza fornire particolare motivazione, salvo l'indicazione dei «documenti, informazioni o dati» oggetto di accesso;
(iii) l'accesso civico generalizzato (sul modello del c.d. FOIA) è previsto dall'art. 5, c. 2, del d.lgs. 33/2013 e consente a «chiunque» – senza particolare motivazione – di presentare un'istanza di accesso ai dati e ai documenti detenuti dalle PA ulteriori rispetto a quelli oggetto di pubblicazione. L'accesso civico generalizzato può essere rifiutato qualora ciò si renda necessario per tutelare gli interessi pubblici e privati (fra i quali la tutela dei dati personali) elencati all'art. 5-bis del d.lgs. 33/2013;
(iv) il riutilizzo dei dati aperti della PA ai sensi del d.lgs. 36/2006[14] – che come detto ai sensi della clausola di salvaguardia non pregiudica i precedenti strumenti sub i-ii-iii ma si basa su di essi andandovisi ad aggiungere – «è finalizzato allo *sfruttamento economico* delle informazioni a disposizione della PA e non a finalità di controllo e partecipazione democratica»[15]. Può essere richiesto da chiunque per finalità sia commerciali sia non commerciali. Mentre le forme di accesso documentale *sub* i) e civico sub ii) e iii) sono destinate a "persone", i dati aperti della PA, oggetto di riutilizzo, sono destinati ad essere rielaborati da macchine ("*machine readable*") secondo la definizione di "dato aperto" accolta dall'art. 1 del CAD[16].
Al fine di tener conto della concatenazione fra gli strumenti in esame rispetto al riuso, occorre tuttavia tener presente che la direttiva (UE) 2019/1024 è fondata sul paradig-

essi. Ognuno di questi presenta caratteri di specialità rispetto all'altro. Di conseguenza, come ritenuto in tale arresto che il Collegio condivide, laddove il richiedente abbia espressamente optato per un modello è precluso all'Amministrazione qualificare diversamente l'istanza, al fine di individuare la disciplina applicabile. Correlativamente il richiedente, una volta effettuata la propria istanza motivata dai presupposti di una specifica forma di accesso, non potrà effettuare una conversione della stessa in corso di causa. Questa infatti si radica su una specifica richiesta e sulla relativa risposta negativa dell'Amministrazione che concorrono a formare l'oggetto del contendere».

[13] N. Durante, *Pubblicità, trasparenza e FOIA: indicazioni operative*, in *ItaliaAppalti.it*, 29 marzo 2018.

[14] Attualmente l'art. 3 del d.lgs. 36/2006 esclude dal riutilizzo, tra l'altro, i documenti «esclusi dall'accesso ai sensi dell'articolo 24 della legge 7 agosto 1990, n. 241».

[15] *Ibidem*.

[16] In proposito E. Tonelli, *Gli obblighi in materia di trasparenza e le caratteristiche dei siti web*, in A. Francioni - P. Saggini - E. Tonelli, *La riforma del Codice dell'Amministrazione Digitale e i Servizi Demografici*, Santarcangelo di Romagna, 2018, spec. 240.

ma "*open by default*", in base al quale gli Stati membri sono incoraggiati a promuovere l'apertura dei dati «fin dalla progettazione e per impostazione predefinita»[17]. Per l'effetto, in sede di trasposizione della clausola di salvaguardia, occorrerebbe chiarire che formano oggetto di riutilizzo *tutti i dati della PA*, che si considerano *open by default* in applicazione dell'art. 1 CAD[18], *ad eccezione* di quanto escluso dall'accesso documentale e civico ai sensi rispettivamente della l. 241/1990 e del d.gs. 33/2013.
Stante la diversità degli istituti dell'accesso rispetto al riutilizzo, dovrebbe rimanere in ogni caso onere del privato, in sede di formulazione dell'istanza, individuare espressamente l'oggetto della propria domanda ai sensi della disciplina sul riutilizzo degli open data[19].

3. Ambito di applicazione soggettivo del riutilizzo: l'ampliamento ai SIEG

L'art. 4 della vigente direttiva 2003/38/CE prevede che:

«[g]li enti pubblici esaminano le richieste di riutilizzo e mettono i documenti a disposizione del richiedente, ove possibile e opportuno per via elettronica o, se è necessaria una licenza, mettono a punto l'offerta di licenza per il richiedente entro un lasso di tempo ragionevole e coerente con quello previsto per l'esame delle richieste di accesso ai documenti».

Per "ente pubblico" la direttiva intende le «autorità statali, regionali o locali» e «gli organismi di diritto pubblico» che soddisfano esigenze generali di carattere non industriale e commerciale[20].

[17] V. considerando 16 della direttiva (UE) 2019/1024.

[18] V. *supra* in nota 7.

[19] Circa l'ammissibilità di istanze congiunte formulate nella medesima domanda da parte del privato, il T.A.R. Lombardia, sez. III, 27 dicembre 2019, n. 2750, ha chiarito che «la domanda di accesso civico generalizzato ben può proporsi manifestando (anche) la sussistenza dei presupposti per la formulazione della richiesta di accesso documentale, ai sensi della L. n. 241 del 1990, con la medesima ed unica istanza, tenuto conto che i presupposti che consentono la formulazione della domanda di accesso civico sono ben definiti nell'art. 5, comma 2, D.lgs. n. 33 del 2013 ("favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico") ed essi sono ben diversi dai presupposti che l'art. 24, comma 7, primo periodo, L. n. 241 del 1990 individua al fine di consentire l'accesso civico documentale (garantire "ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici")». Sui rapporti fra accesso documentale ed accesso civico è più recentemente intervenuto il Consiglio di Stato, Adunanza Plenaria, 2 aprile 2020, n. 10, ove si è chiarito tra l'altro che «la pubblica amministrazione ha il potere-dovere di esaminare l'istanza di accesso agli atti e ai documenti pubblici, formulata in modo generico o cumulativo dal richiedente senza riferimento ad una specifica disciplina, anche alla stregua della disciplina dell'accesso civico generalizzato, a meno che l'interessato non abbia inteso fare esclusivo, inequivocabile, riferimento alla disciplina dell'accesso documentale».

[20] Si veda l'art. 2, n. 2, della vigente direttiva 2003/38/CE che definisce "organismo di diritto pubblico" come «qualsiasi organismo: a) istituito per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale; e b) dotato di personalità giuridica; e c) la cui

La nuova direttiva (UE) 2019/1024 va ad ampliare il novero dei soggetti potenzialmente tenuti al riutilizzo includendovi anche le "imprese pubbliche" secondo la definizione fornita all'art. 2, n. 3:
- si tratta[21] delle imprese attive nei settori: (i) dell'acqua, dell'energia, dei trasporti e dei servizi postali (definiti dalla direttiva 2014/25/UE)[22]; (ii) del trasporto pubblico passeggeri su strada e per ferrovia ai sensi del Regolamento (CE) 1370/2007[23]; (iii) del trasporto aereo di servizio pubblico a norma dell'art. 16 del Regolamento (CE) 1008/2008[24]; del trasporto marittimo di servizio pubblico ai sensi dell'art. 4 del Regolamento (CEE) 3577/92[25];
- oltre ad essere attiva nei predetti settori, l'"impresa pubblica" si caratterizza in quanto sottoposta, direttamente o indirettamente, ad un'influenza dominante degli "enti pubblici". Tale influenza si ritiene presunta qualora gli enti pubblici rientrino in uno dei seguenti casi: a) essi detengono la maggioranza del capitale sottoscritto dell'impresa; b) dispongono della maggioranza dei voti; c) possono designare più della metà dei membri degli organi di amministrazione, direzione o vigilanza[26].
In merito alle "imprese pubbliche" così definite, la direttiva (UE) 2019/1024 applica un approccio di tipo "funzionale" ossia relativo alla tipologia di attività in concreto svolta: potranno essere oggetto di riutilizzo i documenti prodotti dalle imprese pubbliche nell'assolvimento delle attività di servizio pubblico ad esse affidate. Di contro, non saranno riutilizzabili i documenti prodotti nello svolgimento di attività che esulano dai compiti di servizio pubblico (come definiti da norme di legge o, in mancanza, dalla prassi trasparente e soggetta a revisione di ciascuno Stato membro), oppure di attività che sono esposte alla concorrenza ai sensi dell'art. 34 della direttiva 2014/25/UE.
Fra gli "enti pubblici" e le "imprese pubbliche" permane, tuttavia, una sostanziale differenza. Mentre gli "enti pubblici" sono assoggettati all'*obbligo* di concedere il riutilizzo rispondendo alle relative istanze dei privati nei termini indicati dall'art. 4[27], la direttiva

attività è finanziata in modo maggioritario dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico, oppure la cui gestione è soggetta al controllo di questi ultimi, oppure il cui organo d'amministrazione, di direzione o di vigilanza è costituito da membri più della metà dei quali è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico».

[21] V. l'elencazione contenuta all'art. 1, lett. *b)* della direttiva (UE) 2019/1024.

[22] Direttiva 2014/25/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali e che abroga la direttiva 2004/17/CE, in *GUUE* L 94 del 28.3.2014, 243-374.

[23] Regolamento (CE) 1370/2007 del Parlamento europeo e del Consiglio, del 23 ottobre 2007, relativo ai servizi pubblici di trasporto di passeggeri su strada e per ferrovia e che abroga i regolamenti del Consiglio (CEE) n. 1191/69 e (CEE) n. 1107/70, in *GUUE* L 315 del 3.12.2007, 1-13.

[24] Regolamento (CE) 1008/2008 del Parlamento europeo e del Consiglio, del 24 settembre 2008, recante norme comuni per la prestazione di servizi aerei nella Comunità (rifusione), in *GUUE* L 293 del 31.10.2008, 3-20.

[25] Regolamento (CEE) 3577/92 del Consiglio, del 7 dicembre 1992, concernente l'applicazione del principio della libera prestazione dei servizi ai trasporti marittimi fra Stati membri (cabotaggio marittimo), in *GUCE* L 364 del 12.12.1992, 7-10.

[26] V. art. 2, n. 3, lett. *a), b), c)* della direttiva (UE) 2019/1024.

[27] Ai sensi dell'art. 4, l'ente pubblico dovrà provvedere sull'istanza «entro un lasso di tempo ragionevole e coerente con quello previsto per l'esame delle richieste di accesso ai documenti». In caso di rigetto, il provvedimento dovrà essere motivato e includere l'indicazione della «persona fisica o giuridica

(UE) 2019/1024

«non prescrive un obbligo generale di consentire il riutilizzo dei documenti prodotti dalle imprese pubbliche. La decisione di autorizzare o meno il riutilizzo dovrebbe spettare *all'impresa pubblica interessata*, salvo diversamente disposto dalla presente direttiva o dal diritto dell'Unione o nazionale»[28].

A tal riguardo infatti, in sede di recepimento della direttiva che è atto di armonizzazione minima, ciascuno Stato potrebbe decidere di adottare norme interne più stringenti, ampliando l'ambito di riutilizzo obbligatorio rispetto a quanto previsto (sotto il profilo soggettivo e oggettivo) dalla direttiva stessa, fatti salvi i limiti previsti da altri atti dell'UE (es. il GDPR[29]) e dalle clausole di salvaguardia contenute nella direttiva stessa. Fermi dunque il carattere non obbligatorio del riutilizzo da parte delle "imprese pubbliche" e la facoltà degli Stati di introdurre norme più stringenti al riguardo, la direttiva affida comunque ai Paesi membri il compito di *incoraggiare* anche le "imprese pubbliche" a produrre e mettere a disposizione in formato "*open by default*" i documenti prodotti nell'esercizio dei compiti di servizio pubblico[30].

4. I dati dinamici e di elevato valore

L'impatto economico potenziale del riutilizzo dei dati aperti è destinato ad aumentare, a seguito dell'attuazione della direttiva (UE) 2019/1024, anche grazie alla sua estensione ai "dati dinamici". Questi sono definiti come i «documenti in formato digitale, soggetti ad aggiornamenti frequenti o in tempo reale, in particolare a causa della loro volatilità o rapida obsolescenza»[31].
In tale categoria rientrano ad esempio i dati ambientali, relativi al traffico satellitari, meteorologici e i dati generati da sensori, il cui valore economico dipende dall'immediata disponibilità dell'informazione e da regolari aggiornamenti[32]. Per tale categoria di dati, il riutilizzo dovrà avvenire mediante accesso in tempo reale ad interfacce per programmi applicativi (API), per quanto possibile di tipo aperto, come download in

titolare del diritto, se è nota, oppure il licenziante dal quale l'ente pubblico ha ottenuto il materiale in questione», nonché dei mezzi di ricorso a disposizione del richiedente qualora questi intenda impugnare il provvedimento di diniego. Il procedimento previsto dall'art. 4 non si applica alle "imprese pubbliche" né agli istituti di istruzione, alle organizzazioni che svolgono attività di ricerca e alle organizzazioni che finanziano la ricerca.

[28] Si veda il considerando 26 della direttiva (UE) 2019/1024.

[29] 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 o *General Data Protection Regulation* - GDPR), in *GUUE* L 119 del 4.5.2016, 1-88.

[30] V. art. 5, par. 2, della direttiva (UE) 2019/1024.

[31] V. art. 2, n. 8, della direttiva (UE) 2019/1024.

[32] V. considerando 31 della direttiva (UE) 2019/1024.

blocco, salvo i casi in cui ciò comporti uno sforzo sproporzionato[33]. La valutazione della proporzionalità dello sforzo, quanto all'immediata messa a disposizione dei dati, dovrebbe essere svolta in relazione alle reali capacità finanziarie e tecniche, tenendo conto della dimensione e del bilancio di funzionamento dell'ente pubblico o dell'impresa pubblica che detiene i dati in questione[34].
La direttiva (UE) 2019/1024 assicura inoltre la riutilizzabilità di "serie di dati di elevato valore" in termini di benefici associati per la società, l'ambiente e l'economia, in particolare in considerazione di alcuni parametri di riferimento: (i) l'idoneità di tali dati alla creazione di servizi e applicazioni a valore aggiunto; (ii) la capacità di generare nuovi posti di lavoro «dignitosi e di alta qualità»; (iii) il numero dei potenziali beneficiari dei servizi e delle applicazioni a valore aggiunto[35].
A titolo di esempio, la direttiva cita nell'ambito di tale categoria di dati di elevato valore:

«i codici di avviamento postale, le mappe e le carte nazionali e locali (dati geospaziali), il consumo energetico e le immagini satellitari (dati relativi all'osservazione della terra e all'ambiente), i dati in situ provenienti da strumenti e previsioni meteorologiche (dati meteorologici), gli indicatori demografici e economici (dati statistici), i registri delle imprese e gli identificativi di registrazione (dati relativi alle imprese e alla proprietà delle imprese), la segnaletica stradale e le vie navigabili interne (dati relativi alla mobilità)»[36].

L'Allegato I alla direttiva fornisce l'elenco delle categorie tematiche[37], per le quali viene affidato alla Commissione europea il compito di specificare le serie di dati oggetto di riutilizzo, mediante un atto di esecuzione di prossima adozione[38].
I dati di elevato valore dovranno essere leggibili meccanicamente ed essere resi disponibili mediante API in forma gratuita, salvo alcuni casi eccezionali in cui sarà possibile applicare una tariffa. Le eccezioni al principio di gratuità riguardano precisamente i dati di elevato valore in possesso di: (i) imprese pubbliche, nell'ipotesi in cui il riutilizzo possa generare una distorsione della concorrenza; (ii) biblioteche (anche universita-

[33] V. considerando 32 (ove si precisa che «[p]er API si intende un insieme di funzioni, procedure, definizioni e protocolli per la comunicazione da macchina a macchina e lo scambio ininterrotto di dati») e art. 5, par. 6, della direttiva (UE) 2019/1024.

[34] In tal senso v. sempre il considerando 32.

[35] V. art. 2, n. 10, della direttiva (UE) 2019/1024.

[36] V. considerando 66 della direttiva (UE) 2019/1024.

[37] Le categorie tematiche in All. I hanno a oggetto precisamente: 1. Dati geospaziali; 2. Dati relativi all'osservazione della terra e all'ambiente; 3. Dati meteorologici; 4. Dati statistici; 5. Dati relativi alle imprese e alla proprietà delle imprese; 6. Dati relativi alla mobilità. I dati geospaziali rientrano nel campo di applicazione della direttiva 2007/2/CE del Parlamento europeo e del Consiglio, del 14 marzo 2007, che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea (Inspire), in *GUCE* L 108 del 25.4.2007, 1-14, sulla quale si veda K. Janssen, *INSPIRE and re-use of PSI. A model for the sharing and trading of geographic data*, 2004, in *law.kuleuven.be*.

[38] In proposito v. Commissione europea, *A European strategy for data*, COM(2020) 66 final, in *ec.europa.eu*, ove a p. 13 si precisa che la procedura per l'individuazione dei dati di elevato valore dovrebbe essere svolta nel primo trimestre del 2021.

rie), musei e archivi; (iii) enti pubblici che devono generare utili per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico[39].

5. Dati della ricerca scientifica

La direttiva (UE) 2019/1024 estende il campo del riutilizzo anche ai dati prodotti nell'ambito della ricerca finanziata con fondi pubblici[40], da mantenere distinti rispetto agli «articoli scientifici, in cui si riportano e si commentano le conclusioni della ricerca scientifica sottostante»[41]. Per dati della ricerca si intendono infatti:

«[i] documenti in formato digitale, diversi dalle pubblicazioni scientifiche, raccolti o prodotti nel corso della ricerca scientifica e utilizzati come elementi di prova nel processo di ricerca, o comunemente accettati nella comunità di ricerca come necessari per convalidare le conclusioni e i risultati della ricerca»[42].

I dati saranno riutilizzabili a fini commerciali o non commerciali in presenza di alcune condizioni previste dall'art. 10 della direttiva. In particolare, i dati dovranno essere prodotti nell'ambito di ricerche finanziate con fondi pubblici e dovranno essere già resi pubblici attraverso una banca dati gestita a livello istituzionale o su base tematica. Il riutilizzo non riguarda comunque i dati coperti da segreto commerciale o da diritti di proprietà intellettuale di terzi, nonché i dati coperti da riservatezza per motivi di sicurezza nazionale, difesa o sicurezza pubblica[43].

6. Licenze e limitazione ai diritti esclusivi

Una delle caratteristiche essenziali dei "dati aperti", ai sensi dell'art. 1 del CAD[44], è quella di essere «disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato», oltre che essere accessibili attraverso le tecnologie ICT in formati aperti.
La direttiva (UE) 2019/1024 raccomanda agli Stati membri di concedere il riutilizzo sulla base di *licenze standard*[45], mediante le quali sarà possibile imporre ai terzi il rispetto

[39] V. art. 14, parr. 3, 4 e 5.

[40] Il considerando 27 cita ad esempio: «le statistiche, i risultati di esperimenti, le misurazioni, le osservazioni risultanti dall'indagine sul campo, i risultati di indagini, le immagini e le registrazioni di interviste, oltre a metadati, specifiche e altri oggetti digitali».

[41] V. considerando 27 della direttiva (UE) 2019/1024.

[42] V. art. 2, n. 9 della direttiva (UE) 2019/1024.

[43] V. considerando 28 della direttiva (UE) 2019/1024.

[44] V. *supra* in nota 7.

[45] V. art. 2, n. 5, della direttiva (UE) 2019/1024, che definisce la "licenza standard" come «una serie di condizioni predefinite di riutilizzo in formato digitale, di preferenza compatibili con le licenze pubbliche standardizzate disponibili online».

di condizioni solo qualora esse risultino obiettive, proporzionate, non discriminatorie e giustificate sulla base di finalità di interesse pubblico[46]. In ogni caso, le licenze dovrebbero prevedere il minor numero possibile di restrizioni al riutilizzo, limitandole, per esempio, all'indicazione della fonte dei dati[47].

In merito alla titolarità dei diritti sui dati della PA saranno quindi rinvenibili due situazioni:

- vi saranno dati coperti da copyright nella esclusiva disponibilità della PA, quali ad esempio lo stemma o il logo identificativo dell'Amministrazione. Questa tipologia di dati risulta esclusa dall'ambito di applicazione della direttiva (UE) 2019/1024[48], potendo invece essere oggetto di procedimenti amministrativi di autorizzazione all'utilizzo da parte dei terzi[49];

-vi saranno dati propriamente aperti rientranti nella direttiva (UE) 2019/1024, pubblicati mediante licenza che ne indichi le condizioni del riutilizzo. A tal riguardo, la direttiva (UE) 2019/1024 non specifica la tipologia di licenza da impiegare. Sul punto rimangono dunque percorribili le linee già individuate dall'AgID, che propendono per l'uso della licenza *Creative Commons* CC-BY 4.0[50], la quale consente di distribuire, modificare, rielaborare creando opere derivate, anche a scopi commerciali nel rispetto del riconoscimento e menzione della fonte dei dati[51].

Al fine di evitare che il riutilizzo possa portare a fenomeni distorsivi della concorrenza, l'art. 12 della direttiva introduce il generale divieto di attribuzione di diritti esclusivi

---

46 V. art. 8 della direttiva (UE) 2019/1024.

47 V. considerando 44.

48 V. art. 1, par. 2, lett. *g)*.

49 In proposito E. Tonelli, *Gli obblighi in materia di trasparenza e le caratteristiche dei siti web*, cit., 243.

50 AgID, *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico*, versione 2017, disponibile in *dati.gov.it*, spec. azione n. 12 ove si legge che «tenuto conto del contesto normativo di riferimento, delle indicazioni in tema di licenze contenute nella Comunicazione della Commissione 2014/C - 240/01 e dei principi di indisponibilità dei beni del demanio culturale espresso negli artt. 10 e 53 del Codice dei beni culturali (d.lgs. 22 gennaio 2004, n. 42), si ritiene opportuno fare riferimento ad una licenza unica aperta, che garantisca libertà di riutilizzo, che sia internazionalmente riconosciuta e che consenta di attribuire la paternità dei *dataset* (attribuire la fonte). Pertanto, si suggerisce l'adozione generalizzata della licenza CC-BY nella sua versione 4.0, presupponendo altresì l'attribuzione automatica di tale licenza nel caso di applicazione del principio "Open Data by default", espresso nelle disposizioni contenute nell'articolo 52 del CAD». In proposito si veda ancora E. Tonelli, *Gli obblighi in materia di trasparenza e le caratteristiche dei siti* web, cit., 241 ove, con riferimento agli obblighi di trasparenza della PA, l'Autore caldeggia l'adozione di licenze CC BY 4.0, in luogo del rilascio in pubblico dominio (CC 0) anche per ragioni di tutela dei dati personali e del diritto all'oblio degli interessati. Si veda anche M. Ragone, *CC0 o CC-BY. Il dilemma sulle licenze applicate ai dati aperti*, in *Forum PA*, 30 luglio 2019. Con decisione C(2019) 1655 final del 22 febbraio 2019, la Commissione europea ha individuato la *Creative Commons Attribution 4.0 International Public License* (CC-BY 4.0) quale licenza standard per il riutilizzo dei propri dati ai sensi della direttiva 2011/833/UE (v. decisione C(2019) 1655 final, art. 1); fermo l'utilizzo della CC BY 4.0, la Commissione ha inoltre indicato l'applicazione del *Creative Commons Universal Public Domain Dedication deed* (CC0 1.0) in via alternativa per «*raw data, metadata or other documents of comparable nature*» (v. decisione C(2019) 1655 final, art. 2).

51 In proposito M. Palmirani - D. Girardi - M. Martoni - M. Rossi - M. Ragone - F. Faini, *Le licenze per il rilascio degli Open Data della Pubblica Amministrazione. Prime riflessioni alla luce dalla Direttiva UE 2019/1024*, in *Diritto Mercato e Tecnologia*, 14 novembre 2018, 23, ove si precisa che «la CC-by non si pone in contrasto con le teorie dei dati definiti come commons, dal momento che ne garantisce pieno riutilizzo e sfruttamento da parte della collettività e, semplicemente, chiarisce il ruolo dell'autore (la P.a.) che protegge così l'affidamento alla collettività stessa su quel *dataset*».

agli utilizzatori, ai sensi del quale «[i] documenti possono essere riutilizzati da tutti gli operatori potenziali sul mercato, anche qualora uno o più operatori stiano già procedendo allo sfruttamento di prodotti a valore aggiunto basati su tali documenti».
La norma ammette la costituzione di diritti esclusivi nel caso in cui ciò si renda necessario ai fini dell'erogazione di un servizio d'interesse pubblico. Trattandosi di un'eccezione, l'ammissibilità dell'esclusiva dovrà, tuttavia, essere valutata in via restrittiva in concreto caso per caso e sarà soggetta ad un riesame periodico, con scadenza triennale, quanto alla permanenza dei requisiti che giustificano l'esclusiva[52].

7. Gratuità e tariffazione

L'art. 6 della direttiva (UE) 2019/1024 ribadisce che il riutilizzo è di base gratuito[53], mentre potrà essere autorizzato il recupero dei costi marginali sostenuti per la riproduzione, messa a disposizione e divulgazione dei documenti, nonché per l'anonimizzazione di dati personali o per le ulteriori misure adottate per proteggere le informazioni commerciali a carattere riservato.
Il principio generale di gratuità, salvo recupero dei costi marginali necessari al riutilizzo, non si applica in via eccezionale a tre categorie di soggetti, i quali saranno dunque ammessi ad applicare tariffe:
a) gli enti pubblici che devono generare proventi per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico, secondo quanto riportato in un elenco che dovrà essere stilato da ciascuno Stato membro;
b) le imprese pubbliche;
c) le biblioteche, i musei e gli archivi.
Enti pubblici e imprese pubbliche potranno applicare tariffe, inclusive di un margine di utile, determinate sulla base di criteri definiti dagli Stati membri[54]. Biblioteche, musei ed archivi potranno applicare tariffe, anch'esse inclusive di un margine di utile ragionevole, potendo prendere a tal fine «in considerazione i prezzi praticati dal settore

[52] V. art. 12 della direttiva (UE) 2019/1024.

[53] La gratuità è uno dei requisiti essenziali dell'accesso aperto inteso, ai fini della direttiva (UE) 2019/1024, come «la pratica di fornire accesso online ai risultati della ricerca a titolo gratuito per l'utente finale e senza limitazioni di utilizzo e riutilizzo oltre la possibilità di esigere il riconoscimento dell'autore» (in tal senso, considerando 27). L'introduzione di tariffe per il riutilizzo costituirebbe, infatti, un'importante barriera all'ingresso nel mercato per le start-up e le PMI, tale da disincentivare dal riutilizzo proprio i soggetti che più potrebbero trarre vantaggio dalla disponibilità dei dati aperti della PA (v. in tal senso considerando 36).

[54] V. art. 6, par. 4, ove si prevede che: «Il totale delle entrate ricavate dalla fornitura e dall'autorizzazione al riutilizzo dei documenti in un periodo contabile adeguato non supera i costi della loro raccolta, produzione, riproduzione, diffusione e archiviazione dei dati, maggiorati di un utile ragionevole sugli investimenti, e — ove applicabile — di anonimizzazione di dati personali e delle misure adottate per proteggere le informazioni commerciali a carattere riservato». Ai fini della determinazione dell'utile sugli investimenti, il considerando 37 chiarisce che: «[l]'utile sugli investimenti può essere inteso come una percentuale, oltre ai costi marginali, che consente il recupero dei costi di capitale e l'inclusione di un tasso reale di rendimento. Dato che i costi di capitale sono strettamente collegati ai tassi di interesse degli istituti di credito, che a loro volta si basano sul tasso fisso della Banca centrale europea (BCE) sulle operazioni di rifinanziamento principale, l'utile ragionevole sugli investimenti non dovrebbe superare del 5 % il tasso d'interesse fisso della BCE».

privato per il riutilizzo di documenti identici o simili»[55].
Va peraltro tenuto presente che i criteri di tariffazione previsti dalla direttiva sono finalizzati a porre un *limite massimo* agli importi richiesti in sede di riutilizzo, mentre è facoltà degli Stati membri quella di «imporre costi inferiori o di non imporne affatto»[56].

8. Tutela dei dati personali e dei segreti commerciali

Anche ai sensi della nuova direttiva (UE) 2019/1024, la disciplina del riutilizzo non potrà comportare la diffusione di dati personali in violazione delle pertinenti disposizioni UE (il GDPR e la direttiva 2002/58/CE) nonché nazionali (per l'Italia il d.lgs. 196/2003 come adeguato al GDPR dal d.lgs. 101/2018)[57].
Come evidenziato dalla stessa Commissione europea, l'obbligo di tutelare i dati personali non comporta che i documenti della PA contenenti tale tipologia di dati siano automaticamente sottratti dall'ambito di applicazione della direttiva (UE) 2019/1024. Le Amministrazioni dovranno invece compiere una valutazione preventiva in tre passaggi successivi[58]:
1) in primo luogo, occorrerà stabilire se tra i dati oggetto di riutilizzo vi siano "dati personali" ai sensi dell'art. 4 del GDPR;
2) in caso di risposta positiva, si dovrà considerare se il regime di accesso vigente a livello nazionale escluda o limiti l'accesso ai dati personali in questione. Ove la risposta sia affermativa, i dati personali *potrebbero* essere sottratti dal riutilizzo così come lo sono dall'accesso;
3) laddove si decida di assoggettare i dati personali al riutilizzo, essi dovranno essere trattati nel rispetto dei principi e vincoli imposti dal GDPR[59], procedendo ove possibile alla anonimizzazione[60] mediante misure idonee ad impedire efficacemente l'identificazione e la re-identificazione dei soggetti interessati[61].

[55] V. considerando 38.

[56] V. considerando 39.

[57] V. considerando 52 e art. 1, par. 4.

[58] In proposito, Commissione europea, S*tudy to support the review of Directive 2003/98/EC on the re-use of public sector information*, 2018, 135.

[59] In proposito si veda Article 29 Working Party, *Opinion 06/2013 on open data and public sector information ("PSI") reuse (WP207)*, del 5 giugno 2013, in *ec.europa.eu*, la quale – benché antecedente al GDPR – risulta secondo la Commissione europea pienamente applicabile in materia di riutilizzo degli open data della PA in vigenza del GDPR. In tal senso, Commissione europea, S*tudy to support the review of Directive 2003/98/EC* cit., 139.

[60] V. art. 2, n. 7 della direttiva (UE) 2019/1024, ai sensi del quale per anonimizzazione si intende «la procedura mirante a rendere anonimi documenti in modo che non riconducano a una persona fisica identificata o identificabile ovvero la procedura mirante a rendere anonimi dati personali in modo da impedire o da non consentire più l'identificazione dell'interessato».

[61] In proposito si veda Garante Privacy, provvedimento n. 243 del 15 maggio 2014, recante le *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati* (in *GU* 12 giugno 2014, n. 134 suppl. ord. n. 43 e in *gpdp.it*, doc. web n. 3134436), 21, ove si legge che «il riutilizzo di tali documenti non deve pregiudicare il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali fissato dalle disposizioni di diritto europeo e nazionale in materia. In particolare, le nuove disposizioni

Per consentire il corretto trattamento dei dati personali, evitandone la diffusione nel rispetto del GDPR, la direttiva (UE) 2019/1024 ammette le spese di anonimizzazione tra i costi marginali che possono essere recuperati dall'Amministrazione presso gli utilizzatori. In sede di trasposizione della direttiva, gli Stati membri potrebbero introdurre un preciso obbligo a carico degli enti pubblici di svolgere sistematicamente un'apposita valutazione di impatto a norma dell'art. 35 GDPR[62] in merito all'adeguatezza delle misure adottate a protezione dei dati personali[63].
Il riutilizzo non potrà inoltre comportare la diffusione né di dati coperti dai diritti di proprietà intellettuale[64] (intesi come diritto d'autore e diritti connessi, comprese le forme di protezione *sui generis*), né di dati soggetti a diritti di proprietà industriale, quali brevetti, disegni e modelli registrati e marchi[65]. Sono esclusi dal riutilizzo i dati sottratti dal regime di accesso vigente nello Stato membro, in quanto coperti da segretezza nell'interesse nazionale o contenenti segreti commerciali, professionali o d'impresa[66]. Come per i costi sostenuti a tutela dei dati personali, anche le spese funzionali alla protezione delle informazioni commerciali a carattere riservato potranno essere recuperate dalla PA presso l'utilizzatore a titolo di costi marginali[67].

9. Conclusione.

Il recepimento della direttiva (UE) 2019/1024 costituisce l'occasione per diffondere la cultura degli open data presso gli operatori economici, ponendoli nelle condizioni di

della direttiva introducono specifiche eccezioni al riutilizzo fondate sui principi di protezione dei dati, prevedendo che una serie di documenti del settore pubblico contenenti tale tipologia di informazioni siano sottratti al riuso anche qualora siano liberamente accessibili online. Ciò significa che il principio generale del libero riutilizzo di documenti contenenti dati pubblici, stabilito dalla disciplina nazionale ed europea, riguarda essenzialmente documenti che non contengono dati personali oppure riguarda dati personali opportunamente aggregati e resi anonimi».

[62] V. in tal senso il considerando 53 della direttiva (UE) 2019/1024, ove si chiarisce che «[a]l momento di prendere decisioni sulla portata e sulle condizioni del riutilizzo di documenti del settore pubblico contenenti dati personali, per esempio nel settore della sanità, può essere imposto l'obbligo di procedere a valutazioni d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679». Anche in difetto di un preciso obbligo sistematico di legge in sede di trasposizione della direttiva (UE) 2019/1024, l'obbligo di agire ai sensi dell'art. 35 GDPR sorge in base allo stesso GDPR, ove l'Amministrazione – in qualità di titolare del trattamento – ravvisi i profili di rischio richiamati dalla norma.

[63] In proposito si veda Garante Privacy, *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi*, cit., 25 ove si legge che «dal punto vista tecnico, è importante considerare con attenzione quali accorgimenti tecnologici possono essere messi in atto per ridurre i rischi di usi impropri dei dati personali resi disponibili online e delle conseguenze negative che possono derivarne agli interessati. In questo quadro devono essere privilegiate modalità tecniche di messa a disposizione dei dati a fini di riutilizzo che consentano di controllare gli accessi a tali dati da parte degli utilizzatori e che impediscano la possibilità di scaricare o di duplicare in maniera massiva e incondizionata le informazioni rese disponibili, nonché l'indiscriminato utilizzo di software o programmi automatici».

[64] V. art. 1, par. 2, lett. *c)* della direttiva (UE) 2019/1024.

[65] V. considerando 54 della direttiva (UE) 2019/1024.

[66] V. art. 1, par. 2, lett. *d)* della direttiva (UE) 2019/1024.

[67] V. art. 6 della direttiva (UE) 2019/1024.

cogliere le opportunità offerte dalle novità oggetto di trasposizione entro il prossimo 17 luglio[68].

Affinché tali opportunità risultino concretamente fruibili nel contesto nazionale, è tuttavia importante che in sede di recepimento siano chiariti alcuni aspetti: il primo sembra costituito dal rapporto esistente tra il riutilizzo e gli strumenti di accesso (documentale e civico) vigenti nel nostro Paese (par. 2); il secondo riguarda il trattamento dei dati personali ai sensi del GDPR (par. 8), che si pone in stretta relazione con la disciplina delle licenze (par. 6) ed i costi recuperabili (par. 7).

Per incrementare il livello di intellegibilità delle norme, così sostenendo l'impegno delle Pubbliche Amministrazioni in particolare regionali in materia di open data, il legislatore dovrebbe cogliere l'occasione per andare oltre alla mera trasposizione letterale della direttiva (UE) 2019/1024. Questa infatti, come sottolineato più volte, è un atto di *armonizzazione minima*, che consente a ciascuno Stato membro di cogliere in fase di trasposizione, ove lo ritenga necessario, le peculiarità dell'ordinamento interno secondo il principio della certezza del diritto a guida dell'attività della PA.

[68] La direttiva (UE) 2019/1024 è inclusa tra gli atti di recepimento mediante la Legge di delegazione europea 2019, A.S. n. 1721, sulla quale si veda il dossier edito dall'Ufficio Studi della Camera e del Senato in *senato.it*, 235-238.

ICT e nuove forme di interazione tra cittadino e Pubblica Amministrazione*

Cristiana Benetazzo

Abstract

Il presente contributo è dedicato all'esame dell'impatto delle tecnologie emergenti sulla Pubblica Amministrazione, alla luce degli atti di riferimento a livello europeo e nazionale nonché delle prime pronunce giurisprudenziali. Sotto il profilo giuridico, l'impiego dell'Intelligenza Artificiale nella pubblica amministrazione pone la necessità di garantire i principi e le garanzie procedimentali, quali l'obbligo di motivazione, e assicurare trasparenza e apertura non solo dei dati, ma anche della logica degli algoritmi e del processo di funzionamento dei servizi. Al riguardo possono rivelarsi particolarmente critici la definizione della titolarità di dati, algoritmi e relative soluzioni di Intelligenza Artificiale nonché l'individuazione delle responsabilità.

This paper focuses on the impact of emerging technologies on public administration, in light of the reference acts at European and national level as well as the first jurisprudential rulings. From a legal point of view, the use of artificial intelligence in public administration poses the need to guarantee procedural principles and guarantees, such as the obligation to motivate, and to ensure transparency and openness not only of data, but also of the logic of algorithms and the process of operating the services. In this regard, the definition of ownership of data, algorithms and related artificial intelligence solutions as well as the identification of responsibilities can be particularly critical.

Sommario

1. Intelligenza Artificiale e globalizzazione: il quadro in ambito pubblico. – 2. Dall'amministrazione digitale alla partecipazione, in forma telematica, ai processi decisionali delle P.A. – 3. (*segue*) Trasparenza e digitalizzazione come misure di prevenzione della corruzione: il caso delle linee guida ANAC. – 4. Considerazioni conclusive: l'uso di algoritmi nel contesto dell'attività decisionale delle Pubbliche Amministrazioni tra rischi ed opportunità.

(*) Il presente contributo rielabora, con alcune integrazioni, l'intervento introduttivo svolto nell'ambito della seconda conferenza dell'Italian Chapter di ICON-S su "Le nuove tecnologie per il diritto pubblico", tenutasi a Firenze il 22-23 novembre 2019. Il contributo è stato sottoposto a referaggio anonimo.

Parole chiave

ICT – Intelligenza Artificiale – informatizzazione – pubblica amministrazione - algoritmi

1. Intelligenza Artificiale e globalizzazione: il quadro in ambito pubblico

Nel pieno di quella che, a ragione, è stata definita la "quarta rivoluzione industriale"[1], il settore delle amministrazioni pubbliche, così come il mondo delle imprese, è attualmente coinvolto da un inarrestabile processo di trasformazione che ha come minimo comun denominatore un alto grado di automazione e di interconnessione che sta esercitando un impatto importante sull'essere umano stesso[2] e sul suo modo di vivere nel proprio ambiente[3]: basti pensare all'utilizzo del *World-wide-web* o all'*Internet of Things* (*IoT*), solo per citare alcuni dei più recenti sviluppi imposti dall'innovazione tecnologica.

Questi fenomeni, di dimensioni ormai globali e tra loro strettamente collegati, rendono sempre più urgente una riflessione sulle ricadute che l'impiego delle ICT[4] produce o è atto a produrre sui processi decisionali delle istituzioni pubbliche, sui meccanismi del mercato, e più in generale, nell'ambito delle relazioni sociali.

Per introdurre questi temi, appare allora fondamentale partire da una premessa di ordine generale sull'attuale contesto in cui la velocità delle telecomunicazioni, la moltiplicazione delle fonti di informazione, l'annullamento delle distanze attraverso la rete e

[1] L'espressione "industria 4.0" è divenuta negli ultimi anni di uso comune. Per un primo inquadramento del fenomeno cfr. P. Lèvy, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, Milano, 1996; J. Rifkin, *La terza rivoluzione industriale: come il "potere laterale" sta trasformando l'energia, l'economia, il mondo*, Milano, 2011; M. Brettel - N. Friederichsen - M. Keller - M. Rosemberg, *How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective, in International Journal of Mechanical, Industrial Science and Engineering*, 8(1), 2014, 37 ss.; G.E. Vigevani – O. Pollicino - C. Melzi d'Eril - M. Cuniberti - M. Bassini, *Diritto dell'informazione e dei media*, Torino, 2019.

[2] Su questi più recenti sviluppi v., senza alcuna pretesa di completezza, O. Pollicino - M. Bassini, *Freedom of Expression and Defamation in Internet*, in J. Trzaskowski - A. Savjn (a cura di), *Research Handbook on EU Internet Law*, London, 2014, 508 ss.; Id., *The Law of the Internet between Globalization and Localization*, in M. Maduro - K. Tuori (a cura di), *Transnational Law - Rethinking European Law and Legal Thinking,* Cambridge, 2014, 347 ss.; O. Pollicino*, The European Judicial Dialogue and the Protection of Fundamental Rights in the New Digital Environment*, *The Case of Freedom of Speech*, in S. Morando-Foadi – L. Vickers (a cura di), *Fundamental Rights in the EU: a matter for two Courts,* London, 2015, 93 ss.; Id., *European Court of Human Rights and Italian Constitutional Court: No 'Groovy Kind of Love*, in K. Siegler (a cura di), *The UK and of European Court of Human Rights - A Strained relationship*, London, 2015, 362 ss.; Id., *The European and Constitutional Implications of the Google v. Vividown Saga*, Oxford, 2015, 227 ss.; A.G. Biuso, *Corporeità, sicurezza e potere in Internet*, in *Lessico di etica pubblica*, 1, 2018, 11 ss.; D.U. Galetta – J.C. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *federalismi.it*, 3, 2019.

[3] Si veda sul punto, in particolare, K. Schwab - P. Pyka, *Die Vierte Industrielle Revolution*, München, 2016; P. Bianchi, *4.0 La nuova rivoluzione industriale*, Bologna, 2018.

[4] Come è noto, la sigla ICT rappresenta l'acronimo di *Information and Communications Technology*, ovvero l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni (tecnologie digitali comprese).

tutti i complessi fenomeni di trasformazione politica, socio-economica e tecnologica[5] riassunti nel riferimento alla c.d. globalizzazione[6], conducono a sempre più evidenti limitazioni della sovranità statale (sul piano interno e su quello esterno), ma anche all'inadeguatezza dei consueti strumenti di partecipazione fondati sulla rappresentanza politica[7].

Così, ci si interroga sulle specifiche risposte che occorre dare a specifici *deficit* democratici (ad esempio, come costruire istituzioni democratiche sovra-nazionali; o come costruire nuove forme di partecipazione dei cittadini ai processi del *policy-making*; o anche come ripensare il ruolo dei partiti politici)[8].

In particolare, al fenomeno sociale e, quindi, anche istituzionale, della "disintermediazione" ossia della tendenza dell'individuo a proporsi sulla ribalta sociale ed istituzionale senza la mediazione (sociale o politica) di soggetti terzi e anzi a rifiutarla si accompagna un vero e proprio "direttismo" (ossia azione diretta) che si esprime attraverso l'ampliamento delle capacità espressive umane reso possibile dalle nuove tecnologie sia di comunicazione e che di azione[9].

---

[5] Sui cui v. la nota 1.

[6] Per un'analisi del fenomeno da parte della dottrina giuridica cfr., anzitutto, S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997. In argomento, cfr., inoltre, le riflessioni B. Caravita, *Il referendum "di indirizzo" del 1989 sui poteri del parlamento europeo* in Id., *Tra crisi e riforme*, Torino, 1993, 87 ss.; G. Azzolini, *Dopo le classi dirigenti. La metamorfosi delle oligarchie nell'età globale*, Bari-Roma, 2017; L. Castellani - A. Rico, *La fine della politica? Tecnocrazia, populismo, multiculturalismo*, Cesena, 2017; A. Morrone, *L'iniziativa popolare propositiva: per una democrazia plebiscitaria contro la democrazia rappresentativa?*, in *federalismi.it*, 23, 2018.

[7] L'inversione di prospettiva nell'analisi del rapporto tra Autorità e libertà si deve anche alle riflessioni di V. Caputi Jambrenghi, *Uffici ed impiegati pubblici dallo Statuto albertino alla Costituzione nei centocinquant'anni di Unità d'Italia (veduta di scorcio)*, in *giustamm.it*, 12, 2011. Per una disamina dell'evoluzione del rapporto tra i due termini del binomio cfr. B.G. Mattarella, *Il rapporto autorità-libertà e il diritto amministrativo europeo*, in *Riv. trim. dir. pubbl.*, 2006, 909 ss. il quale osserva come la maggiore complessità e la frammentazione soggettiva del «momento dell'autorità» (effetto anche della moltiplicazione dei soggetti preposti a livello nazionale, europeo e globale all'esercizio di pubbliche funzioni), in uno con l'affermarsi di modelli non provvedimentali dell'azione amministrativa, rendano l'analisi della dialettica autorità-libertà non più pienamente adeguata al fine di descrivere i tratti fondamentali del diritto amministrativo del XXI secolo. Sulle forme innovative di coinvolgimento popolare, soprattutto a livello di enti locali, di concezione rispettivamente anglosassone o sudamericana, che la dottrina è solita far rientrare negli istituti della democrazia "deliberativa" e "partecipativa cfr., altresì, L. Bobbio, *Dilemmi della democrazia partecipativa*, in *Dem. dir.*, 4, 2006, 14 ss.; R. Bifulco, *Democrazia deliberativa e democrazia partecipativa*, in *astrid–online.it*, 2 ss.; L. Mazzucca, *Democrazia partecipativa e democrazia deliberativa: alcune riflessioni sul modello di Fung e Wright*, Venezia, Università IUAV, 16-18 settembre 2010, XXIV Convegno Sisp, 3 ss. E. Rossi, *Le finalità e gli strumenti della democrazia partecipativa nell'ordinamento giuridico italiano*, in *Dir. soc.*, 3, 2016, 502 ss.

[8] Così, a fronte di tendenze che vedono l'affermarsi di moderne forme di "oligarchia", di potentati economici o tecno-strutture, che svuotano le sedi "tradizionali" della sovranità, la risposta, simmetrica, sembra essere quella di un "ritorno al popolo", ovvero una visione della democrazia che si appella al recupero di un qualche ruolo immediato e diretto dei cittadini. Si noti che mentre la ripresa più recente dei richiami alla "democrazia partecipativa" si produce sull'onda dei movimenti di critica alla globalizzazione, il modello di *participatory democracy* era sorto originariamente nell'ambito dei grandi movimenti giovanili degli anni '60 e, negli USA, in particolare, dalla mobilitazione studentesca contro la guerra nel Vietnam. L'espressione "democrazia partecipativa" è, poi, tornata alla ribalta soprattutto con i movimenti *new global* dei primi anni Duemila. Per una introduzione alle diverse forme e ai diversi istituti della democrazia diretta, con espliciti intenti applicativi, si rinvia a V. Beramendi et al., *Direct democracy. The international Idea Handbook*, IDEA – International Institute for democratic and electoral assistance, Stokholm, 2008.

[9] L'accessibilità di molti mezzi di espressione e di comportamento di tipo *low cost* e la rilocalizzazione

L'immaterialità del contatto sociale in rete, cancellando molti degli elementi tradizionali della "gerarchizzazione" dei rapporti umani, allude (o, forse meglio, «illude» per usare le parole di S. Cassese)[10] ad un azzeramento degli elementi tipici della autorevolezza se non addirittura di quelli dell'Autorità, anche alla luce di una diffusa percezione di egualitarismo[11]. Impensabile, ovviamente, che da tale straordinario processo di cambiamento possa rimanere escluso il mondo del diritto: e non ci si riferisce solo a quello della rappresentanza politica che produce il diritto, ma anche a quello delle Autorità indipendenti con poteri di regolazione, come, ad esempio, l'ANAC[12].

L'introduzione della nuova «Carta della cittadinanza digitale» (art. 1, l. 7 agosto 2015, n. 124)[13] o del c.d. principio del *digital first* (*ex* art. 1, c. 1, lett. *b*, l. 124/2015) contribuiscono a rendere inevitabile la transizione in corso non tanto in relazione alla necessità che il nostro Paese rispetti gli impegni assunti in sede sovranazionale ed europea, quanto per l'inarrestabilità di un processo nel quale si assiste al mutamento delle relazioni sociali per effetto dell'avvento delle nuove potenzialità di internet, già definito

sia digitale che materiale con le stampanti 3D sono espressione ormai tangibile di questa evoluzione "epocale", che interessa trasversalmente ogni tipo di organizzazione e aspetto della società umana: dalle istituzioni governative e pubbliche, ai sistemi d'informazione, fino alle attività che attengono alla sfera personale e privata di ciascun individuo.

[10] Su tale processo evolutivo cfr. S. Cassese, *La partecipazione dei privati alle decisioni pubbliche. Saggio di diritto comparato*, in *Riv. trim. dir. pubbl.*, 2007, 13 ss., secondo cui la partecipazione può essere richiesta «per consentire all'amministrazione una migliore conoscenza dei fatti e degli interessi sui quali essa deve basare le sue scelte»; per permettere al privato di far valere i suoi diritti; per assicurare il coinvolgimento dei privati interessati nel processo decisionale sicché «essa si colloca sul crinale tra i tre principi che reggono i poteri pubblici, quello di autorità (su cui si fonda il potere esecutivo), quello di giustizia (assicurato, di regola, dalle corti), quello di democrazia (a cui provvedono normalmente le assemblee rappresentative)». Sulla partecipazione procedimentale nel nuovo contesto politico-istituzionale cfr. U. Allegretti, *La democrazia partecipativa in Italia e in Europa*, in *Riv. AIC,* 1, 2011; G. Napolitano, *La logica del diritto amministrativo*, Bologna, 2014, 220 ss.

[11] Cfr., A. Sterpa, *Come tenere insieme la "disintermediazione" istituzionale e la rappresentanza della Nazione?*, in *federalismi.it*, 24, 2018, 6.

[12] Per tale ragione si segnalano "spinte" della Corte di giustizia UE e, finanche, delle autorità nazionali di regolazione affinché – ai sensi della direttiva "servizio universale" 2002/22/CE – la connessione ad internet a banda larga da postazione fissa rientri nel catalogo di prestazioni oggetto di obbligo di servizio universale. Per quanto concerne la giurisprudenza della Corte di giustizia, può essere ricordata, ad es., la sentenza 11 giugno 2015, in causa C-1/14, *Base Company e NV Mobistar NV / Ministerraad*, pubblicata in *federalismi.it*, 13, 2015, nella quale si afferma che le tariffe speciali e il meccanismo di finanziamento previsti dalla direttiva "servizio universale" (2002/22/CE) si applicano ai servizi di abbonamento internet che richiedono una connessione in postazione fissa, a prescindere dall'ampiezza di banda, dalla linea trasmissiva e dalla modalità di connessione. La portata innovativa del principio enunciato dalla Corte di giustizia risiede nella riconosciuta possibilità, per gli Stati membri, di considerare legittimamente e da un punto di vista sostanziale l'accesso a internet veloce da postazione fissa come servizio universale nella nozione rilevante ai fini del diritto UE, con ogni conseguenza in termini di legittimità delle misure perequative indispensabili per rendere effettivo il diritto a godere della prestazione. Quanto agli incentivi al ruolo attivo delle *authorities* nella promozione delle nuove tecnologie per il diritto, cfr., ad es., AGCOM, Delibera 253/17/CONS del 27 giugno 2017, che, esercitando la propria funzione consultiva nei confronti del Ministero per lo Sviluppo economico in riferimento alla revisione periodica del contenuto del servizio universale (art. 65 del d.lgs. 259/2003), ha affermato che la connessione ad Internet da postazione fissa a banda larga dovrebbe rientrare tra gli obblighi di servizio universale.

[13] L'art. 1, l. 124/2015, reca la significativa rubrica «Carta della cittadinanza digitale», a voler riassumere il cambio di prospettiva e l'intenzione del legislatore di rafforzare e rendere effettivi i diritti digitali dei cittadini nei confronti delle P.A.

da autorevole dottrina come «uno spazio sociale dilatato, senza precedenti nella storia dell'umanità […], dove si mescolano soggetti e fenomeni diversi, dove i ruoli possono cambiare vorticosamente e molti interessi trovarsi in conflitto»[14] .

L'opportunità di una riflessione sulle ricadute che l'impiego delle ICT produce o è atto a produrre sui processi decisionali, emerge con maggiore evidenza proprio in rapporto alla disciplina dell'amministrazione digitale[15] ovvero quell'insieme di misure innovative introdotte, a partire dai primi documenti strategici promossi a livello europeo all'inizio del nuovo millennio e poi incrementati con l'Agenda Digitale Europea 2020[16], al fine di accelerare il processo di informatizzazione della P.A.[17] Attualmente anche la Pubblica Amministrazione si trova, infatti, già in una quarta fase di evoluzione, collegata alla c.d. Quarta Rivoluzione Industriale. Si tratta, come già accennato, di un'evoluzione monumentale che è connessa, essenzialmente, a due grandi fenomeni: 1) la mutazione esponenziale delle nozioni di spazio e tempo che è derivata dall'uso massiccio di nuove tecnologie dell'informazione e della comunicazione[18]; 2) la trasformazione della maniera di elaborare dati e informazioni attraverso lo svolgimento automatizzato di

---

[14] S. Rodotà, *Il diritto alla conoscenza*, nella Relazione conclusiva al Seminario alla Scuola per Librai tenutosi presso la Fondazione Cini a Venezia, in *scuolalibraiuem.it*.

[15] Cfr. il panel presieduto da E. Carloni, *Il regime del patrimonio informativo pubblico tra decisione algoritmica e dati aperti* (con interventi di E. Carloni, F. Di Porto, M. Falcone, C. Di Francesco Maesa) nonché, con riguardo al tema specifico del diritto sanitario, quello presieduto da M.A. Sandulli, *Innovazione e diritto sanitario* (con interventi di M.A. Sandulli, M. Sinisi, A. Colante, N. Posteraro, F. Aperio Bella), nell'ambito della seconda conferenza dell'Italian Chapter di ICON-S su "Le nuove tecnologie e il futuro del diritto pubblico", tenutasi a Firenze il 22-23 novembre 2019.

[16] Non sembra inutile qui richiamare brevemente l'evoluzione della disciplina giuspubblicistica relativa all'uso delle ICT. I primi passi della strategia comunitaria relativa alla "Società dell'Informazione" risalgono già alla metà degli anni '80, ma riguardano aspetti puntuali e non una strategia complessiva:
- nel 1984 sono state avviate le attività di ricerca e di sviluppo nel settore delle ICT con il programma ESPRIT (tecnologie dell'informazione), seguito nel 1986 dai programmi concernenti le applicazioni telematiche (trasporti, sanità e formazione a distanza) e dal programma RACE (tecnologie avanzate delle telecomunicazioni);
- nel 1987 è stata varata la politica delle telecomunicazioni con il Libro verde sulla liberalizzazione del mercato delle telecomunicazioni;
- nel 1993 è stato pubblicato il Libro bianco della Commissione, intitolato «Crescita, competitività, occupazione», grazie al quale è stata avviata una politica globale in materia di Società dell'Informazione.

È, però, solo all'inizio del nuovo millennio che sono stati approvati dei documenti strategici europei dal carattere unitario e di ampia portata, e che riconoscono nel digitale una leva importantissima per lo sviluppo della società e dell'economia europea.

In particolare, nella prima decade degli anni 2000, sono tre i documenti di *policy* da ricordare:

- eEurope 2002
- eEurope 2005
- i2010

Successivamente, nel marzo 2010, la Commissione Europea ha presentato «Europa 2020 - Una strategia per una crescita intelligente, sostenibile e inclusiva» con l'intento di uscire dalla crisi e di preparare l'economia dell'UE per le sfide del prossimo decennio (cfr. il documento di FormezPA, *L'Agenda Digitale Europea 2020*, reperibile in *egov.formez.it*). In particolare, tra le sette iniziative "faro" della strategia Europa 2020 c'è l'Agenda Digitale Europea che mira a stabilire il ruolo chiave delle ICT per raggiungere gli obiettivi di crescita «intelligente, sostenibile ed inclusiva» che l'Europa si è prefissata per il 2020 (COM (2010) 245 def./2 del 26 agosto 2010, parr. 2.6 e 2.7).

[17] Su cui v. L. Romani, *La strategia "Europa 2020": obiettivi e criticità, con particolare riferimento all'agenda digitale europea e all'interoperabilità dei sistemi informativi delle amministrazioni pubbliche europee*, in *Riv. amm. Rep. it.*, 2010, 573 ss., spec. 585.

[18] Su cui v., più in generale, V. G. Balandier, *Le désordre. Eloge du mouvement*, Paris, 1988.

attività che, prima, potevano essere svolte solo dall'intelligenza umana[19].

2. Dall'amministrazione digitale alla partecipazione, in forma telematica, ai processi decisionali delle P.A.

Un primo importante versante in relazione al quale le ICT determinano una nuova interazione tra cittadino ed amministrazione attiene al profilo della partecipazione ai processi decisionali. Ci si riferisce non tanto agli istituti classici della partecipazione procedimentale *ex lege* 241/1990 quanto ai nuovi strumenti di partecipazione come le reti locali di attivismo civico che nell'ultimo decennio sono nate intorno alla contestazione delle grandi opere infrastrutturali o dei grandi impianti di trattamento dei rifiuti (basti pensare, ad es., al dibattito pubblico per le grandi opere infrastrutturali, disciplinato dall'art. 22 del Codice dei contratti pubblici).

In tale prospettiva, deve esser garantita ai cittadini «la partecipazione con modalità telematiche *ai processi decisionali* delle istituzioni pubbliche»[20], anche attraverso l'utilizzo di forme di consultazione preventiva sugli schemi di atti da adottare, che richiamano il modello americano dei *legislative rules* assoggettati al *notice and comment*.

Esperienze che sembrano procedere in tale direzione sono già riscontrabili, ad esempio, per l'assunzione di talune decisioni in materia ambientale (in base alla Convenzione di *Aarhus* del 1998) e per gli atti di natura regolamentare o a contenuto generale delle *Authorities*, per i quali si prevedono specifici processi di consultazione pubblica «il più possibile inclusivi, trasparenti ed efficaci» tali da poter condurre a «decisioni informate e di qualità»[21].

In questa fase, invero, anche gli indicati meccanismi rappresentativi, volti a presiedere l'azione degli organi titolari dell'attività di indirizzo politico, sembrano regredire di fronte alla necessità di perseguire una rapidità decisionale corrispondente alle dinamiche dell'economia globale e dei condizionamenti politico-giuridici sovranazionali; il che, sul piano organizzatorio, si risolve nella rimessione di interi settori suscettibili di regolazione politica all'Autorità di «poteri tecnici»[22] .

---

[19] Cfr. D.U. Galetta – J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, cit., 3.

[20] V. l'art. 1, c. 1, lett. *c*), l. 124/2015.

[21] Ministero per la Semplificazione e la Pubblica Amministrazione, *Linee guida sulla consultazione pubblica in Italia,* 2017, in *funzionepubblica.gov.it*.

[22] Il fenomeno citato si risolve in una sempre maggiore utilizzazione, da parte governativa, di strumenti atti ad imprimere un orientamento ed un ritmo vincolati all'attività parlamentare; ciò non solo al fine di far acquisire una certa efficacia normativa all'indirizzo politico concordato al momento della votazione della fiducia, ma anche per fronteggiare le sempre più frequenti situazioni in cui l'Esecutivo è chiamato a decidere su questioni tecniche con una rapidità che non può essere raggiunta attraverso l'ordinario strumento dell'iniziativa legislativa ad esso accordata (art. 71 Cost.). Sempre più spesso, dunque, il Parlamento è indotto alla ratifica vincolata di indirizzi precostituiti sulla base della "forza normativa" del fatto compiuto. Nel senso indicato, trovano, quindi, spiegazione le mutazioni subite da istituti quali la decretazione d'urgenza, la delegazione legislativa, la questione di fiducia, che, secondo una tendenza comune a tutti i Paesi dell'area occidentale, conducono all'emersione sul Parlamento di quella che è stata definita la "centralità del Governo o Potere governante". Sul punto, diffusamente, G. Bognetti, *La divisione dei poteri*, Milano, 1991, 91 ss.

Ma la realtà, probabilmente, è più complessa e la questione va collocata nel contesto evolutivo dello Stato di diritto, in una fase storica nella quale il progresso tecnologico costringe a ripensare i fondamenti stessi del diritto pubblico[23].

C'è poi – a modesto avviso di chi scrive – un aspetto ulteriore nel rapporto tra l'innovazione tecnologica che produce "disintermediazione" e il diritto; e questo aspetto va ricercato nell'impatto che quest'ultima genera sull'applicazione delle norme giuridiche. Si tratta di un profilo di analisi che riguarda, in primo luogo, il procedimento di formazione delle norme stesse.

È, del resto, evidente che, se le ICT si offrono naturalmente come strumento privilegiato di conoscenza e di interlocuzione tra cittadino ed amministrazione – costituendo, così, uno straordinario volano per una piena partecipazione ai processi decisionali – l'uso legittimo delle stesse presuppone regole giuridiche sufficientemente dettagliate e certe che garantiscano la correttezza e l'imparzialità nell'acquisizione, valutazione e trattamento dei dati[24].

---

[23] Sul rapporto tra nuove tecnologie e rappresentanza democratica, cfr., *ex multis*, S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997 e L. Castellani - A. Rico, *La fine della politica,* cit.

[24] Sulla crescente rilevanza dei dati (raccolti, trattati e conservati attraverso la rete) non solo nell'ambito della produzione industriale ma anche nel processo decisionale dell'Amministrazione, si rinvia alle osservazioni di F. Costantino, *Autonomia dell'amministrazione e innovazione digitale*, Napoli, 2012, 178 ss.; Id., *L'uso della telematica nella pubblica amministrazione,* in A. Romano (a cura di), *L'azione amministrativa,* Torino, 2016, 242 ss.; Id., *Lampi. Le decisioni delle pubbliche amministrazioni tra open e big data*, Relazione presentata in occasione del convegno indetto dall'Associazione italiana dei professori diritto amministrativo sul tema "Decisioni amministrative e processi deliberativi", tenutosi a Bergamo, nei giorni 5-7 ottobre 2017. Più in particolare, sul rapporto tra decisione amministrativa e nuove tecnologie, cfr. G. Caridi, *Informatica giuridica e procedimenti amministrativi*, Milano, 1983; G. Sartor, *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Bologna 1990; V. Buscema, *Discrezionalità amministrativa e reti neurali artificiali*, in *Foro amm.,* 1993, 620 ss.; A. Masucci, *L'atto amministrativo informatico. Primi lineamenti di una ricostruzione*, Napoli, 1993; Id., voce *Atto amministrativo informatico*, *in Enc. dir.,* Aggiornamento I, Milano, 1997, 221 ss.; G. Terracciano, *L'applicazione in campo giuridico delle reti neurali artificiali. Il programma "GiuriNet",* in *TAR*, 1998, 497 ss.; Id., *Gli agenti software: nuovi soggetti del ciberdiritto*, in *Contratto e impresa* 2002, 465 ss.; Id., *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Dir. inf.*, 2003, 55 ss.; P.L.M. Lucatuorto, *Intelligenza artificiale e diritto: le applicazioni giuridiche dei sistemi esperti*, in *Cyberspazio e diritto,* 2006, 219 ss.; S. Dettori, *Articolo 3 bis. Uso della Telematica*, cit., 173 ss.; G. Duni, *L'amministrazione digitale. Il diritto amministrativo nell'evoluzione telematica,* Milano, 2008, 53 ss.; P.L.M. Lucatuorto - S. Bianchini, *Discrezionalità e contemperamento degli interessi nei processi decisionali dell'Amministrazione digitale*, in *Cyberspazio e diritto,* 2009, 41 ss.; E. D'Orlando, *Profili costituzionali dell'amministrazione digitale,* in *Dir. inf.*, 2011, 213 ss. A. Valastro, *Le garanzie di effettività del diritto di accesso ad Internet e la timidezza del legislatore italiano*, in M. Pietrangelo (a cura di), *Il diritto di accesso ad Internet. Atti della tavola rotonda svolta nell'ambito dell'IGF Italia (Roma*, *30 novembre 2010)*, Napoli, 2011, 45 ss.; L. Cuocolo, *La qualificazione giuridica dell'accesso a Internet*, *tra retoriche globali e dimensione sociale*, in *Pol. dir.*, 2012, 263 ss., spec. 284; S. Civitarese Matteucci - L. Torchia, *La tecnificazione dell'amministrazione,* in Id. (a cura di), *La tecnificazione*, diretto da L. Ferrara - D. Sorace, *A 150 anni dall'unificazione amministrativa italiana. Studi*, vol. IV, Firenze, 2016, 13 ss.; G. Cammarota, *Servizi pubblici on line e partecipazione migliorativa,* in S. Civitarese Matteucci - L. Torchia (a cura di), *La tecnificazione*, cit., 114 ss.; F. Costantini - P.L. Montessoro, *Il problema della sicurezza tra informatica e diritto: una prospettiva emergente dalle "Smart Cars",* in *Inf. dir.*, 2016, 95 ss.; M.L. Maddalena, *La digitalizzazione della vita dell'amministrazione e del processo*, in *Foro amm.*, 2016, 2535 ss.; M. Pietrangelo, *Le pubbliche amministrazioni sul web tra comunicazione, consultazione e partecipazione"*, in S. Civitarese Matteucci - L. Torchia (a cura di), *La tecnificazione*, cit., 103 ss. Per una ricostruzione delle posizioni della dottrina in ordine a sussistenza, qualificazione e fondamento del diritto d'accesso alla rete, cfr. A. Usai, *Le elaborazioni possibili delle informazioni. I limiti alle decisioni amministrative automatiche,* in G. Duni (a cura di), *Dall'informatica amministrativa alla teleamministrazione*, Roma, 1992, 55 ss.; Id., *Le prospettive di automazione delle decisioni amministrative in un sistema di teleamministrazione*, in *Dir. inf.*. 1993, 163 ss.; D. Marongiu,

In tale situazione, il confronto procedimentale con imprese e cittadini, attraverso consultazioni preventive, dovrebbe favorire regole più chiare e comprensibili per gli operatori economici in quanto formate «attraverso percorsi democratici fatti di partecipazione e trasparenza, tali da vincere la illuministica sfiducia verso il sociale al fine di realizzare un reale pluralismo giuridico espressione di una sincera sussidiarietà. Una arena ove la regola nasce da un confronto procedimentale con imprese e cittadini mediante consultazioni preventive»[25].

3. (*segue*) Trasparenza e digitalizzazione come misure di prevenzione della corruzione: il caso delle linee guida ANAC

In questa direzione possono essere letti anche i nuovi obblighi di pubblicazione previsti dal combinato disposto degli artt. 37 del d.lgs. 14 marzo 2013, n. 33 e s.m.i. (c.d. "decreto trasparenza") e dell'art. 29 Codice dei contratti pubblici, che sono intesi a favorire la trasparenza delle procedure di acquisto, anche ai fini di prevenzione della corruzione[26]. In questo senso, la digitalizzazione, in quanto volta a favorire forme di controllo diffuso sul corretto utilizzo delle risorse pubbliche, può essere considerata anche come misura di prevenzione della corruzione.

Per non dire che nelle pieghe di una legislazione amministrativa caotica[27], oggi si insinuano gli stessi processi corruttivi: «per promuovere la legalità e combattere la cor-

L'attività amministrativa automatizzata, Rimini, 2005; P. Otranto, *Internet nell'organizzazione amministrativa. Reti di libertà*, Bari, 2015; Id., *Procedimento amministrativo e nuove tecnologie. Il procedimento amministrativo elettronico ad istanza di parte,* Torino, 2011, spec. 89 ss.; F. Morollo, *Documento elettronico fra* e-government *e* artificial intelligence *(AI),* in *federalismi.it*, *Focus TMT,* 2015, 17-18.

[25] Cfr. S. Licciardello, *Sulle sanzioni a tutela della concorrenza e del mercato. Italia e Francia a confronto*, in *Riv. it. dir. pubbl. comunit.*, 1993, 97 ss.

[26] Nello specifico, non sembra qui inutile ricordare che gli obblighi di pubblicazione concernenti i contratti pubblici a fini di trasparenza si rinvengono dalla lettura combinata di due norme: l'art. 37 del d.lgs. 14 aprile 2013, n. 33, per come modificato dal d.lgs. 25 maggio 2016, n. 97 proprio in tema di obblighi di pubblicità a fini di trasparenza e l'art. 29 del d.lgs. 18 aprile 2016, n. 50 (Codice dei contratti pubblici), come ora modificato dal d.lgs. 19 aprile 2017, n. 56. In particolare, all'art. 29, rubricato «Principi in materia di trasparenza», si deve l'introduzione di nuovi obblighi di pubblicazione che si sono aggiunti a quelli previsti dall'art. 1, c. 32, della legge n. 190/2012, con la previsione della pubblicazione nella sezione "Amministrazione trasparente" di «tutti gli atti delle amministrazioni aggiudicatrici e degli enti aggiudicatori relativi alle procedure per l'affidamento di appalti pubblici di servizi, forniture, lavori e opere, di concorsi pubblici di progettazione, di concorsi di idee e di concessioni». Tuttavia, non avendo la norma chiarito quali fossero realmente gli atti da pubblicare nel rispetto del d.lgs. 33/2013, l'ANAC, con la delibera n. 1310 del 28 dicembre 2016 in *anticorruzione.it*, ha individuato gli atti oggetto di pubblicazione, tra cui, però, figurano gli avvisi di preinformazione, i bandi e gli avvisi di gara, la delibera a contrarre, l'elenco degli atti relativi ad affidamenti diretti o affidamenti *in house*, compresi i provvedimenti di esclusione o di ammissione nonché l'elenco dei verbali di gara.

[27] Inevitabile, quanto al tema delle nuove tecnologie, il riferimento a V. Mancuso, *Intelligenza delle macchine e libertà dell'uomo*, Relazione al convegno "Uomini e macchine", Roma, 30 gennaio 2018, in *vitomancuso.it*, in cui l'Autore conclude: «Sono stato invitato a parlare di "Intelligenza delle macchine e libertà dell'uomo" e io concludo con l'auspicio che le macchine non ci tolgano il caos. È dal caos infatti, come insegnano tutte le antiche cosmogonie, che prende forma la natura, anche la natura umana, la quale, tra tutte le manifestazioni naturali, è la più caotica, e per questo la più libera».

ruzione si innesca una spirale di adempimenti burocratici che aumentano le occasioni di corruzione»[28].

Un esempio paradigmatico è rappresentato proprio dalle linee guida dell'ANAC in un settore sensibile e strategico come quello degli appalti pubblici, in cui le riforme spesso solo annunciate e poco effettive (a partire da trasparenza e semplificazione) evocano solo angosce per cittadini ed imprese. La prima causa di questa situazione è la proliferazione di leggi spesso oscure, parziali, espressione di interessi particolari, di cui sono prime vittime i cittadini e le imprese[29] ma che finiscono per soffocare la stessa amministrazione, vittima a sua volta di questa legislazione ipertrofica, che neanche davanti ai giudici riesce a trovare univoca interpretazione[30].

4. Considerazioni conclusive: l'uso di algoritmi nel contesto dell'attività decisionale delle Pubbliche Amministrazioni tra rischi ed opportunità

Un altro importante campo di applicazione dei sistemi di Intelligenza Artificiale (AI) alle attività della Pubblica Amministrazione attiene ai procedimenti di formazione delle decisioni amministrative.

A partire dallo studio dell'intelligenza umana, sono state sviluppate molteplici e diverse innovazioni tecnologiche basate principalmente sull'utilizzo di algoritmi di apprendimento – oggi prevalentemente utilizzati nel settore privato – per elaborare informazioni e risolvere problemi o prendere decisioni che in precedenza potevano essere prese solo dall'intelligenza umana.

Come autorevolmente sottolineato[31] potremo potenzialmente, essere in presenza di una pietra miliare nello sviluppo del settore pubblico perché, per la prima volta, potrebbe essere avviato un percorso finalizzato ad automatizzare il processo decisionale delle Pubbliche Amministrazioni applicando l'Intelligenza Artificiale a vaste aree di

[28] In tal senso M. Barberis, *Gli infortuni della virtù. Corruzione, democrazia, diritti*, in *Materiali per una storia della cultura giuridica*, 1, 2016, 170 ss.

[29] Non dissimile il punto di vista di G.M. Racca, *Dall'Autorità sui Contratti Pubblici all'Autorità Nazionale Anticorruzione: il cambiamento del sistema*, in *Dir. amm.*, 2015, 345 ss., secondo la quale, tra i fattori che hanno contribuito e contribuiscono alla diffusione della corruzione, spicca indubbiamente quella che è stata definita come «corruzione delle regole», ossia la predisposizione di regole e testi normativi incoerenti o eccessivamente complessi che favorisce l'abuso o lo sviamento rispetto al perseguimento dell'interesse generale. In argomento, cfr., inoltre, G. Melis, *La burocrazia*, Bologna, 1998, 93 ss., ove si ricorda il Rapporto del Comitato di studio sulla prevenzione della corruzione, Comitato nominato dal Presidente della Camera dei Deputati nel 1996, il quale indicava le principali cause dei fenomeni corruttivi nell'ambito dell'amministrazione pubblica italiana. Sul "costo" della corruzione per la collettività, in generale, cfr. L. Hinna, M. Marcantoni, *Corruzione. La tassa più iniqua*, Roma, 2013. Tra i tanti lavori sulla semplificazione che sottolineano tale aspetto v. G. Sciullo (a cura di), *La semplificazione nelle leggi e nell'amministrazione: una nuova stagione*, Bologna, 2008. Le politiche di semplificazione sono centrali anche nell'agenda politica di altri paesi, come dimostra lo studio di C.R. Sunstein, *Semplice. L'arte del governo nel terzo millennio*, Milano, 2013.

[30] Analoghe, sul punto, le considerazioni di S. Licciardello, *Prime note sulla funzione di regolazione dell'ANAC nel nuovo codice degli appalti,* in *federalismi.it*, 16, 2016, 3.

[31] Cfr. D. Urania Galetta, in D. Urania Galetta – J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, cit., 17-18.

attività di *routine*, ripetitive e standardizzate che, dopo tutto, di solito si traducono in un'attività amministrativa senza margine di discrezionalità alcuno.

Certo, non vi è alcun riferimento specifico, all'interno del Codice dell'Amministrazione Digitale[32], all'uso di algoritmi a fini di una successiva automatizzazione delle attività delle Pubbliche Amministrazioni sulla base dell'utilizzo di questi dati. Per ora è, dunque, soprattutto la giurisprudenza amministrativa – ed in particolare la sezione Terza–*bis* del Tar Lazio – ad avere inserito dei consistenti paletti con riguardo alla possibilità di fare ricorso alla c.d. decisione amministrativa algoritmica (ad es., in tema di concorsi pubblici)[33]. Ma va anche segnalato che, presso l'Agenzia per l'Italia Digitale (AGID) è attualmente al lavoro una *task force* sull'Intelligenza Artificiale che ha già prodotto un ampio Libro bianco sull'argomento[34]. Quindi, anche per quanto riguarda il settore della P.A., il percorso di applicazione di sistemi di Intelligenza Artificiale sembra essere ormai ben avviato.

Al di là delle specifiche questioni di tipo tecnico-informatico, che aprono scenari non del tutto rassicuranti anche in rapporto alla tutela della proprietà intellettuale[35], sul

[32] Istituito con il d.lgs. 7 marzo 2005, n. 82, il Codice è stato successivamente modificato e integrato prima con il d.lgs. 22 agosto 2016, n. 179 e poi con il d.lgs. 13 dicembre 2017, n. 217.

[33] Ci si riferisce ad una serie di pronunzie emesse dalla sezione terza-*bis* del Tar Lazio nel settembre 2018 relative a provvedimenti di trasferimento di sede e assegnazioni di docenti delle scuole pubbliche assunti sulla base del piano straordinario di cui alla l. 13 luglio 2015, n. 107. In tali occasioni, il Tar ha accolto i rilievi formulati dai ricorrenti, che lamentavano, in particolare, lo svolgimento di attività provvedimentale senza la previa attività istruttoria e procedimentale avendo l'algoritmo asseritamente «sostituito l'istruttoria commessa ad un ufficio e ad un responsabile». In accoglimento delle suddette censure, il Tar Lazio ha, inoltre, rilevato come 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 e che pertanto, al fine di assicurare l'osservanza degli istituti di partecipazione, di interlocuzione procedimentale, di acquisizione degli apporti collaborativi del privato e degli interessi coinvolti nel procedimento, deve seguitare ad essere il dominus del procedimento stesso, all'uopo dominando le stesse procedure informatiche predisposte in funzione servente e alle quali va dunque riservato tutt'oggi un ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo». Secondo il collegio osterebbe, infatti, alla «dismissione delle redini della funzione istruttoria e di abdicazione a quella provvedimentale, il presidio costituito dal baluardo dei valori costituzionali scolpiti negli artt. 3, 24, 97 della Costituzione oltre che all'art. 6 della Convenzione europea dei diritti dell'uomo»: in questo senso, v., ad es., Tar Lazio, Roma, sez. III-*bis*, 10 settembre 2018 n. 9224. In senso analogo, v. le sentenze del medesimo collegio, e di pari data, da 9225 a 9230/2018; nonché la più recente sentenza 9 novembre 2018, n. 10828, tutte consultabili in *giustizia-amministrativa.it*.

[34] Il 7 settembre 2017 si è, infatti, riunita presso l'Agenzia per l'Italia digitale (AGid) la *task force* sull'intelligenza digitale a servizio del cittadino. Più recentemente, il Dipartimento della funzione pubblica (Ministero della P.A.) ha promosso, nell'ambito del PON Governance e Capacità Istituzionale 2014-2020, il progetto intitolato «Competenze digitali per la PA», che punta ad accelerare i processi di trasformazione digitale della PA e a migliorarne i servizi, consentendo a tutti i dipendenti pubblici di poter accedere a piani formativi personalizzati per accrescere le proprie competenze in ambito digitale. In prima stesura, il syllabus è stato realizzato grazie ad un gruppo di lavoro, costituito da esperti di formazione e competenze digitali, istituito presso il Dipartimento della funzione pubblica e definisce l'insieme di conoscenze e abilità digitali considerate chiave per la Pubblica Amministrazione, quali ad esempio: la gestione di dati e informazioni, la sicurezza, i servizi on line, la comunicazione, la conoscenza di tecnologie emergenti.

[35] In questo senso, risultano emblematici due casi, risalenti al 2017, nei quali il Tar Lazio ha chiarito la natura del documento amministrativo elettronico e la portata del diritto di accesso ai sensi della legge n. 241/1990 con riferimento al codice sorgente di un algoritmo compilato da una *software house* su richiesta

piano del diritto amministrativo credo sia essenziale definire, anzitutto, quale spazio debba essere riservato all'intervento umano in questo contesto, al fine di garantire la supervisione dei risultati da parte di un "funzionario persona fisica"[36]. A parere di chi scrive, non è, infatti, immaginabile sostituire con un algoritmo la figura del funzionario responsabile del procedimento[37]: piuttosto, è viceversa certamente possibile immaginare che il funzionario responsabile del procedimento si serva utilmente dei sistemi di Intelligenza Artificiale per potere svolgere più rapidamente, e con maggiore precisione, attività della fase istruttoria[38].

Vista in questa prospettiva, l'automazione basata sull'utilizzo di sistemi di Intelligenza Artificiale rappresenta certamente un vantaggio per il funzionario amministrativo, nella misura in cui può consentirgli di ridurrei tempi e gli errori della fase istruttoria; «tuttavia, nonostante il supporto fornito nella gestione ed elaborazione di dati e informazioni, non è certo l'algoritmo a potere valutare gli esiti della frase istruttoria e/o a potere prendere la decisione in modo autonomo ed indipendente: poiché i sistemi di Intelligenza Artificiale non possono in alcun modo sostituire le competenze e le responsabilità del funzionario amministrativo persona fisica»[39]. Questo è un punto fermo che appare imprescindibile nello sviluppo delle possibili applicazioni dell'Intel-

della Pubblica Amministrazione. I casi in questione (Tar Lazio, 21 marzo 2017, n. 3742, in *Foro amm.,* 2017, 741 e Id., 22 marzo 2017, n. 3769, in *giustizia-amministrativa.it*), sono stati promossi da numerosi sindacati italiani contro il MIUR allo scopo di ottenere l'accesso al codice sorgente dell'algoritmo utilizzato dal MIUR per gestire la delocalizzazione territoriale dei professori di scuola nell'ambito delle procedure di mobilità. Sotto tale profilo appaiono particolarmente rilevanti i chiarimenti forniti dal Tar nella prospettiva delle valutazioni di una *industry* tecnologica: secondo il Tar, la protezione del *copyright* del *software* (che comprende anche il codice sorgente) non è argomento tale da escludere il diritto di accesso appunto al codice sorgente dell'algoritmo. Nel caso in questione, l'algoritmo è un *software* creato per uno scopo specifico della Pubblica Amministrazione e, in assenza di indicazioni contrarie nel contratto tra PA e *software house*, si può presumere che la *software house* abbia trasferito alla PA tutti i diritti di sfruttamento economico dell'algoritmo. Ne consegue che la natura del lavoro creativo dell'algoritmo non dovrebbe interferire con il diritto di accesso ai procedimenti amministrativi delle parti interessate, poiché il diritto di accesso non pregiudica il diritto allo sfruttamento della proprietà intellettuale sul *software*. A di là della specificità del caso concreto, a parere di scrive, restano ancora da approfondire gli aspetti di equilibrio tra il diritto di accesso al codice sorgente del *software* e la protezione ai sensi della legge sul copyright dello stesso codice sorgente, tenendo conto in particolare di possibili casi futuri in cui la PA dovesse avvalersi di algoritmi: 1) non specificamente sviluppati per un singolo procedimento amministrativo (presupponendo un trasferimento completo dei diritti di proprietà intellettuale) e/o 2) basato su tecnologie più sofisticate concesse in licenza alla PA nell'ambito di un regime proprietario. Il rischio evidente è che le grandi *industries* tecnologiche possano valutare come eccessivamente "rischioso" per la tutela della loro proprietà intellettuale concedere in licenza il proprio *software* ad una PA in Italia, sapendo che questo potrebbe comportare l'accesso al codice sorgente del loro *software*.

[36] Cfr. Tar Lazio, Roma, sez. III-*bis*, sent. 9224/2018, cit.

[37] Sulla figura del responsabile del procedimento v. G. Banterle - A. Travi, *L. 7 agosto 1990, n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. Capo II - Responsabile del procedimento. Commento all' art. 4*, in *Le Nuove leggi civili commentate*, 1, 1995, 21 ss.; F. Patroni Griffi, *La l. 7 agosto 1990, n. 241 a due anni dall' entrata in vigore. Termini e responsabile del procedimento: partecipazione procedimentale*, in *Il Foro it.*, 2, 1993, 65 ss.

[38] Sul punto cfr. quanto già osservato in 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, spec. par. 4.3 nonché D.U. Galetta – J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, cit., 19 ss.

[39] Così D.U. Galetta – J.G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, cit., 20.

ligenza Artificiale alle attività decisionali della P.A.

Dalla prospettiva del giuspubblicista l'approccio deve, dunque, essere diverso, da quello – quasi mai neutro – seguito quando si affrontano i temi dell'Intelligenza Artificiale, laddove di volta in volta prevale o la paura (che dei robot aumentino il livello disoccupazione, assumano il controllo della nostra vita, del mondo etc.), ovvero l'eccessivo entusiasmo/ottimismo (l'uso dell'Intelligenza Artificiale che può gestire i *Big Data* e consentirci di ottimizzare qualunque attività)[40]. Occorre cioè ragionare sul se (ed in che termini) l'uso dell'Intelligenza Artificiale e, più in generale, l'uso delle ICT più innovative nel settore pubblico possa rappresentare un fattore che contribuisce all'interesse pubblico in termini di sviluppo sostenibile e maggiore benessere della collettività[41]; e ciò in un contesto di azione amministrativa caratterizzato dall'esistenza di un diritto ad una buona amministrazione (sancito nell'articolo 41 Carta dei diritti fondamentali dell'UE), che non lascia facile spazio a determinismi algoritmici[42].

È questo il tempo nel quale il giurista è chiamato a riflettere in una prospettiva duplice: da un lato volta al presente, e perciò allo studio e all'interpretazione delle utilizzazioni attuali e potenziali delle tecniche e degli strumenti informatici, «in funzione di decisioni amministrative sempre più effettivamente partecipate e condivise dai cittadini; dall'altro proiettata verso un futuro dell'amministrazione che ai più pare tuttora avveniristico, ma che non può sorprenderci né coglierci impreparati»[43].

È necessario, perciò, che si approntino regole giuridiche ed etiche idonee a scongiurare esiti non desiderabili delle nuove tecnologie, senza vivere il futuro con il costante timore che «una volta aperto, sia poi difficile richiudere il vaso di Pandora»[44].

---

[40] Emblematico, a questo proposito, è il saggio di R. Kurzweil, *The Singularity Is Near: When Humans Transcend Biology*, New York, 2006, che ha suscitato (e tuttora suscita) ampio dibattito e reazioni opposte fra gli "addetti ai lavori" dell'Intelligenza Artificiale.

[41] Cfr. Resolution adopted by the General Assembly on 20 December 2017 [on the report of the Second Committee (A/72/422/Add.2)], in *un.org* (06.01.2019).

[42] Cfr., in tal senso, D.U. Galetta, *Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedimentali nei confronti della Pubblica Amministrazione*, in *Riv. It. Dir. Pubbl. Comunit.*, n. 3/2005, 819 ss.e, più recentemente, D.U. Galetta - B. Grzeszick, *Kommentar zu Art. 41 Grundrechtecharta*, in K. Stern/M. Sachs (a cura di), *Europäische Grundrechtecharta. Kölner Gemeinschafts-Kommentar*, Köln, 2016, 618 ss.

[43] Come assai efficacemente sottolineato da P. Otranto, *Decisione amministrativa e digitalizzazione della p.a.*, in *federalismi.it*, 2, 2018.

[44] Cfr. il documento *An Open Letter to the United Nations Convention on Certain Conventional Weapons* del 21 agosto 2017, sottoscritto da 116 fondatori di aziende di robotica e Intelligenza Artificiale.

Note a sentenza

Sezione Italia

"*Res telematica*". La problematica corporeità del *file* ed il reato di appropriazione indebita

Maurizio Fumo

Corte di Cassazione, sez. II penale, 7 novembre 2019, n. 11959

Il dipendente a cui è affidato un computer aziendale che, dopo aver effettuato una copia personale dei dati informatici ivi contenuti, lo restituisce all'azienda "formattato" e dunque privo di tali dati pone in essere una condotta che integra il reato di appropriazione indebita. Alla luce di un'interpretazione evolutiva, infatti, il dato informatico rientra nella nozione di "cosa mobile" contenuta nell'art. 646 c.p.: un file ha una dimensione fisica costituita dalla grandezza dei dati che lo compongono, possiede un valore patrimoniale ed è inoltre suscettibile di essere trasferito da un luogo ad un altro. Pertanto, analogamente al caso del denaro, il dato informatico deve essere considerato quale una cosa mobile anche se in concreto manca il requisito della fisicità della sua detenzione.

Sommario

1. La sentenza. – 2. Che cosa è una "cosa". – 3. Parole, concetti, valori. – 4. *Visibilia et invisibila*. – 5. (inevitabili) funambolismi giurisprudenziali.

Keywords

diritto penale – file – informatica giuridica – reati informatici – cosa

1. La sentenza

La seconda sezione penale della Corte di Cassazione, con la sentenza n. 11959, depositata il 10 aprile 2020 (udienza del 7 novembre 2019), ha affermato il principio in base al quale costituisce appropriazione indebita la definitiva sottrazione di dati informatici o *file,* mediante copiatura da un PC aziendale (di cui l'imputato aveva il possesso per motivi di lavoro) e la immediata, successiva cancellazione degli stessi dalla memoria del predetto computer (restituito al datore di lavoro con l'*hard disk* formattato). Ciò, in quanto i dati informatici possono essere definititi "cose mobili" ai sensi dell'art. 624, c. 2, c.p.[1]

[1] Per una prima riflessione sulla sentenza che si commenta, si possono scorrere alcuni articoli *on line*,

Il ragionamento che la Corte sviluppa è lungo e articolato (e non sempre lineare). Esso prende le mosse dalla ricognizione della precedente giurisprudenza, ricordando l'indirizzo prevalentemente negativo e l'unico precedente positivo (sezione quinta, sentenza n. 32383/2015). I giudici di legittimità rilevano come lo stesso art. 624 c.p. consideri "agli effetti della legge penale" cosa mobile anche l'energia elettrica e ogni altra energia che abbia un valore economico; essi poi osservano, sotto altro verso, che, per quel che riguarda la sottrazione di denaro, non si è mai dubitato che essa possa avvenire senza riferimento alla "dimensione fisica" (le banconote), ma anche mediante operazioni bancarie o artifici telematici.

Molto si spende la Corte nella ricerca di un'accezione di "cosa mobile" che sia compatibile con (*scil:* che possa includere) la realtà telematica, osservando che nel concetto di "cosa" sembra implicita la dimensione della fisicità strutturale e le conseguenti possibilità di misurarne le dimensioni e di realizzarne il trasferimento "fisico" da un luogo all'altro. A prima vista, queste sembrerebbero caratteristiche non rinvenibili in un *file*. Da qui problemi di legalità e tassatività circa la estensione del concetto di "cosa mobile" e - conseguentemente - di applicabilità, nel caso in esame, dell'art. 646 c.p. (e, più in generale, della possibilità di inquadrare le condotte di sottrazione di *file* e di altre *res* telematiche nella categoria dei delitti contro il patrimonio).

Fatta questa premessa, i giudici di legittimità osservano tuttavia che i dati informatici occupano una porzione di memoria nell'elaboratore. Non si può dunque negare ad essi una "dimensione fisica", anche se non percepibile sensorialmente. Insomma il *file* è misurabile (a seconda della porzione di memoria che impegna), anche se non visibile e/o tangibile.

Resta il problema della tassatività e determinatezza[2] che deve caratterizzare il precetto penale, problema che la seconda sezione affronta e supera con il conforto di numerose pronunzie della Corte costituzionale, osservando, sulla base di esse, che, quando il legislatore penale, nella descrizione di una fattispecie, fa riferimento ad altre fonti giuridiche o al linguaggio comune, non viola il principio di legalità, anche se la fonte sia stata innovata o la le parole abbiano subìto la loro naturale evoluzione, che può anche aver dato luogo a un ampliamento del loro campo semantico, purché rimangano fermi ed intellegibili "gli estremi costitutivi della fattispecie" (Corte cost., n. 414/1995).

2. Che cosa è una "cosa"

La pronunzia della seconda sezione riveste indubbiamente notevole rilievo perché sviluppa una articolata riflessione in ordine a una problematica che non può più esse-

tra i quali: F. Corona, *Appropriazione indebita, i files sono qualificabili come cose mobili*, in *Altalex,* 30 aprile 2020; R. Talarico, *La configurabilità del reato di appropriazione indebita di file informatici,* in *diritto.it,* 11 maggio 2020; *Sottrazione di files aziendali da parte del dipendente: è appropriazione indebita,* articolo redazionale, in *lavoroediritto.it,* 5 maggio 2020.

[2] Come è noto, sul punto, la dottrina è sterminata, di talché qualsiasi citazione risulterebbe incompleta e ingiustamente discriminatoria. Semplicemente, tra i più incisivi scritti in merito, si possono ricordare: L. Ferrajoli, *Diritto e ragione: teoria del garantismo penale,* Bari, 2000; F.C. Palazzo, *Introduzione ai principi del diritto penale,* Torino, 1999; F. Mantovani, *Diritto penale,* Padova, 2001.

re ignorata o elusa (e che di fatto da tempo impegna la giurisprudenza e la dottrina): quella dell'adattamento di categorie giuridiche e di schemi logici preesistenti alla realtà informatica, al *novum* che, ormai da non pochi anni, ha prepotentemente cambiato il mondo della comunicazione e, di riflesso, i rapporti interpersonali ed interistituzionali.[3]

Ma se la conclusione cui la Corte perviene ci sembra del tutto condivisibile, qualche perplessità desta il percorso argomentativo che la sentenza esibisce.

Invero detto percorso si può così sintetizzare: *a)* l'appropriazione indebita si esercita sulla cosa mobile altrui, *b)* la "cosa" è sempre e solo una realtà fisica, cui, per volontà del legislatore penale, è equiparata l'energia elettrica e qualsiasi altra energia che abbia un valore economico, *c)* il *file*, anche se non si vede e non si tocca, ha una sua fisicità perché occupa uno spazio all'interno di un elaboratore, *d)* il *file* deve ritenersi sottratto solo quando l'agente, dopo averlo abusivamente copiato, distrugga la versione sulla quale ha eseguito la copia, perché in ciò consiste, nel caso di specie, il requisito dello spossessamento in danno della vittima del reato.

Ebbene, il punto sub *b)* – e il conseguente "rimedio" sub *c)* – non appaiono convincenti.

L'art. 812 c.c. pone la *summa divisio* tra beni immobili e beni mobili e, dopo aver definito i primi, afferma, al terzo comma, "sono mobili tutti gli altri beni". I beni mobili vengono quindi individuati per residualità; in tal modo nessun bene resta inclassificato. Questo *horror vacui* del legislatore ha ovviamente una sua spiegazione razionale: non lasciare senza copertura giuridica le "cose" (usa esattamente questo termine l'art. 810 c.c.) che possano "formare oggetto di diritti".

Dunque le cose (mobili ed immobili) vanno considerate beni quando potenzialmente su di esse qualcuno possa accampare ed esercitare diritti. Ma cosa sia una cosa il codice non lo chiarisce e, dunque, non afferma affatto che sia "cosa" solo la *res extensa* di cartesiana memoria.

Vale la pena di osservare che la *divisio rerum* per il maturo diritto romano si articolava in res *corporales* e *incorporales*, le prime essendo quelle che *tangi possunt*, le seconde quelle che *tangi non possunt*. Il tatto era, pertanto, il senso privilegiato perché la corporeità era solo delle cose che si possono toccare. E tra le cose intangibili (e quindi incorporali) Gaio enumerava l'eredità, l'usufrutto, le obbligazioni[4]; dunque non solo diritti, ma anche *universitates juris*, comprendenti diritti e cose (corporali), unitariamente considerati.

La dottrina più recente[5] ha poi sostenuto che, nel vigente ordinamento, il concetto giuridico di cosa si estende anche alle «altre entità giuridiche che non si possono annoverare tra le cose corporali» e che «cose in senso giuridico sono quegli oggetti che,

---

[3] Al proposito, tra le non poche pubblicazioni, ci piace segnalare E. Giannantonio, *Manuale di diritto dell'informatica*, Milano, 1994; D. Obizzi, *I reati commessi su internet: computer crimes e cybercrimes*, in *fog.it*; S. Seminara; *La responsabilità penale degli operatori su internet*, in *Diritto dell'informazione e dell'informatica,* 1998, 745 ss.

[4] G. Astuti, *Cosa in senso giuridico, Diritto romano e intermedio*, in *Enciclopedia del diritto*, vol. XI, Milano, 1967, 5.

[5] B. Biondi, *Corso di istituzioni di diritto romano*, Milano, 1934, 24.

nell'esperienza e nel linguaggio comuni, si designano con quel sostantivo, purché presentino una rilevanza per il diritto, e le energie naturali captate dall'uomo»[6].
Ed è questo il punto: l'esperienza e il linguaggio.
Ed il *file*, in base al linguaggio odierno e, ancor più, all'esperienza contemporanea, può essere definito un bene, cioè una cosa in senso giuridico, ad onta della sua sfuggente corporeità?

3. Parole, concetti, valori

Per rispondere a tale domanda la Corte di legittimità si avventura per una strada lunga e non del tutto rettilinea, punteggiata di citazioni della giurisprudenza costituzionale, che non sempre appaiono in linea con il percorso scelto. Infatti le sentenze evocate si esprimono, non solo sul principio di tassatività, che, come è noto, si risolve nel divieto – per il giudice penale – di «estendere la disciplina delle norme incriminatrici oltre i casi in esse espressamente previsti»,[7] ma anche (e principalmente) sul principio di determinatezza, che riguarda innanzitutto il legislatore e di riflesso l'interprete, in base al quale le norme incriminatrici devono essere formulate in maniera quanto più è possibile netta ed inequivoca, con la precisa descrizione della condotta vietata.
Fatta questa (non breve) premessa, la seconda sezione va alla ricerca degli "indicatori di corporeità" del *file*, che, come premesso, individua nel fatto che esso occupa spazio nella memoria informatica, cosa che, conseguentemente, lo rende misurabile, anche se non si può né vedere, né – tantomeno – toccare. Dunque una nuova corporeità, una corporeità non tattile (che, per tanto, non avrebbe incontrato il favore di Gaio).
Ma, a tal punto, la lunga premessa "costituzionale" non ha grande incidenza sulle conclusioni cui giunge l'estensore. Se comunque il *file* è connotato da "fisicità strutturale", tanto per esprimersi come la Corte, allora esso rientra pacificamente nel novero degli oggetti sui quali solo (secondo la sentenza) si può esercitare l'apprensione ai sensi dell'art. 646 c.p.
E tuttavia, a nostro parere, ritenere che il *file* o un qualsiasi dato informatico sia un oggetto fisico, sia pure *sui generis*, rappresenta un'affermazione arbitraria e, secondo noi, non corretta. Né la "misurabilità" del *file* può essere considerata sintomo della sua corporeità, atteso che si misura la distanza intercorrente, appunto, tra due corpi; ma il problema, nel nostro caso, sono i corpi, non la loro distanza. Il quesito è che cosa esprime la misura (*rectius:* la dimensione) di un *file*? In sintesi: un *file* ha una dimensione, ma non ha un corpo, inteso in senso tradizionale. La sua misurabilità è tutta interna al sistema informatico. Il fatto è che la misura è un concetto di relazione, non una prova di esistenza. Essa presuppone l'esistenza di un qualcosa che, appunto, ha una estensione. E non si esce da questo rompicapo se non si ammette che i dati informatici sono altro rispetto a una *res extensa*.
Che cosa sia ontologicamente un *file* non è facile a dirsi (ammesso che sia utile). Il

[6] S. Pugliatti, *Cosa (teoria generale)*, in *Enciclopedia del diritto*, vol. XI, Milano, 1967, 35.

[7] Tra i tanti, N. D'Agnese, *Manuale di diritto penale,* Parte generale, Napoli, 2019, 75.

fatto è che la realtà informatica fuoriesce dagli schemi che, fino a qualche tempo fa, sembravano stabili, se non immutabili, costituendo un *tertium genus* tra il corporeo e l'incorporeo, di cui, a volte, si è accorto il legislatore; più spesso se ne sono dovuti occupare la dottrina[8] e la giurisprudenza.

A titolo di mero esempio, in campo penale, può essere ricordato l'art. 491-*bis* c.p., relativo ai documenti informatici, equiparati in tutto e per tutto a quelli cartacei. Ed è istruttivo seguire, al proposito, la evoluzione della norma, atteso che, in una prima versione, introdotta dalla legge n. 547/1993[9], il documento informatico veniva identificato col suo supporto «contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». Ebbene, con successivi interventi legislativi (da ultimo il d.lgs. 7/2016, art. 2, c. 1, lett. *a*), il testo è stato riformulato ed è scomparso qualsiasi riferimento al supporto, vale a dire alla dimensione fisica del documento, che dunque "vive" nella memoria dell'elaboratore in attesa di una sua (eventuale) epifania cartacea. Il diritto penale dunque reprime anche le falsità in atti relative a "scritture incorporee". Sarebbe allora scandaloso ipotizzare che esso sia applicabile anche nel caso di indebita appropriazione di tali dati?

Si diceva prima (e qui sì che la giurisprudenza costituzionale citata in sentenza può giocare un suo ruolo chiarificatore) che la norma, anche quella incriminatrice, opera rinvio, nella sua parte descrittiva, tanto alla esperienza, quanto al linguaggio che la rispecchia. Invero, nel descrivere una condotta, il legislatore può far riferimento sia ad «elementi normativi giuridici che richiamano altre norme giuridiche ben individuabili e determinate nel loro contenuto [sia ad] elementi elastici: elementi non astrattamente tipizzati a priori dal legislatore, che esprimono una realtà quantitativa o temporale abbastanza circoscritta»[10].

In fin dei conti, le norme sono fatte di parole e le parole esprimono concetti, descrivono fatti e situazioni, incorporano valori. Il rapporto tra norma giuridica e linguaggio è dunque stretto, anzi consustanziale e ciò pone il problema del mutamento del significato delle parole, mutamento che si può anche esprimere in un ampliamento o una riduzione dei campi semantici o in un loro stravolgimento. E su ciò incide l'esperienza: comune, scientifica e tecnica.

E qui bisogna operare una distinzione. Una cosa è il mutamento della percezione sociale di un concetto, come nell'abusato esempio del comune senso del pudore, altra cosa è ciò che si è appena definito "ampliamento del campo semantico" di una parola, ampliamento che, sempre più frequentemente, avviene in conseguenza dei mutamenti che la tecnologia apporta nella vita di tutti i giorni. Ad esempio, fino ad una certa epoca, con il termine "spettacolo", si intendeva il teatro, l'opera lirica, il circo ecc.

---

[8] In merito, vedasi, tra i molti scritti: L. Luparia, *Le scienze penalistiche nella tempesta digitale. Quali approdi?,* in *Archivio penale*, 3, 2013, 877 ss.; C. Pecorella, *Profili penali delle truffe on line,* in *Archivio penale,* 3, 2013, 799 ss.; V. Spinosa, *La prima sentenza delle Sezioni unite sui reati informatici. Interpretazione estensiva di permanenza abusiva nel sistema*, in *Indice penale*, 2013, 121 ss.; ci sia infine consentito di citare anche: M. Fumo*, La condotta nei reati informatici*, in *Archivio penale,* 3, 2013, 771 ss.

[9] L'art. 491-*bis* è stato introdotto dalla l. 547/1993, quindi riscritto nel 2008 (l. 48/2008 di ratifica della convenzione di Budapest sulla criminalità informatica); esso ha assunto l'attuale struttura a seguito del ricordato d.lgs. 7/2016.

[10] N. D'Agnese, *Manuale di diritto penale,* cit.

Successivamente il medesimo termine ha incluso il cinema, la televisione e tutto un mondo di immagini variamente veicolate. Siamo quindi di fronte a una sorta di rinvio, non recettizio, ma dinamico, che segue da vicino l'evoluzione della lingua, specchio fedele della società.

Il progresso scientifico-tecnologico ha, dunque, "allargato" il vocabolario.

Di tanto si è resa conto per tempo – come giustamente nota il giudice di legittimità – la Corte costituzionale che già dagli anni '60 riteneva compatibile, entro certi limiti, una descrizione della fattispecie penale non completamente dettagliata, nella quale potevano trovare ospitalità anche espressioni «indicative, esemplificative, estensive»[11], ovvero riteneva non incompatibile con la struttura della norma penale il rinvio a nozioni «proprie dell'intelligenza comune»[12].

Cosi, ad esempio, accanto a norme quali quelle degli artt. 644 o 416-*bis* c.p. che definiscono la soglia oltre la quale gli interessi devono considerarsi usurari o le caratteristiche che una struttura criminale deve avere per essere considerata mafiosa, coesistono fattispecie come quelle di cui agli artt. 423, 428 e 613-*bis* del medesimo codice che non specificano che cosa debba intendersi per incendio, per naufragio o per tortura, affidandosi alla comune accezione ed al significato "sociale" del termine. E, mentre un incendio o un naufragio sono tali oggi come nell'antichità, il concetto di tortura può ampliarsi anche in ragione della "scoperta" ed adozione di nuovi e più raffinati strumenti o metodi per indurre sofferenza.

Con l'avanzare degli anni e con il trionfo delle tecnologia, il giudice delle leggi si è ancora di più espresso in relazione alla ammissibilità di norme "aperte", che tengano cioè conto dei rapidi e continui progressi in tal campo[13], così "salvando" i principi di tassatività e determinatezza con riferimento al diritto vivente e all'ovvia metodica della interpretazione sistematica, integrata e teleologica, in base alla quale vocaboli polisensi, espressioni sommarie, concetti elastici acquistano (maggior) concretezza e precisione[14].

Il fatto è che la legge penale, nel rinviare al linguaggio comune o tecnico, più che alla specie, finisce per far riferimento al genere (le armi, la sostanza stupefacente ecc.). Conseguentemente, quando interviene un mutamento tecnico-scientifico, che arricchisce quel genere di una nuova specie (la realizzazione di un'arma di diverso tipo, l'immissione sul mercato di una droga, fino ad allora sconosciuta ecc.), la "copertura normativa" del *novum* non sembra porsi in contrapposizione con i ricordati principi di determinatezza e tassatività.

È da chiedersi tuttavia se tale "meccanismo di inclusione" possa essere accettato anche quando il genere di riferimento ha un carattere quasi "ecumenico", come nell'ipotesi in cui il testo normativo si riferisca alle "cose" o ai "beni". Invero "cosa" è nome comune (e generico), il cui significato muta a seconda del contesto comunicativo nel quale è inserito; e dunque si va dalla kantiana *Ding an sich,* la cosa in sé, il *noumeno,*

[11] Corte cost., 27 maggio 1961, n. 27.

[12] Corte cost., 16 dicembre 1970, n. 191, relativa a pubblicazioni e spettacoli osceni.

[13] Corte cost., 1° agosto 2008, n. 327, in tema di crollo di costruzioni e altri disastri dolosi.

[14] Cfr. Corte cost., 27 febbraio 2019, n. 25; 11 giugno 2014, n. 172; 23 luglio 2010, n. 282; 30 gennaio 2009, n. 21, tutte citate nella sentenza che qui si commenta.

all'uomo misura di tutte le cose, alle cose di tutti i giorni, fino a "cosa nostra". E tuttavia, in un panorama pur tanto vasto, restringendo l'accezione al campo del diritto, si può senza dubbio dire, in base ai testi normativi civilistici che si sono prima citati, che "cosa" è una componente del mondo esterno, atta a un vantaggioso utilizzo, che possa essere oggetto di appropriazione (ecco!) da parte dell'uomo. In sintesi: cosa come un *quid* rilevante giuridicamente, che, presentando un profilo di utilità, può essere definita, in senso giuridico, "un bene"[15].

E allora, nel nostro caso, la questione si riduce alla domanda se il *file*, connotato come è dalla sua natura equivoca tra corporeità e incorporeità, possa essere definito "cosa", non in base a quello che a noi sembra un paralogismo, vale a dire l'ancoraggio della sua pretesa corporeità alla misurabilità, ma in base alla ricordata "apertura" della norma che consente all'interprete – senza violare alcun *tabù* costituzionale – di prendere atto dell'implicito ampliamento semantico (conseguente all'evoluzione tecnologica) del termine "cosa", come utilizzato dal diritto penale.

D'altronde, lo stesso legislatore, includendo tra le cose mobili l'energia, ha dato una chiara indicazione nel senso del superamento di una concezione decisamente arcaica dei beni e delle cose, mentre, sotto altro verso, la giurisprudenza non ha dubitato che ci si potesse appropriare di "cose" come l'acqua corrente, non certo immateriale, ma – come del resto il denaro – mutevole nella sua concreta identificazione.[16]

4. *Visibilia et invisibilia*

Orbene, in base ad una rapida (e sommaria) ricognizione della giurisprudenza, si può affermare che, da tempo, è stato superato il limite dalla stretta corporeità quando si è trattato di affrontare casi legati alla c.d. criminalità informatica ed è stata proclamata, *apertis verbis*, la inclusione dei dati informatici tra le cose in senso giuridico.

Può innanzitutto essere ricordata la equiparazione del giornale *on line* al giornale cartaceo ad opera delle Sezioni unite nel 2015 (sentenza n. 31022), per negarne la sequestrabilità, alla luce della estensione della normativa sulla stampa tradizionale. Ma ancora maggior rilievo ha la medesima sentenza nella parte in cui si occupa, viceversa, del sequestro di un semplice sito *web* (non equiparabile quindi al giornale *on line*), sequestro che, dovendo cadere su di un *quid* smaterializzato, non può avvenire con le modalità tradizionali (apprensione della cosa, apposizione di sigilli ecc.), ma si deve attuare con quelle modalità tecniche atte ad inibire l'accesso di terzi al sito e dunque attraverso l'oscuramento di una risorsa elettronica, ai sensi degli artt. 14, 15 e 16 del d. lgs. 70/2003,

[15] Né il termine è estraneo al diritto penale, solo che si ponga mente all'art. 441 c.p. la cui rubrica è la seguente: "Adulterazione o contraffazione di altre cose in danno delle pubblica salute" e che testualmente recita: «chiunque adultera o contraffà in modo pericoloso alla salute pubblica, cose destinate al commercio, diverse da quelle indicate nell'articolo precedente […]». Le "cose" nominate nell'articolo precedente sono le sostane alimentari e il termine sostanza non è meno omnicomprensivo di "cosa", tanto che è necessaria una specificazione (alimentari).

[16] Innumerevoli sono le sentenze in tema di furto di energia elettrica, fattispecie cui sono ritenute pacificamente applicabili le aggravanti di cui all'art. 625 c.p. (da ultimo: Cass. pen., sez. V, 23 settembre 2019, n. 5055). Per quel che riguarda l'acqua, vedasi, ad esempio, ancora Cass. pen., sez. V, 20 maggio 2019, n. 38098.

in quanto «la equiparazione dei dati informatici alle cose in senso giuridico [testuale nella massima ufficiale n. 264089] consente di inibire la disponibilità delle informazioni in rete e di impedire la protrazione delle conseguenze dannose del reato».

Del resto, l'impiego del mezzo informatico ha apportato altri significativi mutamenti nell'assetto della giurisprudenza penale, mutamenti connaturati alle stesse modalità di utilizzo del mezzo e della organizzazione della diffusione in rete delle notizie. Così, ancora a titolo meramente esemplificativo, si può rilevare come la Suprema Corte abbia finito per ammettere, sia pure implicitamente, la possibilità che la diffamazione sia portata a esecuzione con una condotta omissiva,[17] quando il *blogger*, pur informato del contenuto denigratorio di una comunicazione, non provveda per tempo alla sua rimozione, «atteso che tale condotta equivale alla consapevole condivisione del contenuto lesivo dell'altrui reputazione e consente l'ulteriore diffusione dei commenti diffamatori»[18].

In sintesi, dunque, si deve riconoscere che, con sempre maggior frequenza, il giudice penale è chiamato a pronunciarsi su casi e fattispecie che, implicando in qualche modo il coinvolgimento della "rete", lo spingono a riflessioni (e decisioni) che comportano lo spostamento della sua attenzione dal mondo del concreto e del visibile, alla sfera dell'immateriale e dell'invisibile (*rectius*: di ciò che diviene visibile solo con l'ausilio di adeguati strumenti tecnologici). E tuttavia il dato qualificante di un moderno sistema di controllo normativo consiste nella individuazione di un punto di giusto equilibrio tra la preservazione dei principi di legalità, tassatività e determinatezza e la necessaria elasticità delle norme incriminatrici che, senza pregiudicare il requisito della prevedibilità e conoscibilità dei limiti entro i quali la condotta deve ritenersi lecita, possa abbracciare (e consentire di punire) comportamenti *contra jus* che rappresentino naturali sviluppi di condotte devianti poste in essere con mezzi e metodi messi a disposizione della evoluzione tecnico-scientifica, rispecchiata (più o meno) fedelmente nel vocabolario in uso tra i consociati.

A volte è lo stesso legislatore a lasciare esplicitamente socchiusa la porta alle eventuali future innovazioni tecnologiche che, spesso, finiscono per offrire nuove occasioni all'agire criminale. È il caso, ad esempio, del terzo comma dell'art. 595 c.p., che, come è noto, in tema di aggravante della diffamazione consumata col mezzo della stampa, prevede che sia aggravato il reato anche se l'offesa è recata "con altro mezzo di pubblicità", permettendo di inquadrare in tale tipo di condotta le comunicazioni veicolate dalle nuove tecnologie. Altre volte tale compito tocca all'interprete e costituisce campo di confronto tra dottrina e giurisprudenza[19].

---

[17] Sul punto anticipata dalla dottrina, in relazione alla quale ci permettiamo di segnalare M. Fumo, *La diffamazione mediatica,* Torino, 2011, 99-100.

[18] Cass. pen., sez. V, 8 novembre 2018, n. 12546; in relazione alla quale vedasi: C. Pagella, *La Cassazione sulla responsabilità del blogger per contenuti diffamatori (commenti) pubblicati,* in *Diritto penale Contemporaneo*, 17 maggio 2019 nonché D. Minotti, *Valutato come attivo un comportamento solo connivente,* in *Guida al Diritto,* 20, 2019, 84 ss. e, più in generale, M. Gambulli, *La responsabilità penale del provider per i reati commessi in internet*, in *altalex.com,* 24 ottobre 2005; M. Bassini, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli ISP. Verso un modello di responsabilità complessa?* in *Federalismi.it, Focus medita TMT,* 28 settembre 2015.

[19] In tema: C. Melzi d'Eril – G. E. Vigevani, *La responsabilità del periodico telematico tra facili equiparazioni e specificità di internet,* in *Diritto dell'informazione e dell'informatica*, 2010, 91 ss.; U. Sieber, *Responsabilità penale per la circolazione di dati nelle reti internazionali di computer. Le nuove sfide di internet*, in *Rivista trimestrale di diritto*

5. (Inevitabili) funambolismi giurisprudenziali

La sentenza in commento, come anticipato, ricorda i precedenti di legittimità in tema di reati contro il patrimonio aventi ad oggetto *res* informatiche.
Si è già detto della pronuncia della quinta sezione in cui la Corte ha ritenuto configurabile il delitto di furto nella condotta di un soggetto che, dopo aver comunicato la propria volontà di recedere da uno studio associato, si era impossessato di alcuni *files*, cancellandoli dal *server* dello studio (oltre che di alcuni documenti), al fine di impedire agli altri colleghi il controllo sulle reciproche spettanze[20].
Altra precedente pronunzia, pur ricordata dai giudici della seconda sezione, aveva affermato l'esatto contrario, sostenendo che «oggetto materiale della condotta di appropriazione indebita non può essere un bene immateriale come i crediti di cui si abbia disponibilità per conto d'altri, a meno che non siano equiparabili alle cose mobili perché "incorporati" in un documento» (la fattispecie era relativa ad un agente assicurativo che non aveva versato alla società di assicurazioni, per conto della quale operava, la somma di denaro corrispondente ai premi assicurativi riscossi dai subagenti)[21].
Ma è stata annoverata tra le decisioni contrarie anche altra sentenza, forse non esaminata *funditus*[22], la quale effettivamente esclude la configurabilità del reato di furto nel caso di duplicazione non autorizzata di *file* contenuti in un supporto informatico altrui, non comportando tale attività la perdita del possesso della *res* da parte del legittimo detentore. Il fatto è che la pronunzia in questione parla di "semplice" copiatura, vale a dire non accompagnata dalla distruzione dello scritto informatico copiato.
E si tratta di un punto dirimente, dal momento che, nella appropriazione indebita (come del resto nel furto, nella rapina ecc.), l'apprensione del bene da parte dell'agente comporta lo spossessamento dello stesso in danno della vittima. Ebbene ciò non si verifica quando il malintenzionato si limiti a copiare i dati (e quindi le informazioni) e a utilizzarli *invito domino*. Quest'ultimo, infatti, non ne viene spossessato in quanto "l'originale informatico" è rimasto nella sua disponibilità. Ecco perché va ribadito e posto nella dovuta evidenza che, per aversi appropriazione indebita (ma anche furto ecc.) di un *file,* non è sufficiente che l'agente ricopi abusivamente lo stesso, ma è necessario che distrugga, cancelli o renda inservibile la versione sulla quale ha formato la sua copia.
Insomma, viene a realizzarsi una sorta di reato bifasico, in cui l'impossessamento non è contestuale alla sottrazione, come nella appropriazione indebita o nel furto "tradizionali" (la "cosa" che era nel punto A e nella disponibilità di Tizio, passa nella disponibilità di Caio e potrebbe essere spostata o è di fatto spostata, subito o subito dopo, nel punto B), ma in cui le due condotte sono temporalmente separate: l'agente, prima, si impossessa del *file*, copiandolo, poi, cancella la "matrice" contenuta nel *computer* che ha abusivamente utilizzato. Una sistematizzazione un po' funambolica - che potrebbe porre problemi in tema di momento consumativo e di tentativo - ma inevitabile.
Non c'è dubbio che si tratti, infatti, di una costruzione piuttosto *extra ordinem*, resa

penale dell'economia, 1993, 763 ss.

[20] Cass. pen., sez. V, 19 febbraio 2015, n. 32383.

[21] Cass. pen., sez. II, 12 luglio 2011, n. 33839.

[22] Cass. pen., sez. IV, 26 ottobre 2010, n. 44840.

tuttavia necessaria dall'inerzia del legislatore, che, prodigo a volte nella creazione di nuove fattispecie incriminatrici non sempre indispensabili, bene farebbe a mettere mano a un razionale riordino in tema di *computer crime*.

Diffamazione a mezzo stampa e diritto di critica: no alle aggressioni senza motivato dissenso

Jacopo Antonelli Dudan

Corte di Cassazione, sez. V penale, 20 aprile 2020, n. 12460

La scriminante dell'esercizio del diritto di critica può essere invocata solo ove le espressioni utilizzate esprimano un motivato dissenso, manifestato in termini misurati e necessari, con esclusione di tutte le ipotesi in cui le modalità espressive realizzino un attacco personale, volto a ledere la dignità morale, professionale e intellettuale dell'avversario.

Sommario

1. Il principio. - 2. La vicenda. - 3. L'esito del processo e la decisione della Cassazione. - 4. Il significato ulteriore derivante dall'accostamento di parole.

Keywords

diffamazione – diritto di critica – stampa – libertà di espressione - reputazione

1. Il principio

Con la sentenza in oggetto la Cassazione torna a occuparsi di diffamazione a mezzo stampa e dei suoi limiti, con particolare riguardo al diritto di critica. Richiamando e facendo propri i principi ormai consolidati della materia, la Suprema Corte ribadisce che il limite immanente all'esercizio del diritto di critica è il rispetto della dignità, sicché l'esimente in parola non potrà mai essere validamente invocata tutte le volte che la critica abbia costituito mera occasione per arbitrarie aggressioni all'altrui patrimonio morale.

2. La vicenda

Il Supremo Collegio è intervenuto al termine dell'iter processuale di una vicenda tutta al femminile, svoltasi in Sicilia attraverso la pubblicazione di un articolo su un giornale on-line e la replica al vetriolo dell'imputata, tramite il suo blog personale.
In estrema sintesi, una giornalista pubblicava sul quotidiano on-line *Messina Oggi* un articolo di cronaca nel quale venivano riportate notizie relative, tra l'altro, al decesso

del coniuge dell'imputata. Quest'ultima, ritenendo non corrette le informazioni riportate su tale specifico punto, pubblicava a propria volta uno scritto sul proprio sito personale, dal titolo "*Giornaliste sgallettate da nord a sud*", nel quale si rivolgeva alla collega qualificandola come «una giornalista sgallettata con la fissa dello scoop».

3. L'esito del processo e la decisione della Cassazione

Nel corso del processo, i giudici da un lato accertavano che le notizie pubblicate sul quotidiano *Messina Oggi*, pur se datate, erano corrette e, dall'altro, ritenevano che l'uso della parola «sgallettata» – tra l'altro ripetuta sia nel titolo, sia nel testo – accostata all'espressione «con la fissa dello scoop», fosse lesiva perché idonea ad attribuire alla persona offesa qualità dispregiative tanto sotto il profilo professionale, quanto sotto quello umano. Muovendo, infatti, dalla definizione contenuta nel dizionario della lingua italiana De Mauro, secondo cui per «sgallettata» deve intendersi una «donna che ostenta la propria sensualità in modo sguaiato, che si dimostra eccessivamente disinvolta», i giudici di merito concludevano affermando che le espressioni utilizzate dall'imputata erano lesive della reputazione personale e professionale della querelante, perché la qualificavano come giornalista incline ad un uso spregiudicato delle notizie, riportate in assenza di qualsivoglia doverosa verifica delle stesse, al solo scopo di captare l'interesse dei lettori.

Ad avviso della Suprema Corte, tale conclusione risulta coerente con la consolidata giurisprudenza in materia, secondo cui il reato di diffamazione risulta integrato – sotto il profilo oggettivo – ogni volta che le espressioni utilizzate si traducano in un gratuito attacco alla persona e in arbitrarie aggressioni al suo patrimonio morale, personale e intellettuale.

Acclarato dunque per tale via il carattere oggettivamente lesivo del contenuto dell'articolo incriminato e ritenuto perciò sussistente l'elemento materiale del reato, i giudici del massimo collegio ritengono poi corretta la ritenuta (da Tribunale e Corte d'appello) inapplicabilità della scriminante del diritto di critica, pur invocata dall'imputata, sia per mancanza dell'interesse pubblico suscettibile di giustificare l'agire della predetta, sia per la sproporzione tra le espressioni dalla medesima utilizzate e l'asettico tenore dell'articolo di mera cronaca firmato dalla persona offesa (e dalla prima ritenuto causa legittimante la propria reazione critica). Sul punto, infatti, l'annotata sentenza da un lato ricorda che il limite all'esercizio del diritto di critica – costantemente ribadito dalla stessa giurisprudenza di Cassazione – è il rispetto della dignità altrui, tal per cui il suo esercizio non può mai costituire mera occasione per arbitrarie aggressioni al patrimonio morale e/o personale del destinatario della critica stessa; dall'altro, ricorda come l'invocata esimente non possa mai trovare applicazione in tutti quei casi in cui l'espressione utilizzata non realizzi e non esprima un motivato dissenso, manifestato in modo e con forme e contenuti misurati, ma si concretizzi in un attacco personale, con espressioni direttamente volte a ledere l'integrità morale, intellettuale e/o professionale dell'avversario. Esattamente ciò che sarebbe avvenuto, ad avviso dei giudici, nel caso di specie.

4. Il significato ulteriore derivante dall'accostamento di parole

La sentenza in parola – come detto – si inserisce dunque a pieno titolo nel solco tracciato dalla giurisprudenza in materia di manifestazione del pensiero, ribadendone con chiarezza i limiti. Dal sintetico resoconto dei fatti operato dalla Corte appare difficile non condividerne le conclusioni, in ragione della ripetizione dell'epiteto «sgallettata» nel titolo e nel testo – artificio retorico certamente idoneo a richiamare maggiormente l'attenzione del lettore e a rafforzare il concetto espresso attraverso il ricorso a quella parola – e soprattutto dell'accostamento tra quella medesima espressione e la pretesa «fissa dello scoop», concetti che, in una valutazione d'insieme, appaiono certamente tali da realizzare un attacco offensivo piuttosto gratuito e ingiustificato alla dimensione professionale della persona offesa, più che un giudizio critico nei confronti della medesima, ragionato e fondato su elementi concreti e veritieri (non presenti nell'articolo "incriminato", secondo quanto desumibile dal testo della pronuncia).

Forse la difesa dell'imputata sarebbe stata meno ardua se nel processo si fosse dibattuto solo dell'espressione «sgallettata»: ci si sarebbe probabilmente potuti domandare se quella «ostentazione di sensualità in modo disinvolto» dovesse effettivamente ritenersi un'offesa oggettiva, come tale percepibile e percepita dal "lettore medio" o se, piuttosto, non dovesse considerarsi una semplice sottolineatura, al più venata di sarcasmo, di una inclinazione personale del tutto legittima e comunque priva di qualsiasi valenza offensiva. Opzione interpretativa non solo plausibile, ad avviso di chi scrive, ma con ogni probabilità agevolmente (o comunque più facilmente) sostenibile se il destinatario della piccata "reazione" dell'autrice fosse stato un uomo e non una donna.

Ma, purtroppo per lei, l'imputata si è fatta "prendere la penna", così facilitando il compito del giudicante.

Note a sentenza

Sezione Europa

Il caso Taormina e la Corte di giustizia. Dalla libera espressione alla discriminazione*

Palmina Tanzarella

Corte di giustizia dell'Unione europea, 23 aprile 2020, C-507/18, *NH c. Associazione Avvocatura per i diritti LGBTI-Rete Lenford*

La nozione di «condizioni di accesso all'occupazione e al lavoro» contenuta all'art. 3, par. 1, lett. *a)*, della direttiva 2000/78/CE, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro, deve essere interpretata nel senso che in essa rientrano delle dichiarazioni rese da una persona nel corso di una trasmissione audiovisiva secondo le quali tale persona mai assumerebbe o vorrebbe avvalersi, nella propria impresa, della collaborazione di persone di un determinato orientamento sessuale, e ciò sebbene non fosse in corso o programmata una procedura di selezione di personale, purché il collegamento tra dette dichiarazioni e le condizioni di accesso all'occupazione e al lavoro in seno a tale impresa non sia ipotetico.
La direttiva 2000/78 deve essere interpretata nel senso che essa non osta ad una normativa nazionale in virtù della quale un'associazione di avvocati, la cui finalità statutaria consista nel difendere in giudizio le persone aventi segnatamente un determinato orientamento sessuale e nel promuovere la cultura e il rispetto dei diritti di tale categoria di persone, sia, in ragione di tale finalità e indipendentemente dall'eventuale scopo di lucro dell'associazione stessa, automaticamente legittimata ad avviare un procedimento giurisdizionale inteso a far rispettare gli obblighi risultanti dalla direttiva summenzionata e, eventualmente, ad ottenere il risarcimento del danno, nel caso in cui si verifichino fatti idonei a costituire una discriminazione, ai sensi di detta direttiva, nei confronti della citata categoria di persone e non sia identificabile una persona lesa.

Sommario

1. La strada scelta dalla Corte di giustizia tra i discorsi d'odio e il principio di non discriminazione. – 2. Le linee principali della decisione e le sue contraddizioni interne. – 3. Discorsi d'odio e non discriminazione nella giurisprudenza della Corte di Strasburgo. – 4. Discorsi d'odio e non discriminazione nella giurisprudenza italiana. – 5. Una nuova veste per il principio di non discriminazione e le conseguenze possibili sul ruolo della Corte di giustizia.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo

Keywords

libertà d'espressione - principio di non discriminazione - *hate speech* - discorsi omofobi - Carta di Nizza

1. La strada scelta dalla Corte di giustizia tra i discorsi d'odio e il principio di non discriminazione

Il principio di non discriminazione costituisce, come noto, uno dei capisaldi dell'Unione europea – insieme a pluralismo, giustizia, tolleranza, solidarietà e parità tra uomo e donna[1] – rappresentando nondimeno un chiaro obiettivo del processo d'integrazione europea, soprattutto in chiave politica e sociale[2].

È, questo, un dato ritenuto ormai scontato, ma per nulla prevedibile alle origini, quando Istituzioni europee e Stati membri si erano prefissi come unico scopo la realizzazione di un mercato comune. Tanta strada quindi è stata percorsa, diventando il principio di non discriminazione l'elemento chiave per un'unione sempre più stretta tra i popoli.

Con la sentenza della Grande sezione della Corte di giustizia *NH c. Associazione Avvocatura per i diritti LGBTI-Rete Lenford*[3], si compie un ulteriore e sorprendente balzo in avanti: la non discriminazione si arricchisce di significati forieri di trasformazioni del modo di essere "costituzionale" degli ordinamenti nazionali, compromettendo in parte i principi che li caratterizza.

Più in particolare, al cuore della vicenda c'è il problema di come conciliare la libertà d'espressione con i suoi potenziali risvolti lesivi dell'eguaglianza, a cui questa decisione fornisce una soluzione scivolosa. Detto molto in sintesi, la Corte di giustizia giunge a riconoscere che le dichiarazioni rese nel corso di una trasmissione radiofonica di chi sosteneva che mai sarebbero stati assunti nel proprio studio professionale persone di un determinato orientamento sessuale, rientrano nell'ambito di applicazione della direttiva 2000/78 in materia di occupazione e di lavoro (in particolare dell'art. 3, par. 1, lett. a) relativo alle «condizioni di accesso all'occupazione e al lavoro»), sebbene non fosse in corso o programmata una procedura di selezione del personale. L'importante, chiosa la Corte di giustizia, è che il giudice nazionale verifichi nel caso di specie che il collegamento tra dette dichiarazioni e le condizioni di accesso all'occupazione e al lavoro non sia ipotetico.

Stante alla lettura del dispositivo non ci sarebbero motivi per credere che il riconoscimento del principio di non discriminazione abbia trovato un'espansione applicativa: viene esplicitamente richiesta la verifica del nesso di causalità tra le parole dette e gli effetti prodotti in concreto e ciò è quanto mai opportuno dato che, in generale, le limitazioni alla manifestazione del pensiero sono acconsentite qualora beni di pari rango subiscano un'ingiustificata o eccessiva compressione. Tuttavia, le argomentazioni addotte offrono alcuni spunti di riflessione non solo in ordine a una possibile

[1] Cfr. art. 2, TUE.

[2] Cfr. art. 3, par. 2, lett. *a)*, TUE.

[3] CGUE, C-507/18, *NH c. Associazione Avvocatura per i diritti LGBTI – Rete Lenford* (2020).

"nuova" accezione del principio di non discriminazione in seno all'Unione europea, ma soprattutto in relazione al ruolo che la Corte di giustizia riveste come "giudice dei diritti", chiamata a bilanciare libertà individuali quali la manifestazione del pensiero con l'iniziativa economica privata.
La non discriminazione si prepara ad assumere nuove sembianze? E in ossequio a ciò, la Corte di giustizia che lessico dei diritti utilizza? Rimane ancorata ai vecchi schemi di giudice dell'Unione europea, oppure riesce a imprimere un nuovo registro linguistico ponendosi come giudice dei diritti prima ancora che come giudice dei trattati?
Queste sono le domande che guideranno il presente contributo, alle quali si cercherà di rispondere valutando i fatti del caso di specie e le conclusioni a cui è giunta la Corte di giustizia alla luce del più ampio panorama del Consiglio d'Europa e del contesto specifico italiano da cui la vicenda ha preso le mosse. Ciò perché la sentenza in questione pare essere "contaminata" dalle posizioni istituzionali e giurisprudenziali nazionali e sovranazionali degli ultimi tempi in tema di discorsi "discriminatori", meglio conosciuti come discorsi d'odio (o che dir si voglia di *hate speech*), espressivi di una certa intolleranza nei confronti di collettività accomunate dall'appartenenza a una certa nazionalità, convincimento religioso, etnia, oppure orientamento sessuale. Si tratta di una fattispecie ascritta tra la più ampia categoria dei reati d'opinione la cui caratteristica principale, appunto, non è tutelare una posizione individuale, come ad esempio l'onore, la reputazione o la riservatezza[4].
Tenendo in conto di queste prime coordinate definitorie, in via preliminare è utile analizzare i passaggi salienti della sentenza della Corte di giustizia.

2. Le linee principali della decisione e le sue contraddizioni interne

Con la sentenza che si commenta anche la Corte di giustizia, per la prima volta, si trova a giudicare di un caso di *hate speech*. Infatti, la vicenda muove dalle dichiarazioni di Carlo Taormina, noto avvocato italiano, che durante la trasmissione radiofonica "La Zanzara", andata in onda il 16 ottobre 2013 su Radio24, affermava che mai avrebbe assunto nel suo studio omosessuali[5].
Può un'affermazione del genere, dal sapore certamente omofobo e quindi irrispettoso nei confronti di una certa categoria di persone, costituire una discriminazione nell'accesso al lavoro? È questa in sostanza la questione (la seconda invero) che la Cassazione italiana pone in via pregiudiziale alla Corte di giustizia.

[4] In genere, i reati d'opinione proteggono la personalità dello Stato (tra cui il prestigio delle istituzioni, come il vilipendio) – oppure l'ordine pubblico (come l'istigazione a delinquere o a disobbedire alle leggi, l'apologia di delitti, la diffusione di notizie false e tendenziose). In dottrina, per tutti, C. Fiore, *I reati d'opinione*, Padova, 1972; E. Lamarque, *I reati d'opinione*, in Aa. Vv., *Percorsi di diritto dell'informazione*, Torino, 2011, 141 ss.; M. Cuniberti, *Il buon costume e i reati di opinione*, in Aa. Vv., *Diritto dell'informazione e dei media*, Torino, 2019, 171 ss.

[5] Nello specifico Taormina dichiarava: «se la tenga lei l'omosessualità [...], l'importante è che non mi stiano intorno [...]. Mi danno fastidio [...]. Parlano diversamente, si vestono diversamente, si muovono diversamente, è una cosa assolutamente insopportabile. È contro natura».

Come anticipato, la Corte europea risponde affermativamente, col limite sopra ricordato della verifica del nesso di causalità. Ciononostante, l'esito era poco prevedibile, indice la scelta di un percorso argomentativo che presenta alcune forzature.

Innanzitutto, viene data primariamente risposta alla seconda delle due domande pregiudiziali. In realtà, il giudice rimettente chiedeva preliminarmente se l'Associazione Avvocatura per i diritti LGBTI – Rete Lenford (d'ora in avanti l'Associazione) costituisse un ente esponenziale ai sensi dell'art. 9, par. 2, della direttiva 2000/78[6], per verificare la sua legittimazione ad agire in difesa di interessi di singoli o di gruppi nonostante la sua attività fosse anche a scopo di lucro; solo successivamente si poneva il dubbio circa l'ambito d'applicazione della direttiva relativamente alle dichiarazioni rilasciate da Taormina.

L'ordine delle domande così come prospettato dalla Cassazione aveva una sua logica. Chiarire in prima battuta se un organismo ha la capacità giuridica per denunciare una presunta discriminazione ai danni di un indeterminato gruppo di persone avrebbe contestualmente potuto chiarire se le dichiarazioni come quelle rese nel caso di specie costituivano una discriminazione ai sensi dell'art. 2 della direttiva[7]. È vero, come fa notare la Corte di giustizia, che «nel procedimento principale viene in discussione non già il punto se le dichiarazioni rese da NH rientrino nella nozione di discriminazione, […], bensì la questione se, tenuto conto delle circostanze nelle quali tali dichiarazioni sono state effettuate, esse rientrino nell'ambito di applicazione materiale di detta direttiva là dove questa contempla, all'art. 3, par. 1, lett. *a)*, le «condizioni di accesso all'occupazione e al lavoro […], compresi i criteri di selezione e le condizioni di assunzione»[8]. Ma è altrettanto verosimile che il giudice italiano abbia formulato la seconda questione tralasciando l'interrogativo sulla natura discriminatoria delle dichiarazioni non tanto perché le riteneva essere tali, ma perché evidentemente presupponeva che sarebbe stata la stessa Corte di giustizia a risolvere il punto grazie alla risposta alla prima domanda. Infatti, in assenza di un ricorso adito direttamente da un soggetto determinato che ritiene di aver subito una disparità di trattamento si sarebbe dovuto necessariamente riflettere sulla nozione di discriminazione, al fine di sapere se è possibile denunciarne

[6] L'art. 9 della citata direttiva è compreso nel capo II di quest'ultima, relativo ai mezzi di ricorso e all'attuazione delle norme. Intitolato "Difesa dei diritti", tale articolo prevede, al par. 2, quanto segue: «Gli Stati membri riconoscono alle associazioni, organizzazioni e altre persone giuridiche che, conformemente ai criteri stabiliti dalle rispettive legislazioni nazionali, abbiano un interesse legittimo a garantire che le disposizioni della presente direttiva siano rispettate, il diritto di avviare, in via giurisdizionale o amministrativa, per conto o a sostegno della persona che si ritiene lesa e con il suo consenso, una procedura finalizzata all'esecuzione degli obblighi derivanti dalla presente direttiva».

[7] L'art. 2 così recita: «1. Ai fini della presente direttiva, per "principio della parità di trattamento" si intende l'assenza di qualsiasi discriminazione diretta o indiretta basata su uno dei motivi di cui all'articolo 1. 2. Ai fini del paragrafo 1: a) sussiste discriminazione diretta quando, sulla base di uno qualsiasi dei motivi di cui all'articolo 1, una persona è trattata meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga; b) sussiste discriminazione indiretta quando una disposizione, un criterio o una prassi apparentemente neutri possono mettere in una posizione di particolare svantaggio le persone che professano una determinata religione o ideologia di altra natura, le persone portatrici di un particolare handicap, le persone di una particolare età o di una particolare tendenza sessuale, rispetto ad altre persone, a meno che: i) tale disposizione, tale criterio o tale prassi siano oggettivamente giustificati da una finalità legittima e i mezzi impiegati per il suo conseguimento siano appropriati e necessari (…)».

[8] CGUE, causa C-507/18, cit., § 28.

la sua sussistenza anche in astratto. Ovvero, la Corte avrebbe dovuto illustrare come mai le dichiarazioni estemporanee fatte da chi non aveva in programma di assumere del personale costituissero di per sé stessa una discriminazione. Avrebbe dovuto chiarire, cioè, sul piano giuridico, i motivi per cui anche le parole debbano essere considerate degli atti concreti e non il preludio di un'eventuale (non si sa quanto probabile) lesione dell'eguaglianza. Invece, decidendo di invertire l'ordine delle risposte, la Corte ha potuto soprassedere sul punto, a ben vedere fondamentale per i casi di *hate speech*. È sottinteso nel ragionamento della Corte di giustizia che parlare un linguaggio omofobo equivale a discriminare in modo diretto. Questo è un punto da tener presente e che condizionerà tutto il ragionamento successivo. Vediamo come.

Per stabilire se le dichiarazioni di Taormina rientrano nell'ambito d'applicazione della direttiva relativamente alle condizioni di accesso all'occupazione e al lavoro, la Corte di giustizia specifica che l'interpretazione letterale della disposizione non è sufficiente. Infatti, posto che lo scopo della direttiva è la lotta alle discriminazioni per offrire ad ogni persona le giuste condizioni per entrare nel mondo del lavoro, una interpretazione restrittiva non sarebbe possibile, pena l'esclusione di situazioni pregiudizievoli che altrimenti non sarebbero punite. Di conseguenza, la delimitazione dell'ambito applicativo va individuato considerando il contesto di riferimento: secondo la Corte non è decisivo che vi sia una procedura di selezione in corso o programmata per stabilire se delle dichiarazioni siano relative ad una determinata politica di assunzioni[9]; invece, è necessario che tali affermazioni condizionino le modalità di assunzione. È per questo, ad avviso della Corte, che va cercato il collegamento non ipotetico tra le dichiarazioni e le condizioni di accesso al posto di lavoro.

Fin qui nulla da eccepire, se non fosse che i criteri determinanti per verificare tale nesso – suggeriti dalla stessa Corte – sono tutti indicativi di un preciso modo di intendere le espressioni intolleranti e senza dubbio inaccettabili sul piano etico. Vale a dire, per il sol fatto di essere pronunciate producono determinati effetti negativi. Specificamente, il contrasto alle discriminazioni – obiettivo principale della direttiva – passa attraverso il contrasto al linguaggio anche quando non è detto che questo produca in concreto situazioni di disparità, potendosi arrestare al piano delle minacce, o più semplicemente presentarsi in una forma di ammissione del proprio disprezzo. Infatti, nessuno dei requisiti che la Corte di giustizia suggerisce al giudice del rinvio di verificare ha la caratteristica di provare il sicuro intendimento da parte del datore di lavoro di non assumere persone omosessuali. Analizziamoli uno per uno.

In primo luogo, rileverebbe lo status dell'autore delle dichiarazioni e la veste nella quale si è espresso. Come suggerito nelle conclusioni dell'Avvocato Generale, se lo stesso tipo di dichiarazioni fossero rese da chi svolge un'attività differente da quella a cui le frasi si rivolgono, queste non avrebbero lo stesso impatto in quanto non eser-

[9] Un'affermazione questa che la Corte di giustizia mutua da un suo precedente, che esplicitamente cita nella decisione in commento (v. §§ 40-41), ovvero CGUE, C-81/12, *Asociația Accept* (2013). Anche in questo caso non si era alla presenza di una selezione pubblica di assunzione o di una trattativa privata; tuttavia, le dichiarazioni omofobe erano state rese da un'azionista della stessa società (calcistica) che in seguito non aveva ingaggiato un calciatore proprio perché, presumibilmente, omosessuale. Quindi, differentemente dal caso *NH*, il collegamento tra le dichiarazioni e la politica delle assunzioni si poteva misurare in concreto.

citerebbero un'influenza determinante sulla politica di assunzioni. Stando all'esempio dell'Avvocato Generale, qualora «l'autore dell'affermazione "se fossi un avvocato, non assumerei mai persone LGBTI nel mio studio legale" fosse un architetto, anziché un avvocato, e non ricoprisse alcun ruolo in uno studio legale, tale affermazione, per quanto deplorevole, non presenterebbe alcun nesso effettivo con l'accesso all'occupazione»[10]. Ciò perché, come puntualizzerà poi la Corte, il dichiarante dev'essere «quantomeno, suscettibile di essere percepito dal pubblico o dagli ambienti interessati come capace di esercitare un'influenza siffatta»[11]. Fermiamoci a riflettere meglio su queste parole. Come misurare l'influenza di un qualunque professionista, pur noto nell'ambente, su innumerevoli datori di lavoro titolari di studi professionali sparsi nel territorio nazionale? Chissà quanti, tra questi, hanno preso o prenderebbero le distanze da certe posizioni. Come potrebbe allora il giudice nazionale valutare l'impatto di tale requisito? Non gli rimarrebbe che affidarsi a sue proprie percezioni. Potrebbero forse aiutare delle mirate indagini statistiche per capire a quanto ammonta il numero di omosessuali a cui, dopo le dichiarazioni di Taormina, è stata negata un'assunzione negli studi legali. Ma, verosimilmente, simuli studi non sono stati effettuati, quindi il problema di considerare in termini oggettivi il requisito suggerito dalla Corte di giustizia pare irrisolvibile.

In secondo luogo, si suggerisce di considerare la natura e il contenuto delle dichiarazioni in questione. Nello specifico, «queste ultime devono riferirsi alle condizioni di accesso all'occupazione e al lavoro presso il datore di lavoro di cui trattasi e dimostrare l'intenzione di tale datore di lavoro di discriminare sulla base di uno dei criteri previsti dalla direttiva 2000/78»[12]. Come interpretare questo criterio, il quale in realtà pare essere scollegato dagli altri indicati? È a tutti chiaro che Taormina non abbia parlato in qualità di datore di lavoro che si accingeva ad assumere del personale nel suo studio. Delle due l'una, o il contenuto delle sue dichiarazioni devono essere valutate in seno a procedure di assunzione presso altri studi, al momento ipotetici, oppure a suo esclusivo pregiudizio per la manifesta intenzione di non voler assumere in futuro personale con un preciso orientamento sessuale[13]. Al di là di tutto, in assenza di una situazione concreta di diniego di assunzione di una persona omosessuale in uno studio professionale, le dichiarazioni di Taormina, pur ipoteticamente discriminatorie, non presentano alcun nesso con una specifica e reale situazione. L'unica indicazione chiara che proviene dalla segnalazione di questo requisito è di fare attenzione al modo di essere delle dichiarazioni incriminate, per riconoscerne la "natura" discriminatoria, a prescindere dal dispiegamento dei loro effetti in concreto.

Da ultimo, è rilevante «il carattere pubblico o privato delle dichiarazioni, od anche il fatto che esse siano state oggetto di diffusione tra il pubblico, a prescindere che ciò sia avvenuto attraverso i media tradizionali oppure tramite social network»[14]. Al contrario di quello precedente, questo è un requisito essenzialmente collegato al primo, in quan-

[10] Conclusioni dell'Avvocato generale Sharpston, C-507/18, *NH*, 31 ottobre 2019, § 52.

[11] CGUE, C-507/18, cit., § 44.

[12] Ivi, § 45.

[13] È questa d'altronde la conclusione a cui in primo e in secondo grado erano giunti i giudici italiani. Cfr. Trib. Bergamo, ord. 6 agosto 2014; App. Brescia, sez. lav., 11 dicembre 2014.

[14] CGUE, causa C-507/18, cit., § 46.

to più un'informazione è pubblica e ha un certo grado di diffusione tra i media - che siano classici oppure di nuova generazione poco importa – più ha capacità d'influenzare chi deve decidere.

L'elencazione dei criteri rivela l'inclinazione della Corte di giustizia che, come si vedrà a breve, non è estranea al resto del mondo del diritto, in particolare alle altre Corti, a proteggere le persone più deboli vessate dagli atteggiamenti tracotanti di taluni. Ciò per assicurare loro il posto che spetta nella società. Da come impostata l'intera decisione, è come se il problema legato alla discriminazione risiedesse a monte, più che a valle. Ovvero, le dichiarazioni di natura discriminatoria dissuaderebbero le categorie oppresse alla ricerca di un impiego, contravvenendo allo scopo principale della direttiva che ambisce alla piena partecipazione dei cittadini alla vita economica, culturale e sociale

Il senso di umiliazione sofferto da alcune categorie spinge a vigilare attentamente sull'ambiente circostante, pretendendo anche giuridicamente di creare e mantenere un clima sociale privo di conflitti, tanto che si ritiene rispettato il principio di proporzionalità rispetto all'ingerenza nell'esercizio della libertà di espressione. Come sostiene la Corte «non si va oltre quanto è necessario per realizzare gli obiettivi di tale direttiva, vietando unicamente le dichiarazioni che costituiscono una discriminazione in materia di occupazione e di lavoro»[15].

L'approccio scelto dalla Corte di giustizia non è affatto isolato e può comprendersi appieno se si esaminano le recenti tendenze della Corte di Strasburgo e delle corti italiane sul bilanciamento tra libertà d'espressione e non discriminazione, rivelatrici entrambe di una concezione paternalistica dello Stato, il quale si sente in dovere di censurare certi tipi di linguaggio.

3. Discorsi d'odio e non discriminazione nella giurisprudenza della Corte di Strasburgo

La Corte europea dei diritti dell'uomo è stata tra le prime a riconoscere limiti stringenti ai discorsi d'odio, potendo adottare un approccio ben diverso rispetto a quello che la Corte di giustizia è stata costretta a seguire. A differenza di questa, che per le caratteristiche del sistema entra nella questione dei diritti incidentalmente nonostante la vincolatività della Carta di Nizza[16], il compito esclusivo affidato a Strasburgo è vigilare sulla tutela delle libertà fondamentali. Pertanto, per essa è fisiologico "misurare" i diritti tra di loro, cercando di valutare caso per caso se i limiti esplicitamente richiamati nei singoli articoli della Convenzione europea dei diritti dell'uomo (d'ora in avanti CEDU) siano stati valicati. La conseguenza è che alla Corte Edu vengono proposti svariati motivi per denunciare l'offensività dei discorsi d'odio, tanto da non aver mai dovuto finora giustificare la loro limitazione per lesione del principio di non discriminazione, sebbene

[15] Ivi, § 52.

[16] Cfr. l'art. 51, par. 1, della Carta che nello specifico stabilisce che l'ambito applicativo della Carta si estende «alle istituzioni e agli organi dell'Unione nel rispetto del principio di sussidiarietà come pure agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione. Pertanto, i suddetti soggetti rispettano i diritti, osservano i principi e ne promuovono l'applicazione secondo le rispettive competenze».

questo sia esplicitamente previsto all'art. 14 CEDU e al Protocollo aggiuntivo n. 12. In particolare, questa Corte può attingere al lungo elenco delle restrizioni contemplate al secondo comma dell'art. 10 CEDU[17], oltre che alla clausola di salvaguardia sull'abuso di diritto *ex* art. 17, che scatta qualora i ricorsi abbiano il reale scopo di annientare la libertà di cui si denuncia la lesione[18]. Nel caso della manifestazione del pensiero, la Corte applica tale disposizione per quelle dichiarazioni che vengono utilizzate all'unico scopo di raggiungere fini contrari al testo e allo spirito della Convenzione. Quando, cioè, la Corte teme che la richiesta di protezione di un diritto fondamentale sia strumentale a raggiungere lo scopo opposto di distruggerlo, essa dichiara l'inammissibilità della questione per incompatibilità *ratione materiae*.

In definitiva, Strasburgo usa categorie che esulano dalle posizioni civilistiche di accesso al lavoro, alle prestazioni sociali etc. e che presuppongono una discriminazione ai danni dei soggetti coinvolti. I beni oggetti di tutela sono individuati tenendo conto dell'obiettivo principale della Convenzione, ovvero la salvaguardia della democrazia. Perciò, la censura dei discorsi d'odio si giustifica nella misura in cui questi mettano in pericolo l'ordine democratico. Eppure, come si vedrà, proprio in vista della sua protezione la Corte ha, in tempi più recenti, giustificato la sanzione dei discorsi d'odio per evitare disparità di trattamento tra i consociati. Ossia, la parola diventa atto di discriminazione che fomenta il conflitto, scompaginando l'ordine sociale.

Detto in sintesi, nei primi anni di attività la Corte compiva uno scrutinio molto attento sugli indici di pericolosità che potevano minacciare la tenuta del sistema democratico, richiamandosi alla dottrina del *clear and present danger* elaborata dalla giurisprudenza della Corte suprema statunitense[19]. In definitiva, i discorsi d'odio venivano limitati quando il rischio si riteneva "attuale"; ad esempio quando all'istigazione seguivano veri e propri disordini violenti[20]. Successivamente, il principio a cui la Corte si è sempre

[17] Cfr. art. 10, par. 2, CEDU che dispone: «L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario».

[18] In generale per la genesi e l'applicazione di tale articolo cfr. C. Pinelli, *Art. 17. Divieto dell'abuso di diritto*, in S. Bartole - B. Conforti - G. Raimondi (a cura di), *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2001; 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. In particolare sull'impatto che l'art. 17 ha sulla libertà di manifestazione del pensiero, H. Cannie - D. Voorhoof, *The Abuse Clause and Freedom of Expression in the European Human Rights Convention: An Added Value for Democracy and Human Rights Protection*, in *N.Q.H.R.*, 29, 2011, 54 ss.; D. Keane, *Attacking hate speech under Article 17 of the European Convention on human rights*, ivi, 25, 2007, 641 ss.

[19] Il *clear and present danger* è da intendersi come l'istigazione alla commissione di un reato. La sua prima formulazione risale all'opinione dissenziente del giudice Holmes espressa nella storica sentenza *Abrams v. United States* degli inizi del novecento (*Abrams v. United States*, 250 U.S., 1919). Per un commento sulla giurisprudenza prodotta in applicazione di tale dottrina, R. J. Williams Jr., *Burning crosses and blazing words: Hate Speech and the Supreme Court's free speech clause jurisprudence*, in *Seton Hall L. J.*, 5, 1999, 609 ss.

[20] A tal proposito, si veda il filone dei casi turchi che vedeva coinvolta la popolazione curda, la quale rivendicava attraverso manifestazioni violente la propria indipendenza. Tra i molti, *Zana c. Turchia*, ric. 18954/91 (1997); *Surek. C. Turchia (n. 1),* ric. 26682/95 (1999) e *Surek c. Turchia (n.3),* ric. 26682/95 (1999), *Falakaoglu e Sajgili c. Turchia,* ric. 77365/01 (2007).

ispirata, secondo cui la massima espansione della libertà d'espressione è ingrediente essenziale per la realizzazione del processo democratico – tanto da giustificare le opinioni più scioccanti, che inquietano, che disturbano – è stato ridimensionato e a tratti rinnegato. Nei tempi attuali i pensieri scomodi sono censurati proprio per preservare lo Stato democratico. Per questo, il criterio del *clear and present danger* è stato man mano sostituito con quello dell'*indirect harm*, il quale ammette la punibilità di idee che incitano all'odio o alla violenza, anche quando non costituiscono una minaccia attuale alla democrazia, perché potrebbero comunque rappresentare una minaccia futura.

Ma quanto futura? Solo ipotetica oppure "pressoché" certa? Avendo imboccato la strada della protezione anticipata, la Corte cerca comunque di rimanere prudente per contenere i rischi di un'eccessiva, se non addirittura inutile limitazione ai pensieri che potrebbero rivelarsi poi innocui. A tal fine essa si serve di due tipi di test: l'*incitement test*, il quale prova la "quasi" imminenza del danno conseguente all'adozione di un registro verbale intenzionalmente provocatorio e offensivo; il *bad tendency* test, attraverso cui s'individuano le espressioni d'odio, che lungi dall'avere un reale intento sovversivo, sono considerate "tendenzialmente" portatrici sane di discriminazione e violenza, come ad esempio la diffusione di stereotipi che col tempo rafforzano attitudini e atteggiamenti discriminatori già esistenti o ne alimentano di nuovi[21]. I discorsi d'odio limitabili sono quelli che non superano il primo dei due.

Ciononostante, lo scrutinio che la Corte compie non è sempre lineare, dato che alla prova dei fatti questi test si sono rivelati poco attendibili per la difficoltà di demarcare una netta linea di confine tra di loro. Soprattutto due precisi filoni giurisprudenziali, che interessano l'uno l'odio espresso nei confronti della minoranza ebraica (in particolare attraverso il negazionismo), l'altro l'odio rivolto ai migranti extracomunitari, provano come la Corte europea si spinga oltre la barriera dell'*incitement* test, applicando restrizioni alla libertà di manifestazione del pensiero anche quando non producono conseguenze negative solo nel breve periodo[22].

In tal modo, la protezione della democrazia passa non tanto attraverso la prevenzione di atti sovversivi indotti dall'utilizzo di un linguaggio istigante all'odio, quanto piuttosto grazie alla prevenzione di conflitti sociali dovuti all'esplicito mancato riconoscimento di determinati gruppi deboli. Detto in altri termini, la Corte, negando protezione ai discorsi d'odio, tutela il danno indiretto da discriminazione, pur non dichiarandone la violazione degli articoli della Convenzione ad essa dedicati. Basta il passaggio di questa sentenza per capire l'approccio ormai scelto da Strasburgo: «Attacchi che si concretizzano in insulti, la messa in ridicolo o la calunnia ai danni di specifici gruppi di una popolazione sono motivi sufficienti per le autorità per combattere l'*hate speech,*

[21] Cfr. le opinioni dissenzienti nel caso *Aksu c. Turchia,* ricc. 4149/04 e 41029/04 (2010). Significativo è il passaggio in cui i giudici dichiarano che: «*Stereotypes are ready-made opinions that focus on peculiarities, and prejudices are preconceived ideas that lead to bias: they are dangerous because they reflect or even induce an implicit discrimination*» (§ 2 dell'opinione dissenziente dei giudici Tulken, Tsotsoria e Pardalos). In dottrina, S. Sottiaux, *Bad tendencies in the ECtHR's hate speech jurisprudence*, in *Eu. Const. L. Rev.*, 7, 2011, 40 ss.

[22] Non è questa la sede per una loro compiuta analisi. Sia quindi consentito il rimando a P. Tanzarella, *Discriminare parlando. Il pluralismo democratico messo alla prova dai discorsi d'odio razziale*, Torino, 2020, spec. 99-110.

sfavorendo così la libertà d'espressione esercitata in maniera irresponsabile»[23].
Dietro a decisioni in cui si punisce chi non ha rispetto per le minoranze, paventando un "eventuale" pericolo di discriminazione nei loro confronti, si cela l'esigenza di proteggerle da vessazioni e risentimenti. Sembrano allora confermate le parole del costituzionalista inglese McCrudden, il quale già in un articolo del 1995 avvertiva della china paternalistica su cui iniziava a scivolare la Corte di Strasburgo[24], quando ancora i paesi europei non immaginavano affatto di dover fronteggiare i problemi relativi ai flussi immigratori e al terrorismo di matrice islamica.

4. Discorsi d'odio e non discriminazione nella giurisprudenza italiana

Anche i giudici italiani tentano di seguire la strada europea, ritenendo opportuno condannare il pensiero discriminatorio e non solo l'azione discriminatoria.
Se, come visto, per Strasburgo a fare da grimaldello è stata esclusivamente la tutela dell'ordine democratico, per il nostro ordinamento si è potuta adottare anche una prospettiva molto più vicina a quella della Corte di giustizia.
Inizialmente i discorsi d'odio venivano punti sulla base della legge penale n. 654/1975, oggi abrogata per essere stata inserita nel codice penale agli articoli 604-*bis* e 604-*ter*. Questa legge, che col tempo aveva subito ulteriori modifiche[25], era stata interpretata nel senso di proteggere l'ordine pubblico. Successivamente, grazie a un'interpretazione evolutiva della giurisprudenza – favorita dall'accostamento della fattispecie della propaganda d'idee fondate sulla superiorità o sull'odio razziale o etnico, alla fattispecie dell'istigazione a commettere "atti di discriminazione" per motivi razziali, etnici, nazionali o religiosi – i beni oggetto di tutela sono diventati la dignità sociale e l'eguaglianza, oltre che l'ordine pubblico[26].
Poiché il rispetto dell'eguaglianza passa anche e soprattutto attraverso la tutela del

[23] *Feret c. Belgio,* ric. 15615/07 (2009), § 73. Il ricorrente è il Presidente del partito politico belga *Front National* il quale, durante una campagna elettorale, oltre a comizi dai toni efferati, aveva fatto distribuire degli stampati in cui si illustrava con veemenza il programma di governo incentrato sull'opposizione all'islamizzazione del Belgio. Questo prevedeva, tra i diversi punti, il rimpatrio forzato degli immigrati e la concessione dell'asilo politico ai soli cittadini europei. I giudici interni lo condannano quindi a scontare una pena detentiva di dieci mesi, a svolgere attività di volontariato per un totale di 250 ore in un centro per l'integrazione di stranieri migranti, e all'interdizione dall'elettorato passivo per sei anni. Strasburgo dà ragione allo Stato, non riscontrando quindi la violazione dell'art. 10 CEDU. Sul concetto di esercizio "responsabile" della libertà di manifestazione del pensiero d'odio, C. Frances Moran, *Responsibility and freedom of speech under article 10*, in *Eu. Hum. Rights Law Rev.*, 1, 2020, 67 ss.

[24] C. McCrudden, *Freedom of Speech and Racial Equality*, in P.B. H. Birks (ed.), *Pressing Problems in the Law*, vol. 1, *Criminal Justice and Human Rights*, Oxford, 1995, 125 ss.

[25] La prima modifica si è avuta con la legge n. 205/1993, meglio nota come "legge Mancino"; la seconda con la legge n. 85/2006, aspramente criticata in dottrina. C. Fiore, *I limiti di espressione dell'antagonismo politico*, in *Riv. it. dir. proc. pen.*, 2, 2016, 893 ss.; A. Spena, *Libertà di espressione e reati di opinione*, in *Riv. it. dir. proc. pen.*, 2, 2007, 689 ss.; M. Pellissero, *Osservazioni critiche sulla legge in tema di reati di opinione: occasioni mancate e incoerenze sistematiche*, in *Dir. pen. proc.*, 8, 2006, 960 ss.; D. Pulitanò, *Riforma dei reati d'opinione?*, in *Corr. giur.*, 6, 2006, 745 ss.

[26] Per la rassegna di tale giurisprudenza sia consentito il rimando a P. Tanzarella, *Discriminare parlando*, cit., 136-169.

principio di non discriminazione, non stupisce che gli *hate speeches* abbiano finito con l'essere sanzionati altresì nei procedimenti civili. Ciò è potuto accadere per aver inserito nel decreto legislativo n. 215/2003 – che dà attuazione alla direttiva comunitaria 2000/43/CE «per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica» – il divieto di molestia per discriminazione qualora questa si sostanzi in un «comportamento indesiderato posto in essere per motivi di razza o di origine etnica, aventi lo scopo o l'effetto di violare la dignità di una persona e di creare un clima intimidatorio, ostile, degradante, umiliante e offensivo»[27].

L'interpretazione data dai giudici civili a tale disposizione va nel senso di considerare come "comportamenti" molesti non solo l'adozione di atti materiali di discriminazione, ma anche la comunicazione verbale o scritta di messaggi discriminatori. Tra l'altro, mentre i giudici penali sono costretti a valutare l'elemento soggettivo del dolo (generico o specifico) e quello oggettivo del pericolo (astratto o concreto) – nonostante entrambi siano sempre più ricordati in modo apodittico senza che se ne appuri la loro reale incidenza nel caso di specie – i giudici civili sono esentati dal motivare il nesso di causalità tra pensiero razzista e atto materiale di discriminazione. Infatti, la generica formula "comportamento indesiderato" a cui fa riferimento il testo legislativo consente loro di attribuire alla diffusione di un messaggio (in forma scritta o verbale) una valenza di per sé discriminatoria[28].

Questa impostazione ha potuto facilmente essere adottata anche per valutare l'incidenza dei discorsi omofobi sulla parità di trattamento in materia di occupazione e di condizioni di lavoro, disciplinata dal decreto legislativo n. 215/2003, che ha dato attuazione alla direttiva 2000/78/CE e che rappresenta altresì la normativa di riferimento per la risoluzione del caso di specie che in questa sede si sta commentando.

Nientemeno, la definizione offerta dal testo legislativo che identifica la discriminazione diretta come quella situazione in cui «una persona è trattata meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga»[29], introduce, a parere dei giudici, sia una comparazione attuale, che una meramente ipotetica. Di conseguenza, «è atta a integrare discriminazione anche una condotta che, solo sul piano astratto, impedisce o rende maggiormente difficoltoso l'accesso all'occupazione»[30].

Il punto su cui più s'insiste maggiormente è l'effetto demoralizzante e dissuasivo delle dichiarazioni discriminatorie rese nei confronti di quelle persone che si vorrebbero escludere. O, meglio, il tipo «di pregiudizio, anche soltanto potenziale, che una categoria di soggetti potrebbe subire in termini di svantaggio o di maggiore difficoltà, rispetto ad altri non facenti parte di quella categoria, nel reperire un bene della vita, quale l'occupazione»[31].

---

[27] Art. 2, c. 3, l. 215/2003.

[28] Diverse sono le ordinanze pronunciate dai giudici civili. Ad es., Trib. Brescia, sez. volontaria giurisdizione, ord. 31 gennaio 2012; Trib. Milano, sez. I civ., ord. 28 maggio 2012; Trib. Pescara, sez. civ., 21 giugno 2013; Trib. Roma, sez. I civ., 16 febbraio 2015; Trib. Milano, sez. I civ., ord. 16 aprile 2016; Trib. Milano, sez. I civ., 22 febbraio 2017. Sulle motivazioni proposte se si vuole si rimanda ancora a P. Tanzarella, *Discriminare parlando*, cit., 169-183.

[29] Art. 1, d.lgs. 216/2003.

[30] Trib. Bergamo, ord. 6 agosto 2014, cit.

[31] App. Brescia, sez. lav., 11 dicembre 2014, cit.

Concludendo, sia per Strasburgo sia per i giudici italiani i discorsi che usano parole sgradite, non confacenti a un registro verbale *polite*[32], non possono essere ritenute manifestazioni di opinioni costituzionalmente garantite, perché considerate pensieri-non pensiero, bensì pensieri-azione. Viene così rispolverata la vecchia dottrina penalistica dei limiti logici all'art. 21 Cost[33]. A differenza però di quando fu formulata, tale teoria oggi acquista una nuova veste in quanto il pensiero che si fa azione non consiste necessariamente in un atto violento, ma anche, come ormai chiaro, in un atto discriminatorio. Le manifestazioni d'odio non sarebbero "logicamente" pensieri perché espressioni irrazionali che inducono chi ascolta a rifiutare il prossimo, invece che riconoscerlo come un proprio pari. La difesa della pari dignità sociale, i rischi psico-sociali, il mutuo riconoscimento sono quindi gli argomenti per giustificare la limitazione della libertà d'espressione[34].

5. Una nuova veste per il principio di non discriminazione e le conseguenze possibili sul ruolo della Corte di giustizia

Considerata la prospettiva appena descritta, il bilanciamento tra libertà d'espressione e il principio di non discriminazione proposto dalla Corte di giustizia non rappresenta affatto una nota dissonante rispetto agli orientamenti di Strasburgo e della giurisprudenza ordinaria italiana. Eppure, il modo di argomentare di Lussemburgo nel caso in questione risulta essere fuori dal coro rispetto alla sua propria giurisprudenza pregressa. Le affermazioni relative ai limiti ammessi alla libertà d'espressione e l'interpretazione data al principio di non discriminazione dimostrano come la Corte di giustizia si trovi una volta di più di fronte a una crisi identitaria, divisa tra il suo classico ruolo di custode dei Trattati e quello peculiare di giudice dei diritti, certamente non inedito,

[32] Sui rischi dell'uso spropositato del *politally correct* e dei suoi effetti controproducenti, E. Capozzi, *Politicamente corretto. Storia di un'ideologia*, Venezia, 2018.

[33] G. Bettiol, *Sui limiti penalistici alla libertà di manifestazione del pensiero*, in *Riv. it. dir. e proc. pen.*, 1965, 641 ss.; G. Zuccalà, *Personalità dello Stato, ordine pubblico e tutela della libertà di pensiero*, in *Riv. it. dir. proc. pen.*, 1966, 1154 ss. Insiste sull'opportunità di distinguere tra le forme espressive lecite e quelle illecite anche Nuvolone, il quale ritiene che resterebbero escluse dalla protezione costituzionale della libera manifestazione del pensiero le espressioni «attivizzanti, teleologicamente orientate a suscitare nei destinatari comportamenti modificatori della realtà». P. Nuvolone, *Il problema dei limiti della libertà di pensiero nella prospettiva logica dell'ordinamento*, in Aa.Vv., *Legge penale e libertà del pensiero*, Padova, 1966, 350 ss., spec. 353.

[34] La teorizzazione di questa rinnovata dottrina dei limiti logici arriva dagli Stati Uniti. Particolarmente influenti sono i membri della *Critical Race Theory*, i quali partono dal presupposto che le offese gratuite a danno delle minoranze creano gravi disagi a livello psicologico e sociale in termini di autostima e di accettazione, tali non solo da ledere la dignità umana, ma da contaminare anche l'ambiente circostante, provocando il rischio di disordini con una conseguente instabilità politica. Su una puntuale esplicazione della teoria v. R. Delgado - J. Stefancic, *Critical Race Theory. An introduction*, New York, 2012. Tra gli studiosi italiani cfr. G. Pino, *Discorso razzista e libertà di manifestazione del pensiero*, in *Pol. dir.*, 2008, 307 ss. Particolarmente suggestiva è anche la tesi di Jeremy Waldron, il quale sostiene che una società oltre che "essere", deve anche "apparire" ordinata, tanto da non ritenere necessario che per punire i discorsi d'odio alla loro diffusione debbano seguire atti discriminatori tangibili. J. Waldron, *The Harm in Hate Speech*, Cambridge, 2012.

ma che fatica ad assumere una forma regolare[35]. Guardare più da vicino a questi aspetti aiuta a cogliere meglio il punto.

Lo schema di giudizio adottato per valutare la libertà d'espressione

Per valutare la compressione della libera manifestazione del pensiero viene richiamata la sua natura non assoluta e la conseguente e necessaria verifica del principio di proporzionalità tra i limiti apposti e gli obiettivi da perseguire.

Questi argomenti sono entrambi previsti dalla Carta di Nizza al primo paragrafo dell'art. 52 e utilizzati tipicamente da qualunque Corte costituzionale, così come da Strasburgo. Si pensi ad esempio alla giurisprudenza del nostro giudice delle leggi a tal riguardo. Nella sua prima sentenza aveva affermato che «il concetto di limite è insito nel concetto di diritto»[36], senza però farsi sfuggire l'occasione di dichiarare successivamente che le limitazioni alla libertà di manifestazione del pensiero possono trovare fondamento solo in altri diritti, beni, interessi o valori di rango costituzionale[37].

Come si accennava, è la stessa tecnica che la Corte di giustizia adotta, se non fosse che l'osservanza del criterio della proporzionalità viene solo annunciato, ma non affatto verificato in concreto. Ci si limita ad asserire da un lato che il contenuto essenziale della libertà d'espressione è rispettato visto che le limitazioni applicate «si applicano unicamente al fine di raggiungere gli obiettivi della direttiva 2000/78, ossia garantire il principio della parità di trattamento in materia di occupazione e di lavoro e la realizzazione di un elevato livello di occupazione e di protezione sociale»[38]; dall'altro lato che «limitazioni siffatte rispettano altresì il principio di proporzionalità, nella misura in cui […] l'ingerenza nell'esercizio della libertà di espressione non va oltre quanto è necessario per realizzare gli obiettivi di tale direttiva, vietando unicamente le dichiarazioni che costituiscono una discriminazione in materia di occupazione e di lavoro»[39].

La proporzionalità sarebbe cioè rispettata per il sol fatto che vengono censurate esclusivamente le dichiarazioni relative "all'argomento" lavoro, non per la loro incidenza effettiva sulle condizioni di accesso a un determinato posto occupazionale. Come già spiegato più volte, non ci si pone il problema di verificare il nesso causa-effetto, che rappresenterebbe invero il tratto peculiare dello schema di giudizio della proporzionalità. L'effetto è insito nella causa: frasi dal sapore discriminatorio si sostanziano in un trattamento sfavorevole perché automaticamente dissuadono i destinatari a cui

[35] Naturalmente si fa qui riferimento al modo in cui la Corte di giustizia si è per prima costruita il ruolo di giudice dei diritti in via pretoria dal caso *Stauder* in poi per assicurare il principio del primato del diritto dell'Unione attraverso il richiamo alle tradizioni costituzionali comuni e ai diritti contemplati nella Convenzione europea dei diritti dell'uomo. Per tutti, cfr. M. Cartabia, *L'ora dei diritti fondamentali nell'Unione europea*, in Ead. (a cura di), *I diritti in azione*, Bologna, 2007.

[36] Corte cost., sent. 1/1956. Molto critico rispetto a tale assunto Esposito il quale avvertiva del pericolo di giustificare in via generale limiti alle libertà costituzionalmente garantite e in particolare alla libertà di manifestazione del pensiero. C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958, 15.

[37] Cfr. *ex multis*, Corte cost., sentt. 19/1962 e 9/1965. Per una carrellata dei limiti impliciti utilizzati per la tutela di beni di rango costituzionale individuati dalla giurisprudenza costituzionale cfr. E. Lamarque, *I reati d'opinione*, cit., 155-157.

[38] CGUE, causa C-507/18, cit., § 51.

[39] Ivi, § 52.

sono rivolte dal candidarsi a un posto di lavoro. Il bilanciamento è solo apparante, non proponendo ad esempio nessun argomento per misurare l'eventuale incidenza sul principio del pluralismo, altrettanto caposaldo di riferimento dell'integrazione europea e citato accanto alla non discriminazione come valore fondante dell'Unione. Manca, in sostanza, un ragionamento che è proprio di un giudice costituzionale.

Lo schema di giudizio adottato per valutare il principio di non discriminazione

Se il pressapochismo del giudizio sulla limitazione della libertà d'espressione sconcerta – così come sconcerta quello fatto proprio da Strasburgo e dai giudici comuni italiani – ancora più sbalorditivo risulta essere lo schema di giudizio (non) adottato per valutare la sussistenza della discriminazione denunciata.

Come noto, la discriminazione diretta si caratterizza per il trattamento sfavorevole riservato a una persona. Ad esempio, per il rifiuto dell'accesso a un ristorante o esercizio commerciale, l'attribuzione di una pensione o retribuzione inferiore, l'età di pensionamento più alta o più bassa, l'impossibilità di accedere a una determinata professione, il divieto di indossare simboli religiosi, il rifiuto o la revoca di prestazioni previdenziali. Tuttavia, ai fini della discriminazione, tale trattamento sfavorevole assume rilievo nella misura in cui possa essere raffrontato col trattamento riservato a un'altra persona che si trovi in situazione analoga. Pertanto è necessario avere un termine di confronto, vale a dire una persona in circostanze "materiali" paragonabili, che si differenzi dalla presunta vittima principalmente per la caratteristica che forma oggetto del divieto di discriminazione[40].

Appare evidente come nel caso di specie non solo manchi tale termine di confronto, ma manca nientemeno la eventuale vittima. Infatti, giova ripeterlo, la discriminazione denunciata è solo presunta ed ipotetica.

Cosa spinge allora la Corte a proporre l'argomentazione utilizzata nella sentenza e che prescinde del tutto da questo schema? È vero che il principio di non discriminazione ha gradualmente indossato nuove vesti, divenendo dapprima – in via pretoria – un principio generale dell'ordinamento tale da tutelare situazioni che sarebbero altrimenti rimaste escluse dall'ambito delle competenze dell'Unione se si fosse stati costretti a basarsi solo sulla verifica dell'efficacia diretta delle direttive[41]; in seguito divenendo un valore fondante dei trattati che ha legittimato esplicitamente l'adozione di direttive con effetti diretti orizzontali. Tuttavia, arrivare a sostenere la sussistenza di una discriminazione in assenza di un caso concreto – come fa oggi la Corte di giustizia nel caso Taormina – potrebbe rappresentare il canale per moltiplicare i ricorsi attraverso cui

[40] Sulla necessità di individuare un «termine di confronto» idoneo insiste la giurisprudenza della Corte di giustizia nel caso in cui la vittima della discriminazione sia una donna in gravidanza. *Leading case* CGUE, C-177/88, *Dekker c. Stichting Vormingscentrum voor Jong Volwassenen (VJV-Centrum) Plus* (1990); nello stesso senso CGUE, C-32/93, *Webb c. EMO Air Cargo (UK) Ltd* (1994). In dottrina, sui casi relativi all'antidiscriminazione, tra i molti, E. Ellis - P. Watson, *EU Anti-Discrimination Law*, Oxford, 2012; S. Fredman, *Discrimination Law*, Oxford 2002.

[41] Leading case CGUE, C-144/04, *Werner Mangold c Rüdiger Helm* (2005). Tra i commentatori, L. Cappuccio, *Il caso Mangold e l'evoluzione della giurisprudenza comunitaria sul principio di non discriminazione*, in M. Cartabia (a cura di), *Dieci casi sui diritti in Europa*, cit., 111 ss; A. D'Aloia, *Il principio di non discriminazione e l'integrazione europea «attraverso» la Corte di Giustizia: riflessi del caso* Mangold, ivi, 125 ss.

vengono rivendicati i diritti in sede europea[42] e sui cui la Corte mostra di non essere attrezzata per effettuare un adeguato bilanciamento e per fornire i giusti rimedi[43].
Vi è da chiedersi se questa nuova tendenza non sia semplicemente il frutto di una politica "protettiva" delle istituzioni sovranazionali e nazionali nei confronti dei gruppi deboli – Corte di giustizia compresa – e che le porta tutte a prendere le distanze da certi atteggiamenti immorali censurandoli giuridicamente. Oppure, se questa è una strada che sarà percorsa anche in giudizi futuri relativi alla protezione di tanti altri diritti fondamentali intrecciati alla non discriminazione. Se così fosse, il confronto tanto richiesto dalla Corte costituzionale italiana, concretizzatosi sia con il promovimento delle questioni pregiudiziali da parte sua stessa alla Corte di giustizia sia con lo strumento della doppia pregiudizialità a disposizione dei giudici comuni, si rivelerebbe proficuo, nonostante irto di conflitti e d'incertezze[44].
La protezione dei diritti fondamentali da parte delle giurisdizioni costituzionali nazionali e da parte della Corte di giustizia necessita quanto mai di un serrato contraddittorio. Le debolezze del giudizio europeo sono ormai evidenti quando in gioco ci sono i diritti fondamentali, soprattutto per la propensione della Corte ad allargare le competenze dell'Unione, invece che contenerle in stretti confini[45]. Non sarebbe allora peregrino ragionare attorno all'ultima proposta di Weiler e Sarmiento i quali, criti-

[42] Sulla spinta che la normazione europea ha dato ai cittadini per ricorrere a Lussemburgo e rivendicare la protezione dei diritti fondamentali, E. Muir - C. Kilpatrick - J. Miller - B. de Witte (eds.), *How EU Law Shapes Opportunities for Preliminary References on Fundamental Rights: Discrimination, Data Protection and Asylum*, in *EUI Working Paper*, 7, 2017.

[43] A tal proposito, cfr. M. Dawson - E. Muir - M. Claes, *Enforcing the EU's Rights Revolution: The Case of Equality*, in *Eur. H. R. Law Rev.*, 3, 2012, 276 ss.

[44] Non è questa la sede per ripercorrere i passi compiuti finora in termini di dialogo tra le due Corti. Basti ricordare la saga Taricco e quanto è scaturito dall'*obiter dictum* della sentenza della Corte cost. n. 269/2017. Tra i diversi commenti in dottrina, *ex multis*, R. Conti, *La Cassazione dopo Corte cost. n. n. 269/2017. Qualche riflessione, a seconda lettura*, in *Forum di Quad. Costituzionali*, 2017; G. Di Federico, *La "saga Taricco": il funzionalismo alla prova dei controlimiti (e viceversa)*, in *Federalismi.it*, 11, 2018, 14 ss.; M. L. Ferrante, *La vicenda "Taricco" e la sentenza della Corte di Giustizia dell'Unione europea*, in *Diritti fondamentali*, 1, 2018; D. Gallo, *Efficacia diretta del diritto UE, procedimento pregiudiziale e Corte costituzionale: una lettura congiunta delle sentenze n. 269/2017 e 115/2018*, in *Rivista AIC*, 1, 2019, 220 ss.; A. Guazzarotti, *La sentenza n. 269 del 2017: un «atto interruttivo dell'usucapione» delle attribuzioni della Corte costituzionale?*, in *Quad. costituzionali*, 1, 2018, 194 ss.; R. Mastroianni, *Da Taricco a Bolognesi, passando per la ceramica Sant'agostino: il difficile cammino verso una nuova sistemazione tra Carte e Corti*, in *Osservatorio sulle fonti*, 1, 2018; M. Nisticò, *Taricco II: il passo indietro della Corte di giustizia e le prospettive del supposto dialogo tra le Corti*, in *Osservatorio Costituzionale*, 1, 2018; G. Repetto, *Concorso di questioni pregiudiziali (costituzionale ed europea), tutela dei diritti fondamentali e sindacato di costituzionalità*, in *Giur. Cost.*, 6, 2017, 2955 ss.; L.S. Rossi, *La sentenza n. 269/2017della Corte costituzionale italiana: obiter "creativi" (o distruttivi?) sul ruolo dei giudici italiani di fronte al diritto dell'Unione europea*, in *Federalismi.it*, 3, 2018; A. Ruggeri, *Svolta della Consulta sulle questioni di diritto eurounitario assiologicamente pregnanti, attratte nell'orbita del sindacato accentrato di costituzionalità, pur se riguardanti norme dell'Unione self-executing (a margine di Corte cost. n. 269 del 2017)*, *Rivista di Diritti comparati,* 3, 2017, 234 ss.; G. Scaccia, *Giudici comuni e diritto dell'Unione europea nella sentenza della Corte costituzionale n. 269 del 2017*, in *Osservatorio Costituzionale*, 2, 2017, 2948 ss.; C. Schepisi, *I futuri rapporti tra le Corti dopo la sentenza n. 269/2017 e il controllo erga omnes alla luce delle reazioni dei giudici comuni*, in *Federalismi.it*, 22, 2018, 2 ss.; D. Tega, *La sentenza n. 269 del 2017: il concorso di rimedi giurisdizionali costituzionali ed europei*, in *Quad. costituzionali*, 1, 2018, 197 ss.

[45] Sulla necessità del confronto invece che dello scontro tra giurisdizione europea e giurisdizione costituzionale nazionale insistono anche A. Bogdandy - D. Paris, *La forza si manifesta pienamente nella debolezza. Una comparazione tra la Corte costituzionale e il Bundesverfassungsgericht*, in *Quad. costituzionali*, 1, 2020, 9 ss.

cando la mancanza dell'appellabilità delle decisioni della Corte di giustizia, ritengono necessario prevedere un secondo grado di giudizio limitato a casi eccezionali – che interessano le attribuzioni in tema di diritti – e valutato da una Corte composta sia da giudici della Corte di giustizia sia da giudici costituzionali o delle Supreme Corti nazionali[46].

[46] D. Sarmiento - J.H.H. Weiler, *The EU Judiciary After Weiss-Proposing a New Mixed Chamber of the Court of Justice: A Position Paper*, in *Int'l J. Const. L. Blog*, 2 giugno 2020.

Oltre il mero stoccaggio di prodotti in contraffazione di marchio: una riflessione sul caso *Amazon* deciso dalla Corte di giustizia dell'Unione europea

Alice Fratti – Riccardo Traina Chiarini

Corte di giustizia dell'Unione europea, 2 aprile 2020, C-567/18, *Coty Germany GmbH c. Amazon Services Europe e altri*

L'art. 9, par. 2, lett. *b)*, del regolamento (CE) 207/2009 e l'art. 9, par. 3, lett. *b)*, del regolamento (UE) 2017/1001 devono essere interpretati nel senso che una persona che conservi per conto di un terzo prodotti che violano un diritto di marchio, senza essere a conoscenza di tale violazione, si deve ritenere che non stocchi tali prodotti ai fini della loro offerta o della loro immissione in commercio ai sensi delle succitate disposizioni, qualora non persegua essa stessa dette finalità.

Sommario

1. Le parti del procedimento e i fatti oggetto di causa. - 2. La decisione della Corte di giustizia. - 3. Le conclusioni dell'Avvocato Generale. - 4. La responsabilità degli intermediari. - 5. Considerazioni finali.

Keywords

vendite online – *marketplace* – Corte di giustizia – marchi – Internet service provider

1. Le parti del procedimento e i fatti oggetto di causa

La controversia alla base della decisione della Corte di giustizia dell'Unione europea (*infra*, la "Corte") aveva ad oggetto la vendita sulla piattaforma marketplace www.amazon.de di flaconi di profumo a marchio Davidoff, da parte di un venditore terzo e senza l'autorizzazione della società Coty Germany Gmbh (*infra*, "Coty"), licenziataria del marchio.

Come è noto, nell'ambito della piattaforma Amazon Marketplace le società del gruppo Amazon offrono a venditori terzi la possibilità di pubblicare offerte di vendita dei propri prodotti e di concludere contratti di vendita con gli utenti, nonché di prendere parte al programma "Logistica di Amazon", con possibilità di stoccare i prodotti all'interno di depositi delle varie società del gruppo e di usufruire di altri servizi complementari,

come ad esempio la pubblicità, il servizio clienti per le richieste di informazioni, la gestione dei resi, i rimborsi dei prodotti difettosi e la ricezione dal cliente del pagamento delle merci, che viene poi trasferito al venditore sul suo conto bancario.

In particolare, la società Amazon Services Europe S.à.r.l. (*infra*, "Amazon Services") consente ai venditori terzi di pubblicare offerte dei loro prodotti sulla piattaforma Amazon Marketplace, mentre la società Amazon FC Graben GmbH (*infra*, "Amazon FC") è incaricata di gestire l'immagazzinamento e il deposito di prodotti affidati dal venditore terzo.

Nel caso alla base della decisione in commento, Coty lamentava in particolare che in relazione ad alcuni flaconi di profumo a marchio Davidoff offerti in vendita da un venditore terzo e affidati dalla venditrice ad Amazon FC nell'ambito del programma "Logistica Amazon" i diritti conferiti dal marchio controverso non si erano esauriti, non trattandosi di prodotti immessi in commercio nell'Unione europea dal titolare del marchio o con il suo consenso[1].

Ritenendo i comportamenti di Amazon Services e di Amazon FC in violazione dei propri diritti di marchio, Coty citava le due società a comparire davanti al Landgericht di Monaco, chiedendo in via principale che fosse loro inibito lo stoccaggio o la spedizione in Germania, anche da parte di terzi, di profumi recanti il marchio Davidoff che non fossero immessi in commercio all'interno del territorio dell'Unione europea con il suo consenso.

Le domande di Coty venivano rigettate sia in primo che in secondo grado. In particolare, il giudice d'appello concludeva che Amazon Services non avesse né stoccato né spedito i prodotti in questione, e che Amazon FC avesse conservato tali prodotti per conto del venditore terzo in qualità di depositario che non fornisce alcuna assistenza alla vendita dei prodotti che ha in deposito.

Coty proponeva dunque ricorso per cassazione dinanzi al Bundesgerichtshoff (Corte federale di giustizia tedesca) che, a seguito di una ricostruzione fattuale non del tutto pacifica tra le parti[2], decideva di sospendere il procedimento e rimettere alla Corte di giustizia europea il seguente quesito: «Se una persona che conserva per conto di un

[1] Al riguardo, l'art. 15 del regolamento (UE) 2017/1001, rubricato "Esaurimento del diritto conferito dal marchio UE" prevede che «Il diritto conferito dal marchio UE non permette al titolare di impedirne l'uso per prodotti immessi in commercio nello Spazio economico europeo con tale marchio dal titolare stesso o con il suo consenso». Dalla decisione di primo grado emerge in particolare che Coty contestava ad Amazon la vendita di prodotti immessi per la prima volta in commercio al di fuori dello Spazio Economico Europeo (in particolare, in Pakistan) e poi successivamente importati in Germania senza il consenso del titolare del marchio.

[2] Coty ha contestato la ricevibilità della questione pregiudiziale sostenendo che la decisione di rinvio non rispecchiava in realtà la situazione oggetto della controversia. È stato in particolare sostenuto che la descrizione delle società resistenti nel procedimento principale contenuta nella decisione di rinvio non riflette sufficientemente «il ruolo svolto da Amazon Services Europe e da Amazon FC Graben per quanto riguarda l'immissione in commercio dei prodotti di cui trattasi», poiché «nella comunicazione ai fini della vendita e al momento dell'esecuzione del contratto di vendita tali società si sostituiscono interamente al venditore. Inoltre, su ordine di Amazon Services Europe e di Amazon EU, Amazon Europe Core promuoverebbe in modo continuativo i prodotti sul sito Internet www.amazon.de mediante annunci pubblicitari nel motore di ricerca Google che rinvierebbero a offerte tanto di Amazon EU a proprio nome quanto di terzi, gestite da Amazon Services Europe. Pertanto, considerata nel suo insieme, l'attività delle resistenti nel procedimento principale andrebbe ben oltre il ruolo svolto dalla società eBay nella causa all'origine della sentenza del 12 luglio 2011, L'Oréal» (§ 20 della sentenza).

terzo prodotti che violano un diritto di marchio, senza essere a conoscenza di tale violazione, effettui lo stoccaggio di tali prodotti ai fini dell'offerta o dell'immissione in commercio, nel caso in cui solo il terzo, e non anche essa stessa, intenda offrire o immettere in commercio detti prodotti»[3].

2. La decisione della Corte di giustizia

La questione oggetto del rinvio pregiudiziale riguardava in particolare l'interpretazione dell'art. 9, parr. 1 e 2, del regolamento (UE) 207/2009, applicabile all'epoca dei fatti e poi sostituito dall'art. 9, parr. 1 e 2, del regolamento (UE) 2017/1001, che dispone che la registrazione del marchio dell'Unione europea conferisce al suo titolare il diritto esclusivo di vietare a qualsiasi terzo di usare nel commercio un segno identico a tale marchio per prodotti o servizi identici a quelli per cui esso è stato registrato[4].
In particolare, in tali disposizioni viene riportato un elenco non tassativo, e quindi di carattere meramente esemplificativo, dei tipi di uso che possono essere vietati dal titolare di un marchio, tra cui figurano l'offerta dei prodotti, la loro immissione in commercio, nonché il loro stoccaggio effettuato a tali fini[5].
La Corte è pertanto stata chiamata a stabilire se l'attività di magazzinaggio di prodotti effettuata dalle società Amazon, così come descritta dal giudice del rinvio[6], possa essere considerata un "uso" del marchio e, in particolare, se configuri uno "stoccaggio" dei prodotti ai fini della loro offerta o della loro immissione in commercio, attività dunque che rientra nell'ambito di esclusiva del titolare del marchio.
In primo luogo, la Corte richiama favorevolmente principi già espressi in proprie decisioni precedenti dai quali si evince che gli intermediari, come i depositari di merci e i trasportatori che prestano servizi per conto di terzi, non sono responsabili delle violazioni dei diritti di marchio che questi ultimi potrebbero eventualmente commettere, in quanto essi non utilizzano il segno nella loro comunicazione commerciale, né nelle loro attività economiche. In particolare, nel caso del depositario, è stato affermato che «la fornitura da parte sua del servizio di deposito di merci recanti un marchio altrui non costituisce un uso [di un] segno identico a tale marchio per prodotti o servizi identici o

[3] §18.

[4] Art. 9, parr. 1 e 2, regolamento (UE) 2017/1001, che dispone che «1. La registrazione del marchio UE conferisce al titolare un diritto esclusivo. 2. Fatti salvi i diritti dei titolari acquisiti prima della data di deposito o della data di priorità del marchio UE, il titolare del marchio UE ha il diritto di vietare ai terzi, salvo proprio consenso, di usare nel commercio, in relazione a prodotti o servizi, qualsiasi segno quando: a) il segno è identico al marchio UE ed è usato in relazione a prodotti e servizi identici ai prodotti o ai servizi per i quali il marchio UE è stato registrato».

[5] Art. 9, par. 3, lett. *b)*, che prevede che «Possono essere in particolare vietati (…) l'offerta, l'immissione in commercio o lo stoccaggio dei prodotti a tali fini oppure l'offerta o la fornitura di servizi sotto la copertura del segno».

[6] Dall'impostazione fattuale della decisione di rinvio risultava, da un lato, che le società del gruppo Amazon si erano limitate al magazzinaggio dei prodotti contrassegnati dal marchio, senza averli offerti in vendita o averli immessi in commercio esse stesse, e, dall'altro, che esse non intendevano offrire tali prodotti in vendita o immetterli in commercio.

simili a quelli per cui detto marchio è registrato»[7]. Nella medesima prospettiva, la Corte ha anche valorizzato che nel caso del gestore di un mercato elettronico «l'esistenza di un "uso" di un segno identico o simile al marchio del titolare da parte di un terzo comporta, quanto meno, che quest'ultimo utilizzi il segno nell'ambito della propria comunicazione commerciale. Orbene, nei limiti in cui tale terzo fornisce un servizio consistente nel permettere ai propri clienti di far comparire, nell'ambito delle loro attività commerciali quali le loro offerte in vendita, segni corrispondenti a marchi sul proprio sito, non è lui stesso a fare, su tale sito, un uso dei detti segni nel senso indicato dalla summenzionata normativa dell'Unione»[8].

Nella sua analisi la Corte opera quindi una distinzione tra gli operatori economici per stabilire se vi sia un uso del marchio ed osserva che tale uso non sussiste quando il terzo semplicemente fornisca una soluzione tecnica necessaria per l'uso di un segno, o comunque tenga un comportamento passivo senza controllo diretto o indiretto sull'atto che costituisce l'uso.

A tale riguardo, la Corte ha osservato che il verbo "usare" implica necessariamente un comportamento attivo e di controllo, di tipo diretto o indiretto, sull'atto che costituisce l'uso del marchio e che quindi «il fatto di creare le condizioni tecniche necessarie per l'uso di un segno e di essere remunerati per tale servizio non significa che chi rende tale servizio usi egli stesso il segno»[9], mentre solo il soggetto terzo che abbia il controllo è effettivamente in grado di cessare tale uso e quindi di conformarsi al divieto[10].

Alla luce di tali considerazioni la Corte conclude pertanto nel senso che affinché il magazzinaggio di prodotti contraddistinti da un segno identico o simile al marchio possa essere qualificato come "uso" di tale segno, è necessario che «l'operatore economico che effettua tale magazzinaggio persegua in prima persona le finalità cui si riferiscono tali disposizioni, che consistono nell'offerta dei prodotti o nella loro immissione in commercio» e, quindi, nel caso in cui le società che hanno eseguito lo stoccaggio «non (abbiano; *n.d.r.*) esse stesse offerto in vendita i prodotti di cui trattasi né li (abbiano; n.d.r.) immessi in commercio, (…) esse non fanno, di per sé, uso del segno nell'ambito della loro comunicazione commerciale»[11].

Si noti come in motivazione nessuna considerazione viene, apparentemente, data al fatto che Coty avesse messo le società convenute a conoscenza dell'illiceità dei prodotti contestati. Eppure la circostanza costituisce evidentemente un presupposto (negativo) fondamentale dell'intero ragionamento, essendo specificata nella stessa questione pregiudiziale, che infatti riguarda il caso di colui che operi per conto di terzi su prodotti che violano diritti di marchio «senza essere a conoscenza di tale violazione». Seppure

[7] CGUE, C-379/14, *TOP Logistics c. Bacardi* (2015), § 45.

[8] CGUE, C-324/09, *L'Oréal c. e-Bay* (2011), §§ 102-103.

[9] §§ 37, 38 e 43.

[10] Sotto questo profilo, la Corte nella sua giurisprudenza precedente ha già avuto modo di chiarire che l'espressione "usare nel commercio" implica necessariamente «un comportamento attivo e un controllo, diretto o indiretto, sull'atto che costituisce l'uso. Orbene, ciò non è il caso se tale atto è effettuato da un operatore indipendente senza il consenso dell'inserzionista, o addirittura contro l'espressa volontà di quest'ultimo» (CGUE, C-179/15, *Daimler c. Együd Garage* (2016), § 39: si veda anche CGUE, C-129/17, *Mitsubishi c. Duma* (2018), §38.

[11] §§ 45 e 47.

non costituisca oggetto di specifica argomentazione da parte della Corte, dunque, tale circostanza assume infine rilevanza nelle conclusioni cui essa giunge, risolvendo la questione sottopostale come segue: «L'articolo 9, paragrafo 2, lettera b), del regolamento (CE) n. 207/2009 del Consiglio, del 26 febbraio 2009, sul marchio [dell'Unione europea], e l'articolo 9, paragrafo 3, lettera b), del regolamento (UE) 2017/1001 del Parlamento europeo e del Consiglio, del 14 giugno 2017, sul marchio dell'Unione europea, devono essere interpretati nel senso che una persona che conservi per conto di un terzo prodotti che violano un diritto di marchio, senza essere a conoscenza di tale violazione, si deve ritenere che non stocchi tali prodotti ai fini della loro offerta o della loro immissione in commercio ai sensi delle succitate disposizioni, qualora non persegua essa stessa dette finalità»[12].

3. Le conclusioni dell'Avvocato Generale

Particolare interesse nel caso in esame è stato suscitato dalle conclusioni dell'Avvocato Generale (*infra*, "AG") che hanno fornito anche un'impostazione alternativa dei fatti di causa la quale, come vedremo, non pare essere stata presa in considerazione (almeno apparentemente) dalla Corte nelle sue conclusioni[13].

L'AG osserva infatti che il quesito, così come formulato dalla corte di rinvio, non può che ottenere una risposta nel senso di escludere che le società Amazon Services e Amazon FC utilizzino il marchio in esame nella loro comunicazione commerciale e nelle loro attività economiche. L'AG suggerisce dunque alla Corte di rispondere alla questione pregiudiziale nel senso che, nel caso in cui un soggetto non abbia conoscenza della violazione e solo il venditore terzo intenda offrire o immettere in commercio i prodotti, si debba ritenere che non venga effettuata un'attività qualificabile come stoccaggio di prodotti lesivi dei diritti di marchio ai fini dell'offerta o dell'immissione in commercio.

Osserva però l'AG che le conclusioni potrebbero essere parzialmente diverse nel caso in cui si adottasse un'interpretazione alternativa dei fatti che ponga l'accento sulla situazione specifica delle imprese Amazon in quanto ampiamente implicate nella commercializzazione dei prodotti in questione nell'ambito del programma "Logistica Amazon"[14].

Le imprese del gruppo Amazon, infatti, non si occuperebbero esclusivamente di attività ritenute "neutre", come lo stoccaggio e il trasporto dei prodotti, bensì di una gamma ulteriore di servizi[15], i quali comporterebbero il «coinvolgimento attivo e coordinato

[12] Cfr. conclusioni della sentenza.

[13] Conclusioni dell'Avvocato Generale M. Campos Sànchez-Bordona, 28 novembre 2019.

[14] Si veda § 51 delle Conclusioni dell'Avvocato Generale.

[15] Si veda § 56 delle Conclusioni dell'Avvocato Generale, ove viene osservato che «il venditore consegna ad Amazon i prodotti selezionati dal cliente e le imprese del gruppo Amazon li ricevono, li stoccano nei loro centri di distribuzione, li preparano (possono anche etichettarli, imballarli adeguatamente o confezionarli come regali) e li spediscono all'acquirente. Amazon può occuparsi anche della pubblicità e della diffusione delle offerte sul proprio sito Internet. Inoltre, Amazon offre il servizio clienti per le richieste di informazioni e i resi e gestisce i rimborsi dei prodotti difettosi. Sempre Amazon riceve dal

delle imprese del gruppo Amazon nella commercializzazione dei prodotti e l'assunzione di buona parte dei compiti del venditore»[16].

In quest'ottica, sarebbe dunque necessario concludere che nel processo di vendita le società Amazon Services e Amazon FC, che partecipano entrambe a un modello integrato di negozio, pongono in essere un comportamento di tipo attivo, che secondo l'AG è per l'appunto ciò che la norma di cui all'art. 9 del regolamento (UE) 2017/1001 esemplifica laddove elenca atti quali «l'offerta», «l'immissione in commercio» e «lo stoccaggio dei prodotti a tali fini». Corollario di siffatto comportamento attivo sarebbe, sempre secondo l'AG, l'apparente controllo assoluto del processo di vendita.

Alla luce di questa ricostruzione, l'AG osserva che qualora nel caso in esame fosse confermato a livello fattuale che le imprese del gruppo Amazon hanno in realtà prestato tali servizi "attivi" nell'ambito del programma "Logistica di Amazon", si potrebbe ritenere che nell'immissione in commercio dei prodotti esse svolgono funzioni che vanno oltre la mera creazione delle condizioni tecniche per l'uso del segno. In questa prospettiva, dinanzi alla vendita o offerta in vendita di un prodotto contraffattorio, «il titolare dei diritti di marchio potrebbe legittimamente reagire vietando a siffatte imprese l'uso del segno».[17]

Seguendo questa impostazione fattuale il ruolo dell'intermediario non potrebbe essere ritenuto neutro e le deroghe alla responsabilità dei prestatori di servizi della società dell'informazione di cui all'art. 14, par. 1, della direttiva 2000/31/CE non dovrebbero applicarsi alla presente controversia. Tali deroghe, osserva ancora l'AG, «si limitano al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi» e quindi non dovrebbero trovare applicazione in relazione ad «un'attività come quella di stoccaggio fisico e consegna materiale dei prodotti».[18]

4. La responsabilità degli intermediari

Tanto la decisione della Corte in commento quanto (ed ancor più) le conclusioni dell'AG offrono l'occasione per alcune considerazioni in tema di responsabilità degli intermediari, sia "fisici" che "della rete", in caso di violazione di diritti di proprietà intellettuale.

La fattispecie, infatti, per la particolare configurazione dei servizi offerti dalle società del gruppo Amazon, si presta all'approfondimento - alla luce della precedente giurisprudenza europea - di un parallelismo effettivamente intercorrente tra la disciplina prevista per la responsabilità degli intermediari "offline", fornitori di una soluzione tecnica come un servizio di trasporto o di deposito in magazzino, e quella dettata in riferimento agli Internet service provider, ovverosia i prestatori di servizi della società dell'informazione (per usare la definizione di cui al d.lgs. 70/2003).

cliente il pagamento delle merci, trasferendolo poi al venditore sul suo conto bancario».

[16] § 57 delle Conclusioni dell'Avvocato Generale.

[17] § 58 delle Conclusioni dell'Avvocato Generale.

[18] § 62 delle Conclusioni dell'Avvocato Generale.

I concetti fondamentali da cui un tale tipo di analisi dovrebbe prendere spunto sono quelli - sommariamente affrontati dalla Corte e dall'AG nella causa in esame - della "conoscenza" dell'illecito da parte dell'intermediario e del "controllo" da questi esercitato (in questo caso) sui prodotti illegittimamente commercializzati con l'ausilio della propria attività di intermediazione.

Per quanto riguarda la posizione degli Internet service provider, uno dei primi casi in cui la Corte si è trovata ad esaminare la posizione di un *marketplace* online nell'ambito di una violazione di marchio, nonché a chiarire i menzionati concetti di "conoscenza" e "controllo", è la causa (già citata in precedenza e richiamata pure dalla stessa Corte nella decisione in commento) *L'Oréal c. eBay*. In tal caso, la Corte, nell'interpretazione dell'art. 14 della direttiva 2000/31/CE, ha ricordato come l'esonero di responsabilità previsto da detta norma sia applicabile all'intermediario della rete solo «a condizione di non essere stato "effettivamente al corrente del fatto che l'attività o l'informazione è illecita"», ovvero che non abbia svolto «un ruolo attivo atto a conferirgli una conoscenza o un controllo» dei dati memorizzati dai propri utenti, non occupando una posizione "neutra" rispetto a tali informazioni.[19]

Con la stessa sentenza la Corte ha poi chiarito che «l'art. 11, terza frase, della direttiva 2004/48 deve essere interpretato nel senso che esso impone agli Stati membri di far sì che gli organi giurisdizionali nazionali competenti in materia di tutela dei diritti di proprietà intellettuale possano ingiungere al gestore di un mercato online di adottare provvedimenti che contribuiscano, non solo a far cessare le violazioni di tali diritti ad opera degli utenti di detto mercato, ma anche a prevenire nuove violazioni della stessa natura. Tali ingiunzioni devono essere efficaci, proporzionate, dissuasive e non devono creare ostacoli al commercio legittimo».[20]

Tali principi, ed in particolare quelli espressi in tema di provvedimenti di ingiunzione applicabili dai Giudici nazionali agli Internet service provider, sono stati poi dichiarati "validi" e applicati dalla stessa Corte nella successiva decisione *Tommy Hilfiger c. Delta*[21] anche a prestatori di servizi di intermediazione "offline", quali (nel caso ivi sottoposto al giudizio della Corte) quelli di fornitura di uno spazio in locazione in un centro commerciale, all'interno del quale vengano vendute prodotti contraffattori. Questa decisione, che per la prima volta ha approfondito la tematica della c.d. *landlord liability*[22] in

[19] CGUE, C-324/09, *L'Oréal c. e-Bay* (2011), §§ 113 e 119. La Corte, che aveva già affrontato questi temi, invero, nella precedente decisione CGUE, cause riunite C-236/08, C-237/08 e 238/09, *Google France e Google c. Louis Vuitton e altri* (2010), ha poi confermato più volte i principi ivi espressi; si vedano, tra le altre: CGUE, C-521/17, *Coöperatieve V.S.U. c. D.M.* (2018) e C-484/14, *McFadden c. Sony Music* (2016).

[20] CGUE, C-324/09, cit., § 144.

[21] CGUE, C-494/15, *Tommy Hilfiger c. Delta* (2016).

[22] Con il termine anglosassone *landlord liability* si intende appunto la responsabilità indiretta del locatore per gli atti di contraffazione di diritti di proprietà intellettuale commessi dai locatari all'interno negli stabili ceduti in locazione. In particolare, il giudizio alla base del rinvio pregiudiziale alla Corte nella causa *Tommy Hilfiger c. Delta* ha sollevato la questione se un Giudice nazionale possa ordinare la risoluzione del contratto di locazione tra il locatore e il locatario-contraffattore, oppure se la normativa vigente fornisca ulteriori strumenti, meno invasivi, per ottenere il medesimo risultato. Sotto questo profilo, si può osservare che da un lato, essendo la contraffazione qualificata come reato, la risoluzione del contratto potrebbe apparire senz'altro giustificata, ma dall'altro nei casi in cui l'attività contraffattoria sia quantitativamente limitata uno strumento così invasivo come la risoluzione del contratto potrebbe apparire sproporzionato rispetto all'offesa, sia per il locatore-intermediario, che per il locatario-

Europa, ha infatti chiarito che «La circostanza che la messa a disposizione di punti vendita riguardi uno spazio di mercato online o uno spazio di mercato fisico come un'area di mercato è priva di rilievo al riguardo [*i.e.*: al fine di stabilire se il Giudice nazionale possa adottare provvedimenti ingiuntivi nel senso precisato con la sentenza *L'Oréal*; *n.d.r.*]. Infatti, dalla direttiva 2004/48 non risulta che il suo ambito di applicazione sia ristretto al commercio elettronico»[23].

Alla luce di quanto appena ricordato, si potrebbe osservare che con la sentenza in commento la Corte "chiuda il cerchio" per quanto riguarda, appunto, l'anticipato parallelismo tra la responsabilità degli intermediari "online" e "offline".

Se è vero, infatti, che nel valutare la posizione di Amazon i Giudici europei si sono sostanzialmente rifiutati di esprimersi sulla configurabilità di una responsabilità della medesima piattaforma in quanto fornitore di servizi della società dell'informazione - ed in particolare sull'applicabilità o meno, alla stessa Amazon, dell'esimente di cui all'art. 14 della direttiva 2000/31/CE[24] -, non può sfuggire come proprio i concetti di "conoscenza" e "controllo" - che, come emerge chiaramente dalla sentenza *L'Oréal* (ed invero anche dalle precedenti decisioni *Google France e Google*[25], anch'esse richiamate dalla Corte nella decisione in commento), costituiscono il principale nodo da sciogliere per ogni Giudice nazionale che si trovi ad affrontare problematiche di questa tipologia - assumano un ruolo di primo piano anche nella valutazione della responsabilità delle società di Amazon quali mere fornitrici del servizio di deposito/stoccaggio di merci.

Come abbiamo visto, la Corte nella decisione in esame ricorda innanzitutto come il verbo "usare" implichi un atteggiamento attivo da parte di chi commette l'atto, con esercizio di un «controllo, diretto o indiretto», sullo stesso, e come solo chi eserciti un tale controllo sia in grado di cessare l'uso e, quindi, conformarsi ad un divieto in tal senso.[26]

Inoltre, pur non argomentando sul punto (come pure si è accennato), la Corte ha

contraffattore. In questa prospettiva, un'alternativa potrebbe essere che il Giudice disponga una inibitoria positiva (sostanzialmente un "obbligo di fare") al locatore-intermediario, ossia un obbligo di mettere in atto tutto ciò che è necessario per prevenire la violazione, supportato da penale, lasciando così all'intermediario la possibilità di scegliere tra possibili rimedi per porre fine alla violazione.

[23] CGUE, C-494/15, cit., massime § 1.

[24] Pur riconoscendo astrattamente l'applicabilità al caso di specie della normativa di cui alla Direttiva "E-Commerce", infatti, la Corte ha ritenuto di non potersi pronunciare sulla questione relativa a «se l'attività del gestore di uno spazio di mercato on-line in circostanze come quelle di cui al procedimento principale rientri nell'ambito di applicazione dell'articolo 14 paragrafo 1, della direttiva 2000/31 e, se non vi rientrasse, se un tale gestore debba essere considerato un "autore della violazione" ai sensi dell'articolo 11, prima frase, della direttiva 2004/48» (§ 50), non essendo stata sollevata della decisione di rinvio del giudice nazionale. Su questo punto l'opinione dell'AG è concorde nel ritenere che non sussistano le condizioni per ritenere irricevibile la questione pregiudiziale proposta dalla Suprema Corte tedesca, come richiesto, in extrema ratio, da Coty sulla base del fatto che la pronuncia di rimessione alla Corte avrebbe riportato in maniera erronea i fatti di causa. «Tuttavia [sempre secondo l'AG; n.d.r.], è vero pure che, sebbene spetti al giudice nazionale valutare i fatti, la Corte deve sforzarsi di dargli risposte utili. Nulla osta a che la Corte fornisca al giudice nazionale indicazioni, basate sugli atti e sulle osservazioni presentate, in merito a questioni non trattate nella domanda di pronuncia pregiudiziale, qualora lo ritenga necessario per una migliore collaborazione con il giudice del rinvio». Cosa che, tuttavia, (come detto) la Corte non ha ritenuto di fare.

[25] CGUE, cause riunite C-236/08, C-237/08 e C-238/08, cit.

[26] Cfr. §§ 37-38 della sentenza.

ampiamente valorizzato anche l'ulteriore elemento della "conoscenza" dell'illecito, risolvendo la questione pregiudiziale nel senso di escludere la responsabilità di Amazon solamente nell'ipotesi in cui la stessa non sia ritenuta essere stata al corrente del fatto che la merce tenuta in deposito per conto dei terzi venditori fosse contraffatta.
Non passa inosservato come la terminologia utilizzata ricalchi quella di cui alla direttiva 2000/31/CE, che in particolare per quanto riguarda l'*hosting provider*, al suo art. 14 esclude l'operatività dell'esenzione da responsabilità ivi prevista proprio nel caso in cui, tra l'altro, l'intermediario «sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita» o «il destinatario del servizio agisc[a] sotto l'autorità o il controllo del prestatore». Non è dunque un caso, forse, che la Corte si sia espressa in questi termini nonostante abbia ritenuto di non potersi pronunciare in merito alla configurabilità di una responsabilità di Amazon in qualità di «gestore di uno spazio di mercato on-line»[27]. Ci si potrebbe chiedere, dunque, se anche la Corte abbia in realtà condiviso, in fondo, quanto invece è stato chiaramente esplicitato dall'AG, e cioè che non sia possibile distinguere, in un caso come quello di specie, tra la funzione di «depositari» e quella di «gestori del mercato elettronico»[28]: «Il ruolo rilevante delle imprese del gruppo Amazon nel processo di commercializzazione non può essere sminuito considerando separatamente la singola attività di ciascuna di esse»[29]. Ed è, dunque, l'AG che si "azzarda" a risolvere davvero la questione (mal) sollevata dal Giudice del rinvio, legittimando esplicitamente il parallelismo tra intermediari "online" e "offline", ed affermando (come abbiamo già evidenziato in precedenza) che poiché, «nel caso di specie, il ruolo dell'intermediario non è neutro, le deroghe alla responsabilità dei prestatori di servizi della società dell'informazione di cui all'articolo 14, paragrafo 1, della direttiva 2000/31 non si applicano nella presente controversia. Tali deroghe si limitano al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi. Non sono quindi applicabili a un'attività come quella di stoccaggio fisico e consegna materiale dei prodotti»[30].
Allo stesso modo, l'AG ritiene che la "mancata conoscenza", da parte delle imprese Amazon, del fatto che le merci depositate fossero contraffatte non le esima necessariamente da responsabilità: «Il fatto che tali imprese siano fortemente coinvolte nella commercializzazione dei prodotti attraverso il suddetto programma ["Amazon Logistics"; *n.d.r.*] implica che si possa richiedere loro una cura (diligenza) particolare quanto al controllo della liceità dei beni che immettono in commercio. Proprio perché sono consapevoli che, senza un tale controllo, potrebbero facilmente servire da tramite per la vendita di "prodotti illeciti, contraffatti, piratati, rubati o comunque illeciti o contrari all'etica, che ledono i diritti di proprietà di terzi", esse non possono sottrarsi alla propria responsabilità semplicemente attribuendola in via esclusiva al venditore»[31].
Alla luce del quadro appena delineato, il passo successivo dovrebbe consistere nel

[27] Ivi, § 50.

[28] § 58 Conclusioni dell'Avvocato Generale.

[29] Ivi, § 59.

[30] Ivi, § 62.

[31] Ivi, § 82.

domandarsi quali potrebbero essere le conseguenze, per un (parafrasando le parole dell'AG) "prestatore di servizi della società dell'informazione che svolge attività di stoccaggio e consegna di merci contraffatte". Così che il parallelismo si può allora estendere al dovere di diligenza ed all'onere di attivazione imposto dalla normativa europea sull'intermediario - si vedano in proposito i considerando 46 e 48 della direttiva 2000/31/CE - ed all'assoggettabilità a provvedimenti di inibitoria, anche *pro futuro* (c.d. "*stay down*"), in ossequio a quanto previsto dall'art. 11 della direttiva 2004/48/CE, nell'interpretazione datane dalle sentenze *L'Oréal* e *Tommy Hilfiger*. Sarà legittimo, dunque, tanto aspettarsi che l'intermediario in questione agisca per mettere fine alle violazioni di cui sia venuto a conoscenza prima ancora che ciò gli sia imposto da un'autorità, quanto un provvedimento che, ad esempio, imponga allo stesso prestatore di cessare la fornitura dei propri servizi, anche in futuro, a favore del terzo venditore di merce contraffatta (si ricorda, in proposito, come proprio la decisione nella causa C-494/15, *Tommy Hilfiger c. Delta*, abbia sostanzialmente ritenuto legittimo un provvedimento che preveda l'obbligo «di astenersi dalla conclusione o proroga di contratti di locazione di punti vendita in tale area di mercato con persone il cui comportamento è stato giudicato con decisione definitiva dalle autorità giudiziarie o amministrative come lesivo o potenzialmente lesivo dei diritti conferiti dai marchi menzionati nella domanda»).

5. Considerazioni finali

Le considerazioni appena svolte, nell'ipotizzare che la Corte di giustizia abbia inteso recepire, in qualche modo, attraverso l'utilizzo del linguaggio proprio della disciplina dettata per gli Internet service provider, i suggerimenti dell'AG al fine di dare al Giudice del rinvio «risposte utili», «per una migliore collaborazione» (per utilizzare proprio le parole dell'AG: § 25 delle conclusioni), sono certamente suggestive e, in un certo senso, possono suggerire una evoluzione nella giurisprudenza della stessa Corte, che lascia intravedere all'orizzonte una maggiore responsabilizzazione dei prestatori di servizi della società dell'informazione.

Tuttavia, il peso del rifiuto, da parte dei Giudici europei, di esaminare con la lente della normativa di cui alla direttiva 2000/31/CE una fattispecie di fatto che pure, in un modo o in un altro, è pervenuta alla loro attenzione (ed a quella dell'AG), si fa sentire e, nonostante la sensazione di incompletezza che lascia, non può certamente essere sottovalutato.

La verità è che in punto di responsabilità dei gestori di *marketplace* online la Corte non si è espressa. Punto. Si è espresso, in termini estremamente chiari (ed in linea, vale giusto la pena di ricordarlo, con alcune pronunce nazionali[32]), l'AG; la cui opinione, però, come ben sappiamo, non "fa giurisprudenza".

Sarà dunque interessante capire, a questo punto, come il Bundesgerichtshof recepirà la sentenza in commento. Il risultato del giudizio *a quo*, infatti, non dovrebbe essere così

[32] Si veda ad esempio Cass. civ., sez. I, 19 marzo 2019, n. 7708, *RTI c. Yahoo!*; Trib. Roma, 2 ottobre 2019, *RTI c. Bit Kitchen*; Trib. Roma, 15 febbraio 2019, n. 3512, *RTI c. Facebook*; App. Roma, 29 aprile 2017, *RTI c. Break Media*. In relazione ai servizi forniti da Amazon si veda in articolare AGCM, 9 marzo 2016, Provvedimento n. 2591.

"scontato" come potrebbe sembrare ad una lettura superficiale della sentenza (e delle conclusioni dell'AG) emessa nell'ambito della causa in commento. Vero è che, nell'esaminare la decisione di rimessione della questione pregiudiziale alla Corte di giustizia, non sembra esservi spazio per una rivalutazione, in diritto, della fattispecie (la Corte federale tedesca è infatti chiara nell'affermare che «il successo del ricorso dipende dall'interpretazione dell'articolo 9, paragrafo 2, lettera b), RMC e dell'articolo 9, paragrafo 3, lettera b), RMC»). Ma è altrettanto vero che le circostanze di fatto, riguardanti le caratteristiche dei servizi offerti dalle società di Amazon, sono ivi ben delineate in tutti i loro aspetti. Sarà il Giudice tedesco, in altre parole, a darci un indizio utile a sciogliere il dubbio se i "suggerimenti" che sembrano farsi sentire siano solamente l'eco delle urla dell'AG oppure il suono del bisbiglio della Corte di giustizia dell'Unione europea.

Utilizzo dei *cookie* e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di giustizia nel caso *Planet49*

Riccardo Cabazzi

Corte di giustizia dell'Unione europea, 1 ottobre 2019, C-673/17, *Planet49*

Il consenso che l'utente di un sito Internet deve prestare ai fini dell'installazione di *cookie* sul suo dispositivo non può ritenersi validamente espresso nell'ipotesi in cui compaia una casella di spunta preselezionata. Questi dovrebbe infatti deselezionare tale casella al fine di negare il proprio assenso all'archiviazione o all'accesso di informazioni presenti nel suo terminale. La Corte di giustizia interpreta invero il diritto dell'Unione nel senso, da una parte, di una maggiore responsabilizzazione dei soggetti attivi del trattamento e, dall'altra, mirando all'innalzamento del livello di consapevolezza dell'utenza sull'uso dei propri dati. Non rileva, al riguardo, il fatto che le predette informazioni costituiscano o meno dati personali. Obiettivo della normativa europea (direttiva 95/46/CE, regolamento (UE) 679/2016, direttiva 2002/58/CE) è infatti quello di tutelare l'utente da qualsiasi ingerenza nella sua vita privata ed, in particolare, dal rischio di inconsapevoli introduzioni nell'apparecchiatura terminale. Pertanto, il fatto che un utente di una pagina web attivi il pulsante di partecipazione ad un gioco a premi non è sufficiente per ritenere che questi abbia validamente espresso il proprio consenso all'installazione di *cookie*.

Sommario

1. Fatto e vicenda processuale. – 2. Premessa sulla normativa applicabile. – 3. Sulla validità del consenso dell'utente nell'ipotesi di casella preselezionata. – 4. Le altre questioni sollevate: *cookie*, dati personali e leale trattamento dei dati dell'utente. Cenni conclusivi .

Keywords

consenso - *opt-out* - dati personali - *cookie* - rinvio pregiudiziale

1. Fatto e vicenda processuale

Le questioni pregiudiziali sottoposte all'esame della Corte di giustizia traggono origine da una controversia tra due Federazioni di consumatori tedesche (*Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband*) e la

Planet49 GmbH, una società che propone giochi on-line. Le prime si dolevano quindi del fatto che gli utenti di Internet che intendevano partecipare ad un gioco organizzato dalla predetta società si ritrovavano indirizzati ad una pagina web ove comparivano due didascalie accompagnate da caselle di spunta, da selezionare o deselezionare per usufruire di tale servizio. Più nel dettaglio, la prima casella, non preselezionata, richiedeva loro di acconsentire ad essere contattati da una serie di aziende per ricevere offerte promozionali di natura commerciale. La seconda casella, invece, già preselezionata, richiedeva agli utenti di acconsentire all'installazione di *cookie*, anche per finalità commerciali e di profilazione. Le federazioni contestavano quindi l'aderenza delle suddette dichiarazioni di consenso ai requisiti previsti dalla normativa tedesca e chiedevano pertanto al Tribunale del Land, Francoforte sul Meno (*Landgericht Frankfurt am Main*) di far cessare – con apposito provvedimento di inibitoria – le richieste della società organizzatrice del gioco, oltre alla condanna al risarcimento del danno. Il ricorso veniva quindi parzialmente accolto in primo grado. Tuttavia, la società Planet49 appellava tale decisione dinanzi al Tribunale superiore del Land (*Oberlandesgericht Frankfurt am Main*) il quale riteneva infondate le domande delle federazioni in quanto, da un lato, sarebbe comunque stato possibile all'utente deselezionare la seconda casella e, dall'altro, quest'ultima sarebbe risultata sufficientemente chiara – da un punto di vista tipografico – e completa nel fornire informazioni sulle modalità di utilizzo dei *cookie*. Da ultimo, quindi, con riguardo alla vicenda processuale, la Corte federale di giustizia (*Bundesgerichtshof*), adita con ricorso per cassazione (*revision*) dalle federazioni, si interrogava sulla validità dell'ottenimento del consenso prestato dagli utenti del sito Internet mediante una casella di spunta preselezionata rispetto alla normativa europea (su questa vedi infra). Sospendeva pertanto il procedimento interrogando sul punto, mediante rinvio pregiudiziale *ex* art. 267 TFUE, la Corte di giustizia.

2. Premessa sulla normativa applicabile

Prima di analizzare le principali questioni giuridiche affrontate dal giudice europeo è quindi opportuno soffermarsi brevemente sul quadro normativo di riferimento. Per rispondere alle questioni sollevate dal giudice del rinvio, la Corte ha ritenuto applicabili sia le norme della direttiva 95/46/CE – relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – che quelle del successivo regolamento (UE) 2016/679, più noto come *General Data Protection Regulation* (di seguito GDPR[1]). Si noti invero, al riguardo, che il GDPR, il quale ha abrogato la direttiva 95/46/CE, è entrato in vigore il 25 maggio 2018 e, quindi, successivamente sia alla data dell'ultima udienza tenutasi davanti al giudice del rinvio che a

[1] Si noti che, in Italia, al pari di quanto avvenuto in altri Stati europei, al fine adeguare la normativa nazionale al regolamento, il legislatore è intervenuto. In data 4 settembre 2018 è stato infatti pubblicato in Gazzetta Ufficiale il d.lgs. 10 agosto 2018, n. 101, recante "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". Tale decreto è entrato in vigore il 19 settembre 2018. Sul tema, si rimanda quindi a: G. Finocchiaro, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d. lgs. 10 agosto 2018, n. 101*, Bologna 2019.

quella in cui la questione pregiudiziale è stata sollevata. Tuttavia, la Corte ha osservato, in linea con quanto rilevato in udienza dal governo tedesco, che il GDPR potrebbe risultare applicabile *ratione temporis* anche nell'ambito del procedimento principale, in quanto l'azione fatta valere dalle Federazioni intende non solo censurare la condotta di Plant49 rispetto a fatti pregressi, bensì anche farla cessare pro futuro. Il giudice di Lussemburgo ha pertanto ritenuto di dover prendere in considerazione entrambe le fonti normative citate.

3. Sulla validità del consenso dell'utente nell'ipotesi di casella preselezionata

Ciò premesso, la prima questione sollevata dalla Corte federale di giustizia riguarda la validità del consenso espresso dall'utente in situazioni analoghe a quelle del caso da cui è scaturito il contenzioso tra le Federazioni e la società Planet49. Trattasi invero della particolare ipotesi in cui l'archiviazione di informazioni o l'accesso a informazioni già archiviate, mediante *cookie*, nell'apparecchiatura terminale di un utente di un sito Internet, siano autorizzati mediante una casella preselezionata, che l'utente deve deselezionare per negare il proprio consenso. Il dibattito delle parti si è quindi incentrato sugli effetti che la selezione o de-selezione di una casella, contenente una spunta già preselezionata, può produrre in capo al fruitore del servizio Internet. Si tratta di un dibattito che ruota intorno all'attività o passività della manifestazione del consenso dell'utente al trattamento dei dati personali[2]. Invero, i requisiti da soddisfare affinché questo fosse ritenuto valido erano stati, per diverso tempo, circondati da un alone di incertezza[3]. Proprio per questo, il GDPR si è prefissato, quale obiettivo cardine, quello di garantire "un elevato livello di protezione dei dati personali"[4], ponendo un freno alla frammen-

[2] Cfr. S. El Sabi, *La Corte di Giustizia vieta le caselle di spunta preselezionate per il consenso all'uso dei cookie*, in *giustiziacivile.com,* 2, 2020, 5. Sul tema delle diverse tipologie di consenso necessarie al fine del trattamento dei dati personali dell'utente si rimanda altresì a: F. Caggia, *Il consenso al trattamento dei dati personali nel diritto europeo,* in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, 3, 2019, 405 ss. e a S. Thobani, *La libertà di consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e Diritto Privato*, 2, 2016, 513 ss. Secondo tale Autrice, in particolare: «talune modalità tecnologiche usate per richiedere il consenso, anche se non aggressive o pressanti, rischiano in ogni caso di impedire una scelta consapevole e prestata su un piano di parità rispetto al fornitore dei servizi». Da ultimo vedasi, al riguardo, lo storico contributo di S. Rodotà, *Protezione dei dati e circolazione delle informazioni*, in *Rivista critica del diritto privato*, 1984, 721 ss.

[3] In questo senso argomenta L. Tosoni, *Cookie: l'impatto della sentenza della Corte UE che bandisce le caselle di spunta preselezionate*, in agendadigitale.eu, 3 ottobre 2019.

[4] Dispone invero il considerando 6 del regolamento che: «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali».

tazione normativa[5] in materia prodotta dalla diversa attuazione, nei vari Stati membri, della precedente direttiva 95/46/CE[6]. Per raggiungere tale scopo, il regolamento (UE) 2016/679 ha quindi perseguito due direttrici fondamentali: la prima, volta ad una maggiore responsabilizzazione dei soggetti attivi del trattamento; la seconda, consistente nel fornire agli interessati degli strumenti atti ad innalzare il livello di consapevolezza sull'uso dei propri dati. Ne è quindi disceso – come osservato da attenta dottrina[7] – che entrambe le linee d'azione, se complessivamente considerate, hanno avuto, quale effetto, quello di innalzare il livello di controllo sui dati, come già auspicato dal Garante europeo della protezione dei dati[8]. Coerentemente con quanto sin d'ora affermato, il GDPR prevede quindi, all'art. 4, n. 11, che «il consenso dell'interessato sia qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'utente con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento». Pertanto, alla luce di tale normativa, ai fini della validità del consenso richiesto all'interessato, è senz'altro necessario che questo si sostanzi in un comportamento attivo, manifestato con piena cognizione di causa da parte dell'utente[9]. Corollario di quanto

[5] Proprio alla luce di tale frammentarietà la Corte di giustizia ha affermato, con sentenza del 19 ottobre 2016, causa C-582/14, §§ 56-57 che: «ai sensi dell'articolo 7, lettera f), della Direttiva sulla tutela dei dati personali, il trattamento di dati personali è legittimo se "è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1" di tale direttiva. È importante ricordare che la Corte ha dichiarato che l'articolo 7 della suddetta direttiva prevede un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati personali può essere considerato lecito, e che gli Stati membri non possono né aggiungere nuovi principi relativi alla legittimazione del trattamento dei dati personali del suddetto articolo né prevedere requisiti supplementari che vengano a modificare la portata di uno dei sei principi previsti da detto articolo».

[6] Dispone invero il considerando 9 del regolamento che: «sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE».

[7] Cfr. A. M. Gambino - C. Bomprezzi, *Blockchain e protezione dei dati personali*, in il *Diritto dell'informazione e dell'informatica*, 3, 2019, 619 ss.

[8] Si v. European Data Protection Supervisor (EDPS), Opinion 7/2015, *Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability*, in *edps.europa.eu*, secondo cui (p. 2) «*in order to answer the challenges of big data we need to allow innovation and protect fundamental rights at the same time. It is now up to companies and other organisations that invest a lot of effort into finding innovative ways to make use of personal data to use the same innovative mind-set when implementing data protection law*».

[9] In particolare, il considerando 32 del regolamento afferma che: «Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi

affermato è che non può configurare consenso il silenzio, l'inattività dell'utente o, ancora, la preselezione di caselle. Tale interpretazione è altresì avvalorata anche dal tenore letterale di altre disposizioni ritenute dalla Corte applicabili. In *primis*, la Corte osserva che il concetto di consenso contenuto nella direttiva 2002/58/CE – relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche – deve essere equiparato a quello definito dall'art. 2, lett. *h)* della direttiva 95/46/CE, in quanto espressamente richiamata[10]. Questa disposizione normativa definisce quindi il consenso della persona interessata come «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati che la riguardano siano oggetto di un trattamento». Il giudice di Lussemburgo interpreta quindi tale dato normativo facendo proprie le osservazioni formulate dall'Avvocato Generale nelle sue conclusioni. In particolare, secondo quest'ultimo: «l'articolo 2, lettera h), della direttiva 95/46 fa riferimento a una manifestazione della volontà della persona interessata, con cui evidentemente si indica un comportamento attivo, piuttosto che uno passivo»[11]. La Corte afferma quindi, sulla scorta di tale esegesi normativa, che il consenso espresso mediante una casella di spunta preselezionata non implica un comportamento attivo da parte dell'utente di un sito Internet. Invero, risulterebbe praticamente impossibile determinare in modo oggettivo se, non deselezionando una casella preselezionata, egli abbia effettivamente manifestato il proprio consenso al trattamento dei suoi dati personali, nonché, in ogni caso, se tale manifestazione di volontà sia o meno informata. Non si potrebbe invero escludere aprioristicamente che l'utente non abbia letto l'informazione che accompagna la casella preselezionata o che questi non abbia comunque visto tale casella, prima di continuare la propria navigazione. Pertanto, alla luce delle norme europee richiamate e della loro interpretazione, la Corte risponde all'interrogativo sollevato dal giudice del rinvio tedesco ritenendo che il consenso non può ritenersi validamente espresso nell'ipotesi di cui al procedimento principale. Ovvero quando l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet attraverso *cookie* sono autorizzati mediante una casella di spunta preselezionata (c.d. *opt-out*) che l'utente deve deselezionare al fine di negare il proprio consenso.

chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

[10] In particolare, secondo il considerando 17 della direttiva 2002/58/CE: «ai fini della presente direttiva il consenso dell'utente o dell'abbonato, senza considerare se quest'ultimo sia una persona fisica o giuridica, dovrebbe avere lo stesso significato del consenso della persona interessata come definito ed ulteriormente determinato nella direttiva 95/46/CE. Il consenso può essere fornito secondo qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito internet».

[11] Conclusioni dell'Avvocato Generale Maciej Szpunar, 21 marzo 2019, C-673/17, § 60.

4. Le altre questioni sollevate: *cookie*, dati personali e leale trattamento dei dati dell'utente. Cenni conclusivi

Il giudice del rinvio poneva inoltre alla Corte un ulteriore quesito interpretativo relativo alle norme già richiamate. Questo verte sulla possibilità di interpretarle diversamente a seconda che le informazioni archiviate o consultate nel terminale di un utente di un sito costituiscano o meno dati personali. Sul punto, il Giudice di Lussemburgo osserva che l'art. 5, par. 3, della direttiva 2002/58/CE, nel riferirsi alle suddette informazioni, non ne fornisce una qualificazione, né precisa se queste debbano o meno essere dati personali. Tuttavia, il considerando 24 di tale direttiva sembra chiarire meglio tale questione, in quanto afferma che qualsiasi informazione archiviata nell'apparecchiatura dell'utente fa parte della sua sfera privata e deve essere tutelata ai sensi della CEDU. Il riferimento è, in particolare, all'art. 8 in materia di diritto alla protezione dei dati di carattere personale[12]. Pertanto, sulla scorta di tale ricostruzione, la Corte aderisce alle conclusioni dell'Avvocato Generale, secondo cui l'art. 5, par. 3, della direttiva 2002/58/CE sarebbe volto a proteggere l'utente da qualsiasi interferenza con la sua sfera privata, indipendentemente dal fatto che tale interferenza coinvolga dati personali o di altro tipo[13]. Ne discende dunque che la normativa citata non deve essere interpretata diversamente a seconda che le informazioni archiviate o consultate nell'apparecchiatura terminale dell'utente di un sito Internet costituiscano o meno dati personali.

Da ultimo, la Corte federale di giustizia tedesca poneva al giudice europeo una seconda questione, su cui la pronuncia in commento si sofferma brevemente. Questa riguarda il fatto che l'art. 5, par. 3, della direttiva 2002/58 debba essere interpretato nel senso che tra le informazioni che il fornitore di servizi deve comunicare all'utente rientri il periodo di attività dei *cookie*, nonché la possibilità per i terzi di avere accesso a questi. Tale norma richiama l'art. 10 della direttiva 95/46/CE, in forza della quale vengono elencate una serie di informazioni non esaustive – ciò si deduce dalla presenza del nella norma del termine "almeno" – da fornire all'utente affinché si possa considerare effettuato, da parte del responsabile, un leale trattamento dei dati della persona interessata. Secondo la Corte, quindi, benché la durata del trattamento dei *cookie* non compia tra tali informazioni normativamente previste, questa deve comunque essere oggetto di comunicazione ai fini del leale trattamento dei dati. Invero, in una situazione come quella di cui trattasi nel procedimento principale, un prolungato periodo di attività – peraltro potenzialmente illimitato – implica la raccolta di numerose informazioni sulle abitudini di navigazione, nonché sulla frequenza delle eventuali visite dell'utente ai siti dei partner pubblicitari dell'organizzatore del gioco a premi. La suddetta interpretazione è altresì corroborata – rileva il giudice di Lussemburgo – anche dall'art. 13, par. 2, lett. *a),* del GDPR, secondo il quale il titolare del trattamento deve fornire all'interessato, al fine di garantire un trattamento corretto e trasparente, informazioni relative,

[12] Con riguardo ai principi, alle norme, al contesto e al quadro del diritto europeo in materia di protezione dei dati personali si rinvia al *Manuale sul diritto europeo in materia di protezione dei dati,* edizione 2018, redatto da Agenzia dell'Unione europea per i diritti fondamentali e Consiglio d'Europa, disponibile all'indirizzo web *echr.coe.int*.

[13] Conclusioni dell'Avvocato Generale Maciej Szpunar, 21 marzo 2019, cit., § 107.

in particolare, al periodo di conservazione dei dati personali oppure, se ciò non è possibile, ai criteri utilizzati per determinare tale periodo. Pertanto, alla luce di tale analisi normativa, la Corte afferma che il periodo di attività dei *cookie*, nonché la possibilità o meno per i terzi di avere accesso a questi rientrano tra le informazioni che il fornitore di servizi deve comunicare all'utente di un sito Internet.

In conclusione, sembra quindi potersi affermare che le descritte conclusioni cui è giunto il giudice europeo non costituiscano un approdo giurisprudenziale imprevedibile[14]. La decisione in esame va infatti letta – ad avviso dello scrivente – alla luce soprattutto del tenore normativo del GDPR[15]. Tale regolamento riafferma peraltro, in chiave più rigorosa, principi già contenuti nella Direttiva sulla protezione dei dati e, peraltro, da lungo tempo sostenuti dalle Autorità nazionali[16]. Si pensi, ad esempio, al menzionato art. 4, n. 11, ai sensi del quale il consenso dell'interessato consiste in un'azione positiva inequivocabile. Orbene: in forza di un così chiaro dettato normativo pare difficilmente contestabile il principio enunciato della Corte in merito alla non validità della pratica, piuttosto diffusa, posta in essere dai gestori dei siti Internet, di richiedere il consenso degli utenti all'installazione dei *cookie* mediante caselle di spunta già preselezionate. Un comportamento di questo tipo da parte dell'utente non può infatti certamente essere ricondotto a una manifestazione di consenso attiva ed indiscutibilmente consapevole. Nondimeno, le affermazioni del Giudice di Lussemburgo sembrano comunque potersi apprezzare in quanto atte a sensibilizzare ulteriormente i gestori dei siti che intendono utilizzare i *cookie* sulla necessità di tutelare pienamente la riservatezza degli utenti interessati, onde non incorrere in sanzioni.

---

[14] Argomentano in questo senso: C. Ritzer - N. Filkina - L. White, *No surprises in the recent Planet49 European Court of Justice judgment*, 9 ottobre 2019, disponibile all'indirizzo web *dataprotectionreport.com*.

[15] Si veda, al riguardo, secondo cui: M. Forti, *Le piattaforme online alla prova del Regolamento (UE) 2016/679. Quali tutele per la condivisione dei dati nell'economia collaborativa?*, in *questa Rivista*, 2, 2019, 174: «una tematica di vitale importanza è l'effettività del consenso prestato dall'interessato alla raccolta delle informazioni che lo riguardano; il Regolamento (UE) 2016/679 dovrà impedire la prassi che vedeva le piattaforme processare specifici dati senza che l'interessato ne avesse alcuna contezza».

[16] Da ultimo si veda il caso *dell'Agencia Espanola de Proteccion de Datos*, che con *resolucion* R/00499/2019 del 10 ottobre 2019 ha sanzionato la compagnia aerea Vueling Airlines S.L. con una multa di 30.000 euro per non aver ottenuto dagli utenti del proprio sito un consenso realmente informato sull'uso dei *cookie* e non aver fornito la possibilità di rifiutarli ed accettarli introducendo soluzioni innovative per il *cookie setting* dei siti Internet. In particolare, l'utente lamentava l'impossibilità sia di rifiutare l'utilizzo di *cookie* sia di selezionare attivamente il proprio consenso, ritenuto accordato con la semplice prosecuzione della navigazione sul sito. Al riguardo, il Garante della privacy spagnolo ha quindi effettivamente accertato che la modalità di acquisizione del consenso da parte della Vueling Airlines non fossero conformi a quanto prescritto dall'art. 22.2 della LSSI, la legge spagnola sui servizi della società dell'informazione e del commercio elettronico, e che il trasferimento dei dati a terzi, tramite i *cookie*, avveniva attraverso il consenso implicito dell'utente. In nessun momento veniva infatti offerto a questi la possibilità concreta di opporsi all'installazione di questi *cookie* o di altri *cookie* non strettamente necessari al funzionamento del sito (come quelli finalizzati alla profilazione dell'utente) sul proprio dispositivo. Cfr. C. Agostini, *Il Garante privacy spagnolo ha sanzionato la compagnia aerea Vueling per non aver fornito agli utenti la possibilità di opporsi e di gestire l'utilizzo dei cookie presenti sul proprio sito web*, 21 ottobre 2019, disponibile all'indirizzo web *replegal.it*.

Il bilanciamento tra libertà di espressione degli avvocati e tutela dell'autorità del potere giudiziario: un inquadramento sistematico degli interessi nella prospettiva della Corte europea dei diritti dell'uomo

Federico Ceci

Corte europea dei diritti dell'uomo, 8 ottobre 2019, ric. 24845/13 e 49103/15, *L.P.* e *Carvalho c. Portogallo*

La condanna al risarcimento del danno per diffamazione disposta nei confronti di un avvocato per aver criticato, nell'ambito del mandato difensivo attribuitogli, l'operato di un giudice, costituisce una violazione del diritto alla libertà di espressione garantito dall'art. 10 della Convenzione europea dei diritti dell'uomo. Alla luce del particolare *status* soggettivo attribuito agli avvocati, le sentenze di condanna dei giudici nazionali rappresentano un'ingerenza sproporzionata e non necessaria nell'esercizio della libertà di espressione dei professionisti e non corrispondono ad alcun bisogno sociale imperativo. Inoltre, le sanzioni illegittimamente applicate dalle autorità nazionali rischiano di produrre un effetto deterrente sull'intera professione legale, considerando, in particolare, che le dichiarazioni contestate agli avvocati si inserivano nell'alveo della difesa degli interessi degli assistiti.

Sommario

1. Premessa. – 2. Le vicende all'origine della sentenza. – 3. La limitazione della libertà di espressione e la tutela dell'autorità del potere giudiziario. – 4. La valutazione dello *status* soggettivo dei ricorrenti: tra orientamenti della Corte europea e standard internazionali. – 5. Osservazioni conclusive.

Keywords

libertà di espressione - Art. 10 CEDU - amministrazione della giustizia - tutela dell'autorità del potere giudiziario - diffamazione

1. Premessa

Il perimetro di operatività del diritto alla libertà di espressione degli avvocati nei confronti dell'operato delle corti è stato ulteriormente delineato da un'importante pronun-

cia della Corte europea dei diritti dell'uomo con la quale, come vedremo, non solo è stato valorizzato il ruolo dell'avvocato nella fondamentale realizzazione del diritto di difesa di ogni individuo, ma anche la sua funzione nell'attuazione dell'interesse della collettività nella buona amministrazione della giustizia. La sentenza, resa dalla terza sezione della Corte per i casi *L.P. e Carvalho c. Portogallo* (ricc. 22845/13 e 49103/15) e depositata l'8 ottobre 2019, costituisce, così, da una parte, l'ennesimo passo del percorso con il quale i giudici di Strasburgo hanno proceduto al bilanciamento degli interessi, apparentemente contrapposti, di avvocati e giudici, e, d'altra parte, un significativo apprezzamento del ruolo dei legali nel buon funzionamento del sistema giudiziario, che si inserisce in un dibattito di assoluta attualità, con potenziali sviluppi anche sul piano nazionale, circa l'introduzione di previsioni aggiuntive sulla funzione degli avvocati nella Costituzione[1].

Nonostante i magistrati godano di una posizione particolarmente tutelata - assicurata loro dall'art. 10, par. 2, della Convenzione europea dei diritti dell'uomo[2] (di seguito, Convenzione o CEDU) sia in termini di garanzia dell'autorità e dell'imparzialità del potere giudiziario, sia come protezione della reputazione -, agli avvocati deve essere accordata la possibilità di criticare l'operato delle corti, soprattutto qualora tale attività risulti funzionale all'espletamento del mandato difensivo. Una diversa impostazione, a parere della Corte, potrebbe condurre i professionisti a rifiutare gli incarichi più scomodi e, conseguentemente, ad una palese violazione del diritto alla difesa, garantito, per ogni grado e stato del giudizio, dall'art. 6 CEDU[3].

---

[1] A tal proposito, si vedano le recenti iniziative per la "costituzionalizzazione" dell'avvocatura. Specificatamente, la proposta di legge costituzionale A.C. 1719, depositata alla Camera il 29 marzo 2019, recante "Introduzione degli articoli 110-bis e 110-ter della Costituzione, in materia di autonomia e di esercizio della professione di avvocato, e modifica all'articolo 135, in materia di composizione della Corte costituzionale", e la proposta di legge costituzionale A.S. 1199, depositata in Senato il 4 aprile 2019, per la "Modifica dell'articolo 111 della Costituzione recante l'introduzione di princìpi inerenti la funzione e il ruolo dell'avvocato". Le proposte legislative, entrambe attualmente assegnate alla I Commissione Affari Costituzionali in sede Referente, sono reperibili, rispettivamente, sui siti *camera.it* e *senato.it*.

[2] L'art. 10 della Convenzione stabilisce che «1. 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. 2. L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario». Per un approfondito commento della citata disposizione si veda, per tutti, M. Oetheimer - A. Cardone, *Articolo 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.

[3] Tale diritto, com'è noto, è ricompreso nella tutela dell'equo processo offerta dall'art. 6, par. 3, lett. *c)*, della Convenzione, il quale, in particolare, prevede che «Ogni accusato ha diritto di difendersi personalmente o avere l'assistenza di un difensore di sua scelta e, se non ha i mezzi per retribuire un difensore, poter essere assistito gratuitamente da un avvocato d'ufficio, quando lo esigono gli interessi della giustizia». A tal proposito, con la sentenza CEDU, *Van Mechelen e altri c. Olanda*, ricc. 21363/93, 21364/93, 21427/93 (1997), è stato precisato che «tenuto conto della posizione di preminenza che il diritto ad una buona amministrazione della giustizia ha in una società democratica, ogni misura

Invero, il citato art. 10 CEDU, se, da una parte, assicura il diritto alla libertà di espressione, senza che lo stesso subisca ingerenze delle autorità pubbliche, d'altra parte, sottopone tale diritto, proprio in virtù dei doveri e delle responsabilità derivanti dall'esercizio dello stesso, a talune restrizioni, tutelando, così, altri valori ritenuti fondamentali. Nello specifico, la libertà di espressione, in quanto elemento funzionale alla garanzia di altri diritti e principi essenziali in una società democratica e pluralista, deve essere limitata qualora l'esercizio abusivo della stessa rischi di compromettere proprio quei diritti[4], con specifico riferimento, per ciò che concerne la presente analisi, alla tutela della reputazione e dell'autorità del potere giudiziario.

Le citate limitazioni alla libertà di espressione[5] hanno carattere eccezionale alla luce dell'importanza del diritto in parola, il quale, come detto, appare strumentale alla realizzazione di altre libertà, che, nel loro insieme, costituiscono elementi essenziali di una società democratica. In particolare, dalla suddetta eccezionalità deriva la necessità di applicare dei criteri ermeneutici restrittivi, in ossequio al principio *exceptiones sunt strictissimae interpretationis*[6], così come ripetutamente sostenuto dalla Corte[7], la quale, invero, ha costantemente offerto una lettura ampia e liberale dell'ambito di applicazione del diritto garantito dall'art. 10[8].

In questa prospettiva, pertanto, vanno inquadrati gli obblighi gravanti sugli Stati, cui spetta garantire l'effettività dell'ambito applicativo riconducibile alla libertà di espres-

---

restrittiva della difesa deve essere assolutamente necessaria». Per una raccolta delle pronunce dei giudici di Strasburgo in relazione all'art. 6 della Convenzione si veda M. De Salvia, *Compendium della Cedu. Le linee guida della giurisprudenza relativa alla Convenzione europea dei diritti dell'uomo*, Napoli, 2000, 188 ss.

[4] Relativamente all'abuso della libertà di espressione di vedano M. Castellaneta, *Il negazionismo tra abuso del diritto e limite alla libertà di espressione in una decisione della Corte europea dei diritti dell'uomo*, in *questa Rivista*, 2019, 311 ss. e F. Falconi, *Alcune considerazioni sull'abuso della libertà di espressione nella giurisprudenza di Strasburgo*, in *Studi sull'integrazione europea*, 2020, 359 ss.

[5] La suddetta impostazione, a ben vedere, è altresì riscontrabile nella struttura dell'art. 19 del Patto sui diritti civili e politici, del 16 dicembre 1966 , il quale, *ex* par. 1, prevede il diritto alla libertà di espressione in capo ad ogni individuo e, contestualmente, al par. 3, dispone delle restrizioni - quali, ad esempio, il rispetto dei diritti e della reputazione altrui -stabilendo che le stesse debbano essere espressamente previste dalla legge, nonché necessarie. Il testo del Patto, in versione italiana, è disponibile in R. Luzzato – F. Pocar, *Codice di diritto internazionale pubblico*, Torino, 2016, 164 ss. Per un confronto del Patto con la Convenzione si veda J. Velu – R. Ergec, *La Convention européenne des droits de l'homme*, Bruxelles, 2014, 735 ss. Impostazione parzialmente differente caratterizza, invece, il combinato disposto degli artt. 19 e 29 della Dichiarazione universale dei diritti dell'uomo, adottata dall'Assemblea generale delle Nazioni Unite, il 9 dicembre 1948. Tale atto se, da una parte, riconosce il diritto alla libertà di opinione ed espressione senza porre limitazione alcuna (art. 19), d'altra parte, prevede delle restrizioni di carattere generale, costituite, per l'appunto, dalla garanzia dei diritti e delle libertà altrui, dalle esigenze della morale, dall'ordine pubblico e dal benessere generale. Per un confronto tra i tre atti citati, si veda U. Villani, *Dalla Dichiarazione universale alla Convenzione europea dei diritti dell'uomo*, Bari, 2015, 17 ss.

[6] Sul punto si veda l'analisi di M. Castellaneta, *La libertà di stampa nel diritto internazionale ed europeo*, Bari, 2012, 6, 15 ss. Sempre con riguardo al principio di interpretazione restrittiva delle limitazioni al diritto in esame P. Caretti, *Art. 10. Libertà di espressione*, in S. Bartole – B. Conforti – G. Raimondi (a cura di), *Commentario alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2001, 341 ss.

[7] Si veda, *ex multis*, la sentenza CEDU, *Handyside c. Regno Unito*, ric. 5493/72 (1976), § 49, con la quale la Corte ha avuto modo di affermare che ogni condizione, limitazione o restrizione alla libertà di espressione deve essere proporzionata allo scopo legittimo perseguito dallo Stato.

[8] Una ricostruzione di tale lettura in M. Oetheimer, *L'harmonisation de la liberté d'expression en Europe*, Parigi, 2001, 60 ss.

sione. Se, per un verso, agli Stati viene imposto, infatti, un dovere di astensione da ogni ingerenza con l'esercizio del diritto in parola, per altro verso, in determinate circostanze risulta opportuno che gli stessi pongano in essere misure positive nei confronti degli individui, affinché questi ultimi possano concretamente godere della tutela loro accordata dalla Convenzione. Nel determinare un ambiente favorevole alla partecipazione pluralista di tutti i cittadini alla vita della società attraverso l'esercizio del diritto alla libertà di espressione, gli Stati devono contemperare l'interesse generale con quello individuale, considerando, in particolare, le peculiarità delle differenti situazioni e degli *status* soggettivi.

A tal proposito, e per ciò che concerne specificatamente la presente analisi, la Corte ha avuto occasione di evidenziare come, nonostante l'ampio riconoscimento offerto dalla Convenzione alla libertà di espressione, alcune categorie individuali possono essere oggetto di restrizioni in termini soggettivi, o, al contrario, di un'estensione della portata della tutela di detta libertà, proprio in virtù del ruolo sociale svolto.

È il caso, rispettivamente, di magistrati ed avvocati. Infatti, se, da un lato, la salvaguardia di una buona amministrazione della giustizia conduce ad ampliare i limiti alla libertà di espressione nei confronti dei giudici, dall'altro lato, la funzione svolta dagli avvocati, intermediari tra società e corti, non può non comportare una più intensa protezione degli stessi, qualora, nell'espletamento diretto o indiretto del mandato difensivo, muovano delle critiche nei confronti dell'operato della magistratura.

2. Le vicende all'origine della sentenza

Preliminarmente all'analisi dei limiti all'esercizio della libertà di espressione e del conseguente complesso bilanciamento tra tutela dell'autorità giudiziaria e libertà di critica dell'operato delle corti da parte degli avvocati, appare opportuno ricostruire, seppure brevemente, le vicende che hanno condotto alla pronuncia in esame. I due casi, trattati congiuntamente per via delle analogie tra i ricorsi, si iscrivono in un percorso giurisprudenziale ventennale con cui la Corte ha rafforzato la tutela offerta agli avvocati, alla luce del particolare ruolo svolto dagli stessi – funzionale tanto al buon andamento dell'amministrazione della giustizia, quanto all'esercizio del diritto di difesa –, e limitato, di conseguenza, il potere d'ingerenza degli Stati[9].

2.1. Il caso *L.P.*

La prima vicenda affrontata dalla Corte ha avuto ad oggetto il ricorso presentato da un avvocato portoghese che aveva promosso un reclamo nei confronti di un giudice davanti al *Conselho Superior da Magistratura*. Alla luce di alcuni comportamenti adottati dal magistrato nel corso di un'udienza preliminare, il professionista aveva lamentato delle

[9] In assenza di una precisa qualificazione del concetto di ingerenze nell'ambito dell'art. 10 della Convenzione, la Corte ha fornito delle esemplificazioni alla luce delle finalità, del momento e delle conseguenze delle stesse. A tal proposito si veda B. Rainey – E. Wicks – C. Ovey, *Jacobs, White, and Ovey: The European Convention on Human Rights*, Oxford, 2017, 485 ss.

irregolarità procedimentali. In particolare, l'avvocato aveva contestato l'eccessivo ritardo per la fissazione dell'udienza, la sommaria analisi della documentazione e delle dichiarazioni delle parti, affermando, inoltre, di aver notato un clima di "grande intimità" tra il giudice ed il difensore di controparte. Il reclamo era stato respinto dal Consiglio Superiore della Magistratura portoghese a seguito delle spiegazioni fornite dal giudice, il quale, negando ogni irregolarità, aveva sostenuto che le accuse formulate dall'avvocato non fossero supportate da alcun riscontro probatorio. Quindi, il magistrato aveva citato l'avvocato per diffamazione, asserendo che la faziosità ingiustamente addebitatagli avesse leso la sua reputazione. L'avvocato, in propria difesa, aveva sottolineato come il reclamo al CSM fosse stato avanzato in una procedura non pubblica e nell'ambito del suo mandato di legale, affermando, inoltre, che il clima di intimità fosse riconducibile a varie circostanze, tra cui il fatto che il suo cliente non fosse stato sentito nell'ufficio del giudice, al contrario di quanto accaduto per l'assistito dell'avvocato avversario.
Il Tribunale di Lisbona aveva dichiarato l'avvocato colpevole di diffamazione aggravata, condannandolo al pagamento di Euro 300,00, a titolo di multa, ed alla corresponsione di Euro 750,00 come risarcimento del danno in favore del magistrato. La pronuncia di condanna aveva evidenziato come le accuse relative al clima di intimità costituissero valutazioni prive di basi fattuali e, in quanto tali, idonee a ledere l'imparzialità del giudice ed il suo onore professionale. La sentenza era stata parzialmente - e *in peius* per l'avvocato - riformata dalla Corte d'appello di Lisbona, che aveva condannato il ricorrente al pagamento del maggiore importo richiesto dal giudice, di Euro 5.000,00, ritenendo le accuse offensive e gravi, e, conseguentemente, oltre l'ambito delle critiche ammissibili, nonostante lo *status* di difensore di parte.
Infine, la Suprema Corte portoghese, adita in considerazione dell'asserita contraddittorietà della sentenza della Corte d'appello di Lisbona con altro precedente giurisprudenziale, aveva respinto il ricorso, sostenendo che il caso invocato dal ricorrente non potesse essere applicato per via delle circostanze fattuali differenti.
La vicenda, così, è stata sottoposta al vaglio della Corte europea che, come si avrà modo di osservare, ha valutato la condanna nei confronti del ricorrente in contrasto con l'art. 10 della Convenzione.

2.2. La vicenda *Carvalho*

Il secondo ricorso esaminato dalla Corte è stato proposto da un avvocato portoghese, condannato al risarcimento del danno nei confronti di un giudice, per aver leso la reputazione di quest'ultimo. Il legale era costituito quale difensore di due persone di origine gitana, giudicate colpevoli dal Tribunale di Felgueiras dei reati di ingiurie, resistenza a pubblico ufficiale e violenza nei confronti delle forze dell'ordine. Nel formulare la citata sentenza, il giudice aveva tuttavia utilizzato espressioni dure e inappropriate nei confronti degli imputati e, più in generale, della loro comunità. Invero, nella pronuncia del Tribunale, i gitani erano stati qualificati quali folla "ululante", "clienti del posto" delle forze dell'ordine, gruppo etnico dalla scarsa igiene e, infine, come bugiardi e dipendenti dai sussidi statali. Il magistrato giudicante, inoltre, aveva ritenuto non veritiere

le versioni presentate dagli accusati, in quanto parti della commedia "della persecuzione e della vittimizzazione dei poveri zingari".
La suddetta pronuncia, proprio in virtù delle motivazioni adottate dal giudice, era stata ampiamente riportata e criticata dalla stampa e dai media. L'avvocato, inoltre, aveva rilasciato un'intervista radiofonica nella quale definiva inappropriate le espressioni utilizzate. Successivamente, allo stesso difensore erano state attribuite alcune dichiarazioni relative alla sentenza della Corte d'appello di Porto - che aveva annullato parzialmente la prima decisione -, con le quali aveva ritenuto che le espressioni utilizzate dal giudice di primo grado fossero razziste e xenofobe.
Alla luce del tenore della citata sentenza, l'avvocato, sempre rappresentando i due individui di origine gitana, aveva presentato, da una parte, una denuncia penale per diffamazione e discriminazione razziale e, d'altra parte, una richiesta di risarcimento del danno in sede civile, ambedue nei confronti del giudice. Entrambe le richieste, tuttavia, erano state respinte poiché, nonostante la sentenza contenesse espressioni eccessive e superflue, le stesse non potevano essere considerate attacchi personali, finalizzati a danneggiare l'onore e la reputazione degli imputati.
Il giudice, a seguito di dette azioni, aveva dunque promosso un'azione di responsabilità civile nei confronti dell'avvocato dinanzi al Tribunale di Felgueiras, sostenendo che l'utilizzo da parte dello stesso di alcuni estratti della sentenza e le richieste in sede civile e penale avanzate nei suoi confronti avessero comportato un danno alla sua reputazione.
Il Tribunale adito aveva accolto la suddetta richiesta di risarcimento, soffermandosi, in particolare, sulle azioni legali promosse dall'avvocato nell'interesse dei clienti. Invero, i ricorsi per diffamazione erano stati ritenuti inadeguati ed incoerenti poiché inquadrati come comportamenti ultronei rispetto alla critica per il linguaggio utilizzato, presupponendo dei giudizi di valore del giudice nei confronti degli imputati gitani. Il Tribunale aveva sostenuto che, nonostante le eccessive formulazioni contenute nella sentenza, non vi fosse alcuna ragione per ritenere che il magistrato avesse voluto esprimere un'opinione personale finalizzata ad offendere l'onore e la reputazione degli imputati. Tale conclusione era stata peraltro avallata, nella prospettiva del Tribunale, proprio dallo *status* dell'avvocato che, in quanto tale, avrebbe dovuto dare una lettura più oggettiva delle circostanze fattuali. Al contrario, accettando il patrocinio di azioni legali illegittime, il professionista aveva causato, con grave negligenza, un danno alla reputazione del giudice.
Il Tribunale aveva condannato l'avvocato al pagamento di Euro 16.000,00, a titolo di risarcimento del danno morale subito dal giudice[10].
La sentenza era stata poi appellata dinanzi alla Corte d'appello di Porto, la quale, pur sottolineando l'importanza delle immunità di cui godono gli avvocati nell'esercizio del loro mandato, ai sensi dell'art. 208 della Costituzione[11], aveva riformato solo parzial-

[10] L'art. 483 del codice civile portoghese, disposizione in virtù della quale è stata decisa la vicenda, disciplina la responsabilità aquiliana e, con una formulazione simile all'art. 2043 c.c., prevede che chiunque, con dolo o colpa, violi illecitamente i diritti altrui, o qualsiasi altra disposizione di legge volta a tutelare gli stessi, è tenuto a risarcire il danneggiato per il pregiudizio derivante da tale atto.

[11] In virtù della citata disposizione costituzionale «la legge concede agli avvocati le immunità necessarie per l'esercizio del loro mandato e ne regola l'esercizio come elemento essenziale nell'amministrazione della giustizia».

mente la decisione di primo grado, riducendo la condanna ad Euro 10.000,00. La Corte aveva ritenuto gravante, in capo all'avvocato, l'obbligo di rifiutare mandati finalizzati a scopi illeciti o comunque non professionali. Con le due azioni contestate, al contrario, il difensore aveva posto in essere condotte non giustificate dalla funzione sociale e pubblica della professione ed esorbitanti rispetto ai parametri, giuridici e deontologici, che egli stesso avrebbe dovuto rispettare nell'ambito della difesa degli interessi degli assistiti.

Infine, dopo una pronuncia di irricevibilità adottata dalla Corte Costituzionale portoghese, la vicenda è stata sottoposta all'analisi dei giudici di Strasburgo, i quali, come anticipato, hanno ritenuto opportuno esaminare congiuntamente i due ricorsi citati.

3. La limitazione della libertà di espressione e la tutela dell'autorità del potere giudiziario

Ricostruite le vicende, passiamo a verificare i criteri individuati dalla Corte europea applicabili per rispettare le norme convenzionali e raggiungere un giusto bilanciamento tra i diritti in gioco, ossia libertà di espressione e garanzia dell'autorità e dell'imparzialità dei giudici. Come anticipato, l'art. 10 della Convenzione non stabilisce un diritto assoluto, bensì contempla ipotesi in cui l'esercizio della libertà di espressione, nelle varie declinazioni possibili, risulti in contrasto con altri diritti, riconosciuti dalla stessa Convenzione quali parimenti strumentali allo sviluppo dell'individuo e della società, prevedendo così delle limitazioni.

In questa prospettiva, risulta semplice comprendere le ragioni dell'intensa tutela accordata all'autorità del potere giudiziario, trattata, soventemente, anche in termini di pregiudizio all'altrui reputazione[12]. Ed, invero, dalla mera definizione dell'estensione del concetto di autorità del potere giudiziario offerta dalla Corte, quest'ultima ha riscontrato la necessità di ampliare il perimetro applicativo della limitazione in parola. In particolare, i giudici di Strasburgo hanno affermato che il potere giudiziario «*comprises the machinery of justice or the judicial branch of government as well as the judges in their official capacity*» e l'autorità dello stesso «*includes, in particular, the notion that the courts are, and are accepted by the public at large as being, the proper forum for the ascertainment of legal rights and obligations and the settlement of dispute*»[13]. Partendo dalla suddetta qualificazione, la Corte ha riscontrato la necessità che la collettività nutra rispetto e fiducia nei confronti della magistratura e della capacità della stessa di adempiere la fondamentale funzione affidatale.

Tale impostazione, riflettendo la comune visione degli Stati membri di garanzia dell'autorità e dell'imparzialità del potere giudiziario, è stata seguita dalla Corte, che ha in-

[12] In questo senso C. Focarelli, *Trattato di diritto internazionale*, Milano, 2015, 1068.

[13] Tale inquadramento è stato compiuto dalla Corte, nel caso CEDU, *Sunday Times n°1 c. Regno Unito*, ric. 6538/74, (1979), § 55,56, *leading case* della materia in esame, nel quale, tra l'altro, i giudici hanno evidenziato la necessità di valutare l'importanza dell'art. 6 che «consacra il principio fondamentale della preminenza del diritto». La citata pronuncia è analizzata in R. Sapienza, *La libertà di espressione nella Convenzione europea dei diritti dell'uomo: il caso Sunday Times*, in *Rivista di Diritto Internazionale*, 1981, 43 ss. Sul punto si veda altresì la sentenza CEDU, *Worm v. Austria*, ric. 22714/93 (1997), § 40.

globato la concezione anglosassone di *contempt of court*[14]. Questa teoria, in sintesi, è finalizzata a prevenire ogni forma di interferenza con l'amministrazione della giustizia, evitando, nello specifico, gli oltraggi alla corte[15]. L'ambito di operatività di detti principi può pertanto arrivare a ricomprendere l'ottemperanza alle statuizioni emesse dai giudici, la reputazione dell'intero sistema giudiziario e la fiducia delle parti nell'istituzione che amministra la giustizia. Quest'ultimo aspetto, a ben vedere, risulta la vera ragione dell'estensione dei limiti alla libertà di espressione prevista dalla Convenzione. Invero, la necessità che la collettività conservi fiducia nella buona amministrazione della giustizia e, conseguentemente, riconosca l'autorità del potere giudiziario e delle decisioni dallo stesso adottate, costituisce un pilastro portante di ogni Stato di diritto, nel quale, per l'appunto, le controversie vengono rimesse ad organi imparziali e indipendenti, le cui pronunce regolano i rapporti tra privati, nonché tra cittadini e Stato.

Sulla scorta di tali premesse, a partire dalla sentenza del caso *Sunday Times*, la Corte è intervenuta in molteplici occasioni per delineare i confini delle critiche permesse, in quanto funzionali al controllo dell'operato dei giudici e allo sviluppo di dibattiti di pubblico interesse, individuando, allo stesso tempo, i criteri per ritenere legittime le ingerenze statali all'esercizio della libertà di espressione. In questa direzione si inquadra l'orientamento seguito dai giudici di Strasburgo sin dalla risalente sentenza nel caso *Barfod c. Danimarca*[16], con cui la Corte ha ritenuto legittima la condanna di un giornalista al pagamento di un'ammenda, per aver sostenuto, senza un sufficiente fondamento probatorio, che i giudici si fossero mostrati di parte durante il giudizio. Invero, in quella vicenda, la critica verso l'operato dei magistrati era stata qualificata quale «*defamatory accusation against the lay judges personally, which was likely to lower them in the public esteem and put forward without any supporting evidence*»[17] e, conseguentemente, lo Stato aveva legittimamente posto in essere delle misure, necessarie in una società democratica, per tutelare la reputazione dei magistrati e l'imparzialità dell'intero sistema giudiziario. Allo stesso modo, ogni qual volta le critiche mosse nei confronti dei giudici sono risultate prive di una base fattuale e non rilevanti ai fini del pubblico dibattito, la Corte non ha riscontrato alcuna violazione dell'art. 10 della Convenzione. Tale conclusione è stata sostenuta in casi in cui le espressioni utilizzate nei confronti dei giudici travalicavano il perimetro della critica, diventando eccessive o, addirittura, offensive. Nella vicenda *Prager e Oberschlick c. Austria*[18], ad esempio, alcuni giornalisti avevano definito un giudice "*arrogant*" e

[14] Sul punto si veda M. Verpeaux, *Freedom of expression*, Strasburgo, 2010, 103 ss. A ben vedere, la volontà del Regno Unito di prevedere espressamente la tutela dell'autorità giudiziaria quale limitazione alla libertà di espressione, proprio in ossequio alla citata dottrina del *contempt of court*, è riscontrabile anche nei lavori preparatori alla Convenzione, disponibili sul sito *echr.coe.int*.

[15] La rilevanza della teoria in parola per gli ordinamenti di *common law* è constatabile, ad esempio, nell'adozione da parte del Regno Unito del *Contempt of Court Act*, del 1981. Tale atto normativo - emanato, tra le altre ragioni, anche come reazione dello Stato alla citata sentenza *Sunday Times, n.1* – prevede una responsabilità in capo a chiunque ponga in essere condotte «*which creates a substantial risk that the course of justice in the proceedings in question will be seriously impeded or prejudiced*». Per un'analisi del concetto di *contempt of court*, ed in particolare dell'illecito qualificato come "*scandalizing the court*" si veda, *ex multis*, C.J. Miller – D. Perry, *Miller on Contempt of Court*, Oxford, 2018.

[16] CEDU, *Barfod c. Danimarca*, ric. 11508/85 (1989).

[17] Ivi, § 35.

[18] CEDU, *Prager e Oberschlick c. Austria,* ric. 15974/90 (1995). In questa pronuncia la Corte ha

"*bullying*" nello svolgimento della sua funzione, sostenendo, inoltre, che avesse trattato gli imputati come fossero già condannati sin dall'inizio del giudizio. La Corte, anche in questo caso[19], ha ritenuto che le restrizioni imposte dalle autorità austriache rispondessero ad un bisogno sociale impellente, ovverosia quello di proteggere il giudice – che, «*as the guarantor of justice, a fundamental value in a law-governed State*», deve poter vantare della fiducia della società – da «*destructive attacks that are essentially unfounded*» anche in considerazione del dovere di imparzialità che impedisce ai membri della magistratura di replicare liberamente alle accuse mosse nei loro confronti.

Alla luce di quanto osservato, l'ampiezza della limitazione posta a protezione dell'autorità e dell'imparzialità del potere giudiziario risulta particolarmente estesa, tanto da apparire, ad una prima analisi, quasi in contrasto con il principio di stretta interpretazione delle restrizioni alla libertà di espressione[20]. A ben vedere, tuttavia, la Corte, a nostro avviso, ha operato un corretto bilanciamento degli interessi, applicando criteri che, allo stato, appaiono sempre più definiti, soprattutto in ragione dello *status* soggettivo degli individui coinvolti e della corrispondenza delle critiche mosse nei confronti dei giudici a fini parimenti tutelati dalla Convenzione[21]. A tal proposito, occorre sottolineare come qualora le osservazioni mosse nei confronti del sistema giudiziario, per quanto aspre, siano mirate a sviluppare un dibattito critico relativamente al funzionamento dello stesso, senza ridursi in attacchi distruttivi, devono ritenersi ricomprese nella tutela offerta dall'art. 10 della Convenzione. In questo senso, infatti, si è espressa la Corte nel caso *Kobenter e Standard Verlags GmbH c. Austria*[22], nel quale era stata ravvisata una violazione dell'art. 10, dovuta alla sanzione inflitta ad un giornalista ed alla società editoriale per aver criticato, seppure duramente, un giudice che aveva utilizzato in una sentenza espressioni offensive nei confronti degli omosessuali. In particolare, stante il dibattito sviluppatosi inerentemente alla questione, non era stato riscontrato alcun bisogno sociale imperativo per porre limitazioni alla libertà di stampa dei ricorrenti. Allo stesso modo, la Corte ha riconosciuto la violazione del diritto alla libertà di espressione nel caso *Katrami c. Grecia*[23] alla luce di una condanna di un giornalista per aver evidenziato errori procedurali commessi da un magistrato durante un processo[24].

altresì ricordato che la stampa rappresenta uno dei principali mezzi di cui dispongono i responsabili politici e l'opinione pubblica per assicurare che i giudici si sottopongano alle loro alte responsabilità conformemente allo scopo della funzione che è loro affidata.

[19] Nel medesimo senso la Corte si è espressa nei casi CEDU, *Perna c. Italia*, ric. 48898/99 (2003), e *Sgarbi c. Italia*, ric. 37115/06 (2008), nei quali i ricorrenti avevano accusato i giudici di parzialità allo scopo di sostenere determinate fazioni politiche.

[20] Di questo avviso M.K. Addo, *Article 10 of the ECHR and the Criticism of Judges*, in M.K. Addo (ed.), *Freedom of Expression and the Criticism of Judges: A Comparative Study of European Legal Standards*, Burlington, 2000, 229 ss.

[21] Per una approfondita analisi del rapporto tra libertà di stampa e tutela del potere giudiziario si veda M. Castellaneta, *La libertà di stampa nel diritto internazionale ed europeo*, cit., 122 ss.

[22] CEDU, *Kobenter e Standard Verlags GmbH c. Austria,* ric. 60899/00 (2006).

[23] CEDU, *Katrami c. Grecia*, ric. 19331/05 (2007).

[24] Nella medesima direzione la sentenza CEDU, *De Haes e Gijsels c. Belgio*, ric. 19983/92 (1997), con la quale la Corte ha sottolineato che «la libertà di espressione vale non solo per informazioni o idee accolte con favore o considerate inoffensive o indifferenti, ma anche per quelle che urtano, scioccano o inquietano lo Stato». Il principio generale per cui il diritto di libertà di espressione sia posto a tutela

Dunque, se, da un lato, può ritenersi necessario offrire una più ampia tutela alla magistratura in casi di attacchi infondati e potenzialmente capaci di minare la fiducia della società nel sistema giudiziario, dall'altro lato, la suddetta tutela non può condurre ad un sostanziale divieto in capo ai singoli di esprimere la propria opinione, sempre attraverso giudizi di valore non offensivi o dichiarazioni con una sufficiente base fattuale, su questioni di interesse pubblico relative al funzionamento del sistema giudiziario. Al contrario, la libertà di critica nei confronti dell'operato delle corti, proprio in considerazione della percezione comune di quest'ultimo come espressione di una valutazione obiettiva che impegna non solo il singolo giudice ma anche l'intero sistema, può, e deve, essere ritenuta un elemento essenziale ai fini del buon funzionamento e della buona amministrazione della giustizia. Tale assunto risulta vieppiù fondato qualora le espressioni critiche, oltre che rientrare in un dibattito di pubblico interesse ed essere sostenute da basi fattuali, vengano mosse da altri membri dell'apparato giudiziario, ovverosia gli avvocati che, tra l'altro, in quanto esperti del sistema giustizia, possono contribuire con le proprie osservazioni ad "accendere i riflettori" su disfunzioni dello stesso, a vantaggio dell'intera collettività.

4. La valutazione dello *status* soggettivo dei ricorrenti: tra orientamenti della Corte europea e standard internazionali

La conclusione raggiunta appare confermata dal fatto che, nella sentenza in commento, la valutazione circa la necessità dell'ingerenza in una società democratica ha avuto ad oggetto, per l'appunto, lo *status* dei ricorrenti e la funzione svolta dagli stessi[25]. In particolare, la Corte, dopo aver constatato la sussistenza di un'ingerenza nell'esercizio della libertà di espressione[26] ed aver accertato la presenza di un fondamento normativo di detta restrizione[27], ha valutato se quest'ultima perseguisse un obiettivo legittimo, ai

anche di osservazioni provocatorie, o addirittura inquietanti, subisce dunque un'eccezione quando le affermazioni sono rivolte al sistema giudiziario. Per l'orientamento tradizionale si veda CEDU, *Barthold c. Germania*, ric. 8734/79 (1985), analizzata in F. Abruzzo, *Libertà di stampa, tutela dell'informazione e dei giornalisti alla luce della Convenzione europea dei diritti dell'uomo*, in B. Nascimbene (a cura di), *La Convenzione europea dei diritti dell'uomo. Profili ed effetti nell'ordinamento italiano*, Milano, 2002, 121 ss. Sul punto, anche D. Bosi, *Art. 10, Libertà di espressione*, in C. Defilippi – D. Bosi – R. Harvey (a cura di), *La Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Napoli, 2006, 418 ss.

[25] CEDU, *L.P. e Carvalho c. Portogallo*, cit., § 65.

[26] La Corte europea, com'è noto, è solita affrontare le questioni concernenti possibili violazioni della libertà di espressione attraverso un test trifasico: in primo luogo, l'accertamento della sussistenza dell'ingerenza; in seconda analisi, la ricerca della previsione di legge in base alla quale le autorità nazionali hanno posto in essere l'interferenza; infine, il perseguimento di un fine legittimo di quest'ultima, considerando la necessità della stessa in una società democratica. Nel caso di specie, il fatto che le condanne per diffamazione nei confronti dei ricorrenti costituissero un'ingerenza nell'esercizio dei loro diritti è risultato pacifico anche per le parti stesse. Ivi, § 61.

[27] A tal proposito si rileva, come anticipato, che, per il primo caso, la previsione normativa alla base dell'ingerenza era rappresentata dagli artt. 180 e 184 del codice penale portoghese, i quali puniscono chiunque imputi ad un'altra persona un atto da cui deriva una lesione dell'onore o della reputazione, con una maggiorazione di pena se la vittima di tale reato è un pubblico ufficiale nell'esercizio delle sue funzioni. Nel secondo caso, invece, la responsabilità extracontrattuale è fondata sul citato art. 483 del

sensi dell'art. 10, e risultasse, dunque, una misura necessaria in una società democratica. Nel prendere queste determinazioni, i giudici di Strasburgo hanno sostenuto che, in entrambi i casi, i ricorrenti avevano agito nell'esercizio del mandato attribuitogli e, pertanto, in difesa degli interessi dei loro clienti. La Corte, inoltre, ha anche valutato la natura delle espressioni contestate, distinguendo, come di consueto, le dichiarazioni di fatto dai giudizi di valore[28].

A tal riguardo, nel primo caso, è stato ritenuto che la lettera di contestazione inviata al CSM andasse qualificata come dichiarazione di fatto, in quanto finalizzata a mettere in luce gli errori procedimentali commessi dal Tribunale di Gouveia. In aggiunta, relativamente alle affermazioni con cui l'avvocato aveva sostenuto l'esistenza di un "clima di intimità" tra magistrato e controparte, ritenute giudizi di valore dalle autorità nazionali, i giudici di Strasburgo hanno rilevato che l'art. 127 del codice di procedura civile portoghese prevede espressamente dette parole quale motivo di impugnazione delle sentenze, rendendole, pertanto, «*critiques que tout juge peut s'attendre à recevoir dans l'exercice de ses fonctions*»[29], con esclusione della possibilità che le stesse fossero atte ad offendere l'onore e la reputazione del giudicante. La Corte, in questo caso, ha valutato ammissibile la critica mossa dall'avvocato in considerazione della normale dialettica tra difensori e giudicanti, considerando, inoltre, che l'asserito danno alla reputazione del magistrato appariva comunque di lieve entità, alla luce della natura riservata del procedimento avviato dal professionista dinanzi al CSM.

Per la seconda vicenda, la Corte ha sottolineato come, con la presentazione di un'azione per diffamazione nei confronti del giudice, sia in sede civile sia in sede penale, l'avvocato si fosse limitato a difendere gli interessi dei suoi clienti. Le autorità nazionali, dunque, avevano illegittimamente censurato il solo fatto che il difensore avesse accettato il mandato, ritenendo tale comportamento contrario ai doveri etici imposti dal codice forense. Per giunta, è stato osservato che le accuse mosse dall'avvocato erano fondate su basi fattuali riscontrate dalle stesse corti portoghesi, le quali, difatti, avevano evidenziato come le espressioni utilizzate nei confronti degli imputati gitani risultassero eccessive e superficiali. Circostanza, quest'ultima, che aveva determinato un'elevata copertura mediatica della vicenda, rendendola parte di un dibattito di interesse pubblico sul funzionamento della giustizia.

Infine, i giudici di Strasburgo hanno altresì affrontato l'esame della natura delle sanzioni inflitte ai ricorrenti, identificandolo quale ulteriore parametro per la valutazione della proporzionalità dell'ingerenza delle autorità statali. Nel caso di specie, le severe misure adottate dai giudici portoghesi, ovverosia la condanna al risarcimento di ingenti importi e la sanzione penale inflitta ad uno dei due avvocati, sono state ritenute sproporzionate e potenzialmente idonee a produrre un effetto inibente sull'intera professione forense, con un evidente pericolo di minorazione della difesa degli interessi

codice civile.

[28] Una più analitica disamina della distinzione tra dichiarazioni di fatto e giudizi di valore, compiuta dalla Corte in un recente caso, in M. Castellaneta, *Tutela della reputazione dei politici, libertà di stampa e giudizi di valore con linguaggio provocatorio: la Corte europea procede a un bilanciamento a favore dei giornalisti*, in *questa Rivista*, 2020, 237 ss.

[29] CEDU, *L.P. e Carvalho c. Portogallo*, cit., § 68.

degli assistiti[30].

La stretta connessione tra libertà di espressione ed esercizio del mandato difensivo, presente nei casi analizzati, ha dunque consentito alla Corte di ribadire che, nell'ambito delle loro funzioni e nel rispetto di principi etici e comportamentali, il perimetro di applicabilità della libertà di critica degli avvocati nei confronti dell'operato delle corti è soggetto ad una notevole estensione, con conseguente detrimento della limitazione posta a tutela dell'autorità del potere giudiziario.

Tale conclusione, come anticipato, appare in linea con il consolidato orientamento della Corte europea sul tema oggetto della presente analisi. Ed, invero, sin dalla sentenza *Casado Coca c. Spagna*[31] i giudici di Strasburgo hanno evidenziato che l'avvocato «*en sa qualité d'auxiliaire de la justice, il bénéficie du monopole et de l'immunité de plaidoirie, doit témoigner de discrétion, d' honnêteté et de dignité dans sa conduite*». Alla luce del rapporto di stretta strumentalità tra la libertà di espressione degli avvocati e l'esercizio effettivo del diritto di difesa, la Corte, invertendo l'approccio analizzato in precedenza nell'ambito del bilanciamento dei suddetti interessi coinvolti, ha accordato una maggiore tutela ai professionisti, specialmente in favore di dichiarazioni prodotte nell'interesse diretto dei propri assistiti[32]. In particolare, al riconoscimento in favore degli avvocati del ruolo di «*intermediaries between public and courts*»[33] è conseguita l'attribuzione, in capo agli stessi, di una responsabilità di protezione dell'integrità del sistema giudiziario e del buon funzionamento dello stesso. A tal proposito, giova rilevare che, in un primo momento, la tutela offerta alla libertà di espressione dei difensori era stata ancorata al contesto in cui gli stessi rendevano le dichiarazioni contestate, con un'estensione della protezione per le arringhe pronunciate nelle aule giudiziarie e una restrizione della stessa per osservazioni compiute in contesti diversi[34]. Tuttavia, lo sviluppo di nuovi canali di comunicazione e la conseguente evoluzione della stessa professione forense, dovuta, tra gli altri fattori, ad un sempre maggiore interessamento della collettività alla gestione di importanti vicende giudiziarie, ha comportato un superamento del citato approccio interpretativo ed applicativo dell'art. 10 della Convenzione[35]. In particolare,

[30] La Corte, a ben vedere, aveva trattato una simile questione in precedenza, e, in particolare, nella sentenza CEDU, *Mor. c. Francia*, n. 28198/09 (2001), § 61, e nella più recente pronuncia *Rodriguez Ravelo c. Spagna*, ric. 48074/10 (2016), in cui la violazione dell'art. 10 della Convenzione era stata ravvisata, per l'appunto, in ragione della sola severità della condanna penale inflitta ad un avvocato, capace, dunque, di avere un *chilling effect* sull'intera categoria.

[31] CEDU, *Casado Coca c. Spagna*, ric. 15450/89 (1994). Sul punto, si veda F. Tulkens, *Quel rôle pour les avocats devant la Cour européenne des droits de l'homme*, in *I diritti dell'uomo*, 2017, 7 ss.

[32] A tal proposito si veda l'analisi di D. Spielmann - C. Henry, *Les avocats et la Convention européenne de droits de l'homme*, in *I diritti dell'uomo*, 2016, 510 ss.

[33] CEDU, *Schöpfer c. Svizzera*, ric. 25405/94 (1998), §§ 29-30, con cui la Corte ha altresì precisato che «*regard being had to the key role of lawyers in this field, it is legitimate to expect them to contribute to the proper administration of justice, and thus to maintain public confidence therein*».

[34] In questo senso si veda CEDU, *Steur c. Paesi Bassi*, ric. 39657/98 (2003), nella quale uno dei parametri per sostenere che vi fosse stata una violazione dell'art. 10 della Convenzione è stato, per l'appunto, che «*the criticism was confined to the courtroom*».

[35] Nella sentenza CEDU, *Kyprianou c. Cipro*, ric. 73797/01 (2005), i giudici di Strasburgo hanno evidenziato come gli avvocati «*are certainly entitled to comment in public on the administration of justice, […] their criticism must not overstep certain bounds*» e, allo stesso modo, «*a lawyer's freedom of expression in the courtroom is not unlimited and certain interests, such as the authority of the judiciary, are important enough to justify restrictions on*

pur permanendo una distinzione nel trattamento delle dichiarazioni rese fuori o dentro le aule di giustizia, tale dicotomia, nella più recente giurisprudenza della Corte, è stata utilizzata quale parametro meramente suppletivo ed aggiuntivo, e non più, come accaduto in precedenza, quale elemento fondante la ragione della tutela[36].

Tale impostazione è stata adottata nel caso *Morice c. Francia*[37], in cui la Grande Camera ha ravvisato una violazione della libertà di espressione di un avvocato, condannato per diffamazione per aver sostenuto che determinate condotte dei giudici erano risultate «*completely at odds with the principles of impartiality and fairness*»[38]. Il professionista aveva mosso le suddette critiche attraverso una lettera indirizzata al Ministro della Giustizia, i cui estratti erano stati successivamente ripresi dal noto quotidiano *Le Monde*, alla luce della rilevanza pubblica della questione oggetto del processo. La Corte, da una parte, ha avuto modo di chiarire che la tutela accordata agli avvocati deve necessariamente essere correlata all'indipendenza della professione legale, considerata un elemento «*crucial for the effective functioning of the fair administration of justice*» e, d'altra parte, ha identificato i limiti con i quali i difensori devono adempiere alla suddetta funzione, citando, in particolare, la dignità, l'onore, l'integrità e l'impegno per il buon funzionamento della giustizia[39]. E, a ben vedere, i citati principi di condotta impongono agli avvocati il dovere di «*defend their clients' interests zealously*», motivo per il quale la loro libertà di espressione non può che essere funzionale all'effettivo e concreto esercizio del diritto di difesa[40].

Nella sentenza *L.P. e Carvalho c. Portogallo*, la Corte, però, a nostro avviso, compie un passo decisivo nel rafforzare il diritto alla libertà di espressione degli avvocati. Il diritto di critica all'operato delle corti, seppur soggetto a precise limitazioni – quale, per l'appunto, il fatto che la critica sia mossa in ottica costruttiva, sia per la difesa del cliente, sia per l'intero apparato giudiziario[41]– ha così trovato un'estensione applicativa di ampia portata.

Giova rilevare che la tutela accordata dalla Corte alla libertà di espressione degli avvocati con la citata pronuncia rispecchia, in maniera più che organica, i principi di condotta sanciti, sia sul piano internazionale sia su quello europeo, per stabilire il ruolo

this right». Per un'analisi della pronuncia si veda P.F. Docquir, *Variables et variations de la liberté d'expression en Europe et aux Etats-Unis*, Bruxelles, 2007, 93 ss.

[36] A tal proposito si veda la recente sentenza CEDU, *Ottan c. Francia*, ric. 41841 (2018), per un'analisi della quale ci si permette di rinviare a F. Ceci, *Libertà di espressione degli avvocati e tutela dell'autorità del potere giudiziario: la Corte europea dei diritti dell'uomo procede al bilanciamento dei differenti interessi*, in *questa Rivista*, 2018, 394 ss.

[37] CEDU, *Morice c. Francia*, ric. 29368/10 (2015).

[38] In prima battuta, la Corte aveva invece sostenuto che l'ingerenza da parte delle autorità nazionali rispondesse ad un bisogno sociale imperioso, evidenziando che «*the applicant had overstepped the limits that lawyers had to observe in publicly criticising the justice system*». Ivi, § 95.

[39] Sul punto, F. Krenc, *Les fils du dialogue entre l'avocat et la Cour européenne des droits de l'homme*, in *L'observateur de Bruxelles*, 105, 2016, 26 ss.

[40] Tale conclusione anche in T. Bontinck, *La liberté d'expression de l'avocat*, in *Journal des Tribunaux*, 2016, 362 ss.

[41] A tal proposito si veda la sentenza CEDU, *Peruzzi c. Italia*, ric. 39294/09 (2015), analizzato in R. Incutti, *La libertà di espressione (art. 10 CEDU)*, in A. Di Stasi (a cura di), *CEDU e ordinamento italiano. La giurisprudenza della Corte europea dei diritti dell'uomo e l'impatto nell'ordinamento interno*, Vicenza, 2016, 883 ss.

degli avvocati nella società. E, invero, i *Basic Principles on the Role of Lawyers*[42], adottati nel 1990 nell'ambito dell'ottavo Congresso delle Nazioni Unite sulla prevenzione del crimine e sul trattamento dei trasgressori, offrono una tutela a più livelli alla libertà di espressione degli avvocati – definiti «*as essential agents of the administration of justice*»[43] - declinandola, per l'appunto, in ragione dalla strumentalità della stessa alla salvaguardia di altri valori. Per un verso, difatti, l'art. 20 dei *Principles* dispone che «*Lawyers shall enjoy civil and penal immunity for relevant statements made in good faith in written or oral pleadings or in their professional appearances before a court, tribunal or other legal or administrative authority*», ponendo, dunque, la libertà in parola in connessione con l'esercizio del diritto di difesa. Per altro verso, il combinato disposto degli artt. 16 e 23 dei principi in esame tutela esplicitamente l'esercizio della libertà di espressione degli avvocati in rapporto al diritto degli stessi di partecipare a «*public discussion of matters concerning the law, the administration of justice and the promotion and protection of human rights*», prevedendo, a tal fine, che «*Governments shall ensure that lawyers are able to perform all of their professional functions without intimidation, hindrance, harassment or improper interference*».

Allo stesso modo, il Comitato dei Ministri del Consiglio d'Europa, con l'adozione della Raccomandazione n. 21 del 2000 sulla libertà di esercizio della professione forense[44], ha espressamente previsto che gli avvocati godano di ampia libertà di espressione, specialmente con riferimento al loro diritto/dovere di contribuire al buon funzionamento del sistema giudiziario. A tal fine, l'art. 1 della citata Raccomandazione invita gli Stati all'adozione di ogni misura necessaria per proteggere e promuovere la libertà di esercitare la professione «*without discrimination and without improper interference from the authorities or the public*».

L'evidente parallelismo tra le menzionate disposizioni internazionali ed i principi enunciati a più riprese dalla Corte, oltre a confermare l'evoluzione dei membri della professione forense da ausiliari a protagonisti del sistema giudiziario[45], introduce un ulteriore elemento, ossia che le azioni legali nei confronti degli avvocati possono avere un *chilling effect* non solo sulla libertà di espressione degli stessi, ma anche – aspetto ben più grave nella prospettiva della Corte - sul concreto esercizio del diritto alla difesa, con serie ricadute sul buon funzionamento del sistema giudiziario.

5. Osservazioni conclusive

Alla luce della disamina svolta, la sentenza analizzata costituisce, a nostro avviso, un fondamentale intervento per riportare l'esercizio del diritto di critica al sistema giudiziario nei binari della prevedibilità e della certezza giuridica, considerandolo, per di

[42] United Nations, *Basic Principles on the Role of Lawyers*, 7 settembre 1990. Il testo del documento è reperibile sul sito *refworld.org*.

[43] Ivi, art. 12.

[44] *Recommendation Rec (2000)21 of the Council of Europe's Committee of Ministers to member States on the freedom of exercise of the profession of lawyer*, adottata il 25 ottobre 2000, disponibile all'indirizzo *coe.int*.

[45] CEDU, *Morice c. Francia*, cit., § 148. Per una considerazione opposta, si veda la *concurring opinion* del giudice Kuris nella medesima pronuncia, per il quale «*A lawyer always represents a party and by definition is not able to occupy a central position in the administration of justice*».

più, centrale nell'interesse della buona amministrazione della giustizia. L'ampliamento della tutela offerta alla libertà di espressione degli avvocati, nell'espletamento del mandato conferitogli, restituisce il loro ruolo professionale ad una duplice funzione strettamente connessa ad altri principi enunciati dalla Convenzione. Se, da una parte, il difensore è portatore degli interessi individuali del cliente, tutelati dall'art. 6 della Convenzione, d'altra parte, lo stesso diviene un rappresentante dell'interesse pubblico qualora, con il proprio operato, contribuisca al corretto funzionamento del sistema giudiziario, anche attraverso critiche costruttive nei confronti di quest'ultimo che, come osservato, trovano sistematica tutela nell'alveo dell'art. 10.

In virtù della più alta funzione pubblica svolta dagli avvocati - che, oltre ad essere intermediari tra le corti e la società, assolvono anche un ruolo fondamentale nell'amministrazione della giustizia -, questi ultimi sono sostanzialmente posti sullo stesso piano dei magistrati, con la conseguenza che, per una sorta di principio dei vasi comunicanti[46], abbassare il livello di tutela di una delle due categorie, comporta un detrimento della protezione anche dell'altra.

In questa prospettiva, pertanto, il riferimento ai doveri ed alle responsabilità di cui all'art. 10, par. 2, della Convenzione trova riscontro nelle limitazioni poste a tutela tanto della libertà di espressione, quanto dell'autorità del potere giudiziario. Il bilanciamento compiuto dalla Corte, in altri termini, può, a nostro avviso, essere letto come inquadramento sistematico dei diritti/doveri solo apparentemente contrapposti di avvocati e magistrati, l'esercizio dei quali, nella prospettiva della fisiologica complementarità, garantisce la dialettica collaborativa tra gli stessi e costituisce un pilastro fondamentale dello Stato di diritto.

Conseguentemente, e volendo individuare il precipitato di tale conclusione sul piano nazionale, il percorso compiuto della giurisprudenza di Strasburgo potrebbe offrire un fondamentale contributo all'implementazione del ruolo dell'avvocatura nell'ambito della Costituzione italiana. A ben vedere, infatti, la funzione svolta dai professionisti forensi risulta essenziale per la concreta applicazione delle previsioni costituzionali degli artt. 24 e 111, che, da un lato, tutelano il diritto alla difesa e, dall'altro lato, scolpiscono le garanzie del giusto processo e del contraddittorio. La Costituzione, così, seppure implicitamente, stabilisce un modello di giurisdizione che prevede due principali soggetti: gli avvocati e i giudici[47]. Ad una magistratura indipendente ed autonoma, libera da pressioni e ingerenze di qualsiasi altro potere, corrisponde l'individuazione di un soggetto la cui funzione è posta a controllo, equilibrio e garanzia di questo potere, ovverosia l'avvocato che, pertanto, deve anch'esso poter esercitare la professione in autonomia e indipendenza e, soprattutto, nel rispetto del principio di complementa-

[46] Cfr. P. Calamandrei, *Elogio dei giudici scritto da un avvocato*, Firenze, 1936, 52. L'autore, trattando della legge dei vasi comunicanti, si riferisce, in realtà, ai rapporti tra magistrati ed avvocati, con osservazioni tuttora attuali. Sul punto, in particolare, ritiene inoltre che «giudici e avvocati sono ugualmente organi della giustizia, sono servitori ugualmente fedeli dello Stato, che affida loro due momenti inseparabili della stessa funzione. […] Qualsiasi perfezionamento delle leggi processuali rimarrebbe lettera morta, là dove, tra i giudici e gli avvocati, non fosse sentita, come legge fondamentale della fisiologia giudiziaria, la inesorabile complementarità, ritmica come il doppio battito del cuore, delle loro funzioni».

[47] In questo senso, si vedano le riflessioni di M. Laforgia - F. Contri, *Il lavoro dell'avvocato, ecologia e organizzazione della professione forense*, Bari, 2018, spec. 25 e 41 ss.

rietà di cui si è detto.

In questa direzione, la fiducia nella giustizia ed il buon funzionamento della giurisdizione, a fondamento del patto sociale senza il quale lo Stato perde la sua legittimazione, trovano, anche nella prospettiva della Corte europea, un efficace strumento attuativo nella libertà di espressione degli avvocati.

Note a sentenza

Sezione comparata

Soluzioni tradizionali per piattaforme moderne: la *state action* (non) mostra i segni del tempo

Davide Zecca

Corte d'appello federale degli Stati Uniti d'America per il Nono circuito, 26 febbraio 2020, *Prager University, v. Google and YouTube*, No. 18-15712, D.C. No. 5:17-cv-06064-LHK

Non integra uno *state actor* una piattaforma di *social networking* in rete, poiché di proprietà privata e non esercitante una funzione tradizionalmente ed esclusivamente statale, essendo pertanto esclusa dall'obbligo di assicurare agli utenti le garanzie di libertà di manifestazione del pensiero di cui al Primo emendamento alla Costituzione.

Sommario

1. *Prager University* e la policy di moderazione dei contenuti di YouTube. – 2. Quale *freedom of speech* senza *state action*? – 3. Le piattaforme di *Internet hosting* fra *public forum* e Drittwirkung.

Keywords

hosting provider - state action doctrine - public forum - collateral censorship - Drittwirkung

1. *Prager University* e la policy di moderazione dei contenuti di YouTube

La controversia in commento origina dall'azione intrapresa dalla Prager University (d'ora innanzi, "PragerU") presso la Corte federale distrettuale per il Distretto della California settentrionale avverso YouTube e la sua società controllante, Google. L'attore aveva chiesto al giudice adito la concessione della misura cautelare della esclusione dei video caricati dal proprio account di riferimento dalla categoria di quelli ad accesso riservato. Al diniego di concessione delle dette misure e all'invito a riformulare l'oggetto della domanda rivolta al giudice, PragerU ha impugnato la pronuncia di prime cure sull'istanza cautelare presso la Corte d'appello federale per il Nono circuito, che nel febbraio scorso si è pronunciata confermando la sentenza del giudice distrettuale.
PragerU, a dispetto del nome, non è un'autentica istituzione accademica, bensì un'organizzazione senza scopo di lucro a fini di istruzione, che si prefigge lo scopo di "fornire punti di vista e prospettive conservatrici riguardo a questioni pubbliche che essa ritiene sovente trascurate". La sua attività principale consiste nella realizzazione di contenuti

multimediali, per lo più audiovisivi, che sono resi disponibili sul proprio sito Internet e caricati altresì su YouTube, la nota piattaforma di *video hosting* di proprietà della multinazionale Google.

Gli utenti che aprano un account Google o YouTube allo scopo di caricare contenuti sulla piattaforma devono fornire il proprio consenso ai termini di servizio e rispettare le linee guida della comunità, i quali prevedono che i gestori della piattaforma possano rimuovere un contenuto o circoscrivere l'accesso a esso. Questo può avvenire laddove si verifichino violazioni degli stessi termini di servizio o quando i contenuti siano ritenuti non adatti ai minori di età. Il caso di specie ricade in questa seconda fattispecie, poiché concerne l'inclusione di alcuni dei video caricati da PragerU nella categoria di quelli che non siano mostrati fra i risultati di ricerca all'utente o non siano accessibili allo stesso allorquando sia attivata la c.d. "Modalità con restrizioni". Le linee guida della piattaforma relative a questo filtro specificano che i contenuti ritenuti idonei a un pubblico adulto, vale a dire quelli contenenti immagini o riferimenti ad alcool, sostanze stupefacenti, scene a carattere sessuale e violenza (ivi compresa quella scatenata da agenti della natura), ma anche quelli che forniscano dettagli specifici su vicende di terrorismo, guerra, crimine e controversie di natura politica, potrebbero non essere accessibili una volta attivata la "Modalità con restrizioni". L'inclusione di un video in questa categoria avviene a opera di un algoritmo automatico programmato per analizzare metadati, titolo e linguaggio utilizzato nel video oppure personalmente dall'utente. Tale qualificazione del contenuto a opera dell'algoritmo viene notificata a chi lo abbia caricato, il quale può richiedere che la decisione sia esaminata nuovamente da un gruppo di moderatori in carne e ossa.

Le doglianze di PragerU nascono dall'inclusione di diverse decine di video caricati dall'account della stessa sulla piattaforma nel novero di quelli esclusi dalla visualizzazione in "Modalità con restrizioni" e dalla decisione di YouTube stessa di impedire a terzi di pubblicizzare i propri prodotti con brevi clip video prima o durante i video di PragerU (c.d. demonetizzazione), che ha come effetto la perdita di una possibile fonte di approvvigionamento di risorse finanziarie per l'organizzazione stessa. Nonostante la qualificazione dei video in tale categoria sia stata impugnata come previsto dalle regole della piattaforma, l'accesso ad alcuni video è ancora possibile soltanto disattivando il filtro di ricerca e a essi non è ancora possibile associare alcuna promozione pubblicitaria.

PragerU ha dunque citato in giudizio YouTube e la sua società controllante Google per non aver garantito all'organizzazione stessa la libertà di manifestazione del pensiero di cui essa gode a norma del I emendamento alla Costituzione degli Stati Uniti d'America e per la violazione delle disposizioni sulla pubblicità ingannevole di cui al Lanham Act[1], a causa dello slogan di YouTube che afferma come la piattaforma sia "impegnata a coltivare una comunità ove ciascuna voce possa essere sentita".

[1] 15 U.S.C. § 1125(a)(1)(B).

2. Quale *freedom of speech* senza *state action*?

Seattle e la tendenzialmente progressiva Corte d'appello federale per il Nono circuito non sono Washington e la Corte Suprema, così come la redattrice della sentenza (Margaret McKeown, che scrive anche per i colleghi Jay Bybee e Fernando Gaitan Jr.) non è *Justice* Kavanaugh. Ciononostante, l'esito della pronuncia in questo febbraio 2020 è il medesimo di quella del giugno 2019 dinanzi alla più alta Corte federale: infatti, l'inevitabile e costante riferimento della Corte d'appello nell'ambito della pronuncia in commento è il caso *Manhattan v. Halleck*, deciso di misura (5-4) dalla Corte Suprema giusto otto mesi prima[2].

La decisione comincia prendendo il toro per le corna, con l'argomentazione che la doglianza relativa all'illegittima censura della libera manifestazione del pensiero dell'organizzazione da parte della piattaforma di *video hosting* incontra un ostacolo apparentemente insormontabile, vale a dire la natura privatistica del gestore dello spazio in questione, che, peraltro, nemmeno l'appellante contesta. La clausola relativa alla libertà di manifestazione del pensiero di cui al I emendamento, ricorda la Corte d'appello citando anche il caso *Hudgens v. NLRB*[3], proibisce soltanto l'interferenza con il godimento di tale prerogativa a opera di una pubblica autorità, sia essa federale o di uno Stato federato. Né si può ritenere che l'avvento dell'era digitale abbia scardinato, a parere della Corte d'appello, tale principio: prova ne è l'applicazione che ne ha fatto la Corte Suprema nel *term* precedente con riferimento ai canali televisivi via cavo a pubblico accesso, la cui gestione a opera di una società privata creata *ad hoc* dall'amministrazione cittadina di New York non è stata ritenuta sufficiente a qualificare l'attività della stessa come *state action*. D'altronde, ricorda la sentenza citando la recente pronuncia della Corte Suprema, la condotta consistente nel mero offrire una piattaforma per la manifestazione del pensiero ai terzi non è funzione tradizionalmente ed esclusivamente pubblica e un'entità privata non si trasforma per ciò stesso soltanto in un'istituzione pubblica, che, come tale, è vincolata ad assicurare le garanzie di cui al I emendamento. Il riferimento della argomentazione non è però la sola recente sentenza della Corte Suprema, poiché la stessa Corte d'appello per il Nono circuito si era già espressa venti anni or sono conformemente con riferimento a piattaforme Internet[4] e più di recente altre corti distrettuali a livello federale hanno statuito nella medesima direzione con riferimento alle piattaforme di *social networking* emerse nell'ultimo decennio[5].

---

[2] *Manhattan Community Access Corp. v. Halleck*, 139 S. Ct. 1921. A proposito, sia consentito rinviare a D. Zecca, *I canali a pubblico accesso non sono un* public forum*: i perché di un'occasione persa*, nota a Corte Suprema degli Stati Uniti d'America, 17 giugno 2019, *Manhattan Community Access Corp. v. Halleck*, No. 17–1702, in *questa Rivista,* 1, 2020, 270 ss.

[3] 424 U.S. 507 (1976).

[4] *Howard v. Am. Online Inc.*, 208 F.3d 741, 29 marzo 2000.

[5] La stessa pronuncia cita *Freedom Watch v. Google*, 368 F. Supp. 3d 30, 40, 14 marzo 2019 (Corte distrettuale per il District of Columbia); *Green v. YouTube*, 2019 WL 1428890, 13 marzo 2019 (Corte distrettuale per il New Hampshire); *Nyabwa v. Facebook*, 2018 WL 585467, 26 gennaio 2018 (Corte distrettuale per il distretto meridionale del Texas); *Shulman v. Facebook.com*, 2017 WL 5129885, 6 Novembre 2017 (Corte distrettuale per il New Jersey); *Forbes v. Facebook*, 2016 WL 676396, 18 febbraio 2016 (Corte distrettuale per il distretto orientale di New York); *Doe v. Cuomo*, 2013 WL 1213174, 25 febbraio 2013 (Corte distrettuale per il distretto settentrionale di New York).

L'allegazione di PragerU, secondo la quale YouTube diviene entità pubblica ai fini dell'opponibilità delle prerogative contenute nel *Bill of rights* federale in ragione della funzione pubblica svolta (la messa a disposizione di uno spazio privato per la discussione e la manifestazione del pensiero di terzi) non trova terreno fertile dinanzi al giudice d'appello, che ricorda come sia la stessa giurisprudenza del Nono circuito a richiedere che tale funzione sia tradizionalmente ed esclusivamente appannaggio delle pubbliche autorità[6]. Peraltro, si tratta della medesima argomentazione a cui è ricorsa meno di un anno fa la stessa Corte Suprema in *Manhattan v. Halleck*, come dimostrato anche dall'abbondanza di richiami a precedenti decisioni conformi dello stesso vertice del giudiziario federale.

Nemmeno il riferimento al riconoscimento dell'obbligo di garanzia delle prerogative costituzionali individuali degli utenti che i proprietari privati sono tenuti ad assicurare laddove mettano determinati beni privati a disposizione del pubblico come delineato in *Marsh v. Alabama*[7] convince il collegio, che ricorda come la Corte Suprema abbia precedentemente interpretato tale principio restrittivamente, da applicarsi soltanto in quelle poco frequenti circostanze ove un soggetto privato svolga tutte le funzioni di un'autorità municipale[8]. In tutta evidenza, afferma la Corte d'appello, non è questo il caso di YouTube.

Nemmeno si può concludere, prosegue la sentenza, che la piattaforma svolga una funzione pubblica per antonomasia mediante la regolazione della manifestazione del pensiero in uno spazio pubblico (*public forum*). Non persuade la Corte neanche l'allegazione di PragerU secondo la quale un soggetto privato diverrebbe un *public forum* laddove adibisse uno spazio di sua proprietà privata a luogo di pubblica discussione: si tratta di uno spunto tratto dalla teoria del *designated public forum*, la quale tuttavia richiede che sia una pubblica autorità a designare con un esplicito atto di disposizione un dato spazio (non rientrante nella definizione di *traditional public forum*[9]) come aperto al pubblico dibattito[10]. YouTube non rientra nemmeno in tale categoria, non essendo né di proprietà, né in uso né controllata da alcuna pubblica autorità, così frustrando ogni possibile appello alla dottrina di cui sopra.

Nemmeno soccorre il disperato tentativo di PragerU di qualificare la piattaforma come *public forum* argomentando a partire dalla dichiarazione di YouTube stessa in questo senso. La formulazione di generici impegni a favorire la libera manifestazione del pensiero o anche un'isolata affermazione pronunciata dall'amministratore delegato della stessa dinanzi a una commissione congressuale di considerare la piattaforma uno spazio pubblico di discussione neutrale non sono sufficienti a trasformare un bene di titolarità privata in *public forum*. Tale natura di un dato spazio non è infatti una libera scelta disponibile a ciascun soggetto privato, conclude la Corte d'appello, rifiutando di conferire alcuna patente di legittimità a una supposta *opt-in theory* del I emendamento.

Per quanto concerne la doglianza relativa alla violazione delle disposizioni in tema di

[6] *Lee v. Katz*, 276 F.3d 550, 10 gennaio 2002.

[7] 326 U.S. 501 (1946).

[8] *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972).

[9] Per la quale si veda *Hague v. CIO*, 307 U. S. 496 (1939).

[10] *Cornelius v. NAACP Legal Def. & Educ. Fund, Inc.*, 473 U.S. 788 (1985).

pubblicità ingannevole, la Corte d'appello ricorda come essa abbia precedentemente interpretato lo *statute* di riferimento come richiedente l'allegazione (e prova) in giudizio che il convenuto abbia posto in essere una rappresentazione falsa o fuorviante di un fatto nell'ambito di attività commerciale o promozionale che abbia descritto in modo errato la natura, le caratteristiche, le qualità o l'origine geografica di merci, servizi o attività commerciali proprie o altrui[11]. Poiché le affermazioni di YouTube relative alla propria *policy* di moderazione dei contenuti non rientrano nella categoria delle attività di pubblicità commerciale o promozionali, bensì sono formulate al mero scopo di illustrare una funzione della piattaforma a disposizione degli utenti, il giudice respinge l'argomentazione dell'appellante. Né, prosegue il collegio, sussiste alcun elemento ingannevole o fuorviante nell'indicazione di un video come non accessibile in "Modalità con restrizioni". D'altronde, le vanterie di YouTube relative al proprio impegno per la libera manifestazione del pensiero altro non sono che affermazioni pubblicitarie condite da una vena di esagerazione e, in quanto tali, non azionabili in giudizio.

3. Le piattaforme di *Internet hosting* fra *public forum* e *Drittwirkung*

Se nulla di innovativo pare potersi trarre dalla pronuncia della Corte d'appello federale per il Nono circuito rispetto all'orientamento tradizionale della giurisprudenza federale in ordine all'opponibilità delle garanzie di cui al *Bill of rights* ai soggetti privati, nel solco della recente (seppur contrastata) pronuncia della Corte Suprema in *Manhattan v. Halleck*, giova svolgere alcune brevi riflessioni sull'attualità della dottrina della *state action* con specifico riferimento alla *Free Speech clause*, mettendo in luce alcuni profili che rendono il caso di YouTube non del tutto sovrapponibile a quello della *Manhattan Neighborhood Network*.

Come sopra ricordato e noto, la giurisprudenza federale americana ha costantemente e convintamente ritenuto le disposizioni del *Bill of rights* federale come unicamente pertinenti i rapporti sul piano verticale tra autorità federali (e, a partire dal momento in cui si è avviata la c.d. *selective incorporation*, anche statali[12]) e cittadini[13], in una logica che vedeva il testo originario della Costituzione definire i principi della forma di governo e il catalogo dei diritti delineare quelli della forma di Stato. Confinare l'efficacia delle disposizioni dei primi dieci emendamenti al rapporto fra autorità e cittadini ha dunque significato che negli Stati Uniti d'America non ha attecchito la dottrina c.d. della *Drittwirkung*, vale a dire dell'efficacia orizzontale dei diritti sanciti in Costituzione: pur con qualche (rilevante) eccezione, infatti, essi non fondano pretese nei rapporti fra i privati[14]; d'altronde, la cultura giuridica americana sembra appunto circoscrivere l'applicabilità delle disposizioni del *Bill of rights* al rapporto fra governo e cittadinanza,

[11] *Southland Sod Farms v. Stover Seed Co.*, 108 F.3d 1134, 11 marzo 1997.

[12] *Gitlow v. New York*, 268 U.S. 652 (1925).

[13] La nascita della *state action doctrine* si fa risalire a *The Civil Rights Cases*, 109 U.S. 3 (1883).

[14] G. Romeo, *Building Integration through the Bill of Rights: The European Union at the Mirror*, in *Ga. J. Int'l & Comp. L.*, 47, 2018, 40-42.

lasciando che la sfera dei rapporti privatistici sia regolata dal secolare patrimonio giuridico di *common law*.

Invero, tale perentoria affermazione è stata mossa in dubbio, sottolineando come, se è vero che non esiste un effetto orizzontale diretto delle disposizioni costituzionali concernenti i diritti individuali dei cittadini (salvo il caso straordinario dell'abolizione della schiavitù a opera del XIII emendamento), il caso degli Stati Uniti d'America sarebbe piuttosto ascrivibile alla categoria degli ordinamenti giuridici caratterizzati da un'efficacia orizzontale indiretta (forte); ciò si concretizzerebbe tramite la subordinazione delle norme che regolano i rapporti privatistici alle disposizioni costituzionali sui diritti, così che l'efficacia della Costituzione nei rapporti fra privati non si concretizzerebbe in una mera influenza dei principi in essa sancita sulla legislazione, bensì in un vero e proprio vincolo di validità della disciplina di diritto privato[15]. Non potendo discutere con l'opportuno grado di dettaglio in questa sede la questione, si consenta di precisare, con brutale sintesi che giustizia non fa alla complessità della questione, come la ragione addotta per giustificare una ricostruzione dell'effetto orizzontale indiretto nel sistema americano appaia piuttosto una conseguenza diretta del principio di supremazia gerarchica della Costituzione rispetto alle fonti del diritto di rango inferiore (che, peraltro, viene invocato alla luce della c.d. *Supremacy Clause*) che non una spia dell'applicabilità verso terzi dei diritti sanciti dalla *supreme law of the Land*.

Questa ricostruzione ha fondato una recente proposta di lettura del I emendamento non più secondo la tradizionale logica bipolare, che si muove sull'asse Stato-soggetto privato e sacrifica pertanto i diritti dei cittadini laddove si faccia altresì questione della libertà di manifestare il pensiero di piattaforme private, bensì suggerendo un approccio pluralista che ponga sul piatto della bilancia, da un lato, il diritto degli intermediari a non vedere compressa la propria libertà di espressione, dall'altro, il diritto dei cittadini a esprimere liberamente il proprio pensiero in tali spazi digitali[16]; una tale prospettazione della questione, che non si limita a confrontare interessi perseguiti da un'amministrazione pubblica e diritti di un intermediario privato, come evidente, è suscettibile di condurre il giudizio di bilanciamento a un esito differente.

La suddetta sembra, tuttavia, una strada impervia da percorrere; d'altronde, non pare facile nemmeno l'alternativa, vale a dire dimostrare la possibilità di sussumere l'attività svolta dalle piattaforme di *hosting* sotto la fattispecie di quelle tradizionalmente ed esclusivamente pubbliche, alle quali la giurisprudenza federale ha riconosciuto la natura di *state action* anche quando poste in essere da soggetti formalmente privati[17].

Nemmeno sembra plausibile la qualificazione degli intermediari Internet alla stregua dei c.d. *traditional public forum*: per quanto l'ampiezza dell'*audience* e l'accessibilità siano paragonabili, se non superiori, a quelli di molti altri luoghi fisici appartenenti a tale categoria, la giurisprudenza sul tema è piuttosto conservatrice e pare avere cristallizzato un *numerus clausus* di luoghi pubblici non estendibile per via analogica. Non che la sug-

[15] S. Gardbaum, *The Horizontal Effect of Constitutional Rights*, in *Mich. L. Rev.*, 102, 2003, 387 ss., spec. 414-422.

[16] M. Yemini, *Missing in State Action: Toward a Pluralist Conception of the First Amendment*, in *Lewis & Clark L. Rev.*, 23, 2020, 1201 ss.

[17] *Jackson v. Metropolitan Edison Co.*, 419 U. S. 345, 352 (1974).

gestione di paragonare gli stessi a pubbliche piazze sia stata del tutto ignorata, come dimostrano i *dicta* dell'opinione dell'ormai ritirato Justice Kennedy in *North Carolina v. Packingham*[18]; in ogni caso, la decisione della Corte in *Manhattan v. Halleck* del *term* successivo sembra escludere che la maggioranza dei *Justices* in carica voglia prendere seriamente in considerazione l'ipotesi (per quanto, in ogni caso, desumere da un giudizio su canali televisivi conclusioni certe con riferimento al diverso caso di piattaforme Internet potrebbe rivelarsi incauto)[19].

D'altronde, pare opportuno fare brevemente presente come si faccia largo, in un mondo sempre più caratterizzato dal dibattito pubblico in rete (a maggior ragione in un'epoca dove il distanziamento sociale sembra essere una prospettiva di medio-lungo periodo), il rischio crescente di una diffusione sempre più capillare di forme di cosiddetta *collateral censorship*, che si palesa quando viene assegnato un potere molto significativo agli operatori e gestori di tali piattaforme, i quali svolgerebbero, eventualmente anche in buona fede, quella funzione di censura che tradizionalmente spetterebbe allo Stato e che, per ragioni di eccessiva prudenza, potrebbero depauperare la sfera pubblica di contributi utili ad arricchire il dibattito[20].

Se le circostanze reali che si manifestano con crescente frequenza vedono lo Stato limitarsi sempre più allo svolgimento di funzioni regolatorie, delegando il potere di censura agli intermediari, non pare però più inconcepibile accettare il dato di fatto che le piattaforme esercitino attività analoghe a quelle dello Stato: stando così le cose, la regolazione della manifestazione del pensiero da parte delle suddette diviene la regola e non più l'eccezione.[21] Se si accetta tale premessa, basata in larga parte su evidenze empiriche, la logica conseguenza sarebbe di constatare come tali soggetti svolgono ora tale attività in percentuale preponderante, da cui a cascata discenderebbe che, in quanto si tratta di attività tradizionalmente ed esclusivamente svolta dallo Stato, essi sarebbero tenuti al rispetto delle garanzie di cui al *Bill of rights*, non potendo più schermarsi dietro la barriera della *state action doctrine*.

Per quanto le considerazioni di cui sopra possano apparire giuridicamente e argomentativamente fondate, sia consentito, in chiusura, esprimere un certo scetticismo sulla possibilità di uno scostamento della giurisprudenza federale da quella che per oltre un secolo è stata considerata una stella polare, nonostante l'implicazione concreta di tale orientamento rischi di essere non tanto la garanzia di un più vivace pluralismo, derivante dalla libertà degli operatori di tali piattaforme, bensì una restrizione delle opinioni e dei pareri ai quali il pubblico dibattito possa attingere, denotando una tendenziale sfiducia nel buon funzionamento della sfera pubblica di discussione, in quella dinamica che all'inizio del secolo scorso Oliver Wendell Holmes contribuì a delineare come *marketplace of ideas*[22].

---

[18] 137 S. Ct. 1730 (2018).

[19] M. Yemini, *Missing in State Action,* cit., 1176-1179.

[20] Il concetto fu menzionato per la prima volta da M.I. Meyerson, *Authors, Editors, and Uncommon Carriers: Identifying the Speaker within the New Media*, in *Notre Dame L. Rev.*, 71, 1995, 118; la questione è stata poi delineata più approfonditamente e compiutamente da J.M. Balkin, *Free Speech and Hostile Environments*, in *Colum. L. Rev.*, 99, 1999, 2298.

[21] J.M. Balkin, ivi, 1195.

[22] O.W. Holmes, *Dissenting Opinion*, *Abrams v. United States*, 250 U.S. 630 (1919).

Una stampa libera e pluralista è essenziale per garantire un giornalismo di qualità. Il diritto d'autore e i diritti connessi tutelano il patrimonio culturale

Cecilia Trevisi

Autorité de la concurrence, 9 aprile 2020, decisione 20-MC-01, *Syndicat des éditeurs de la presse magazine e altri*

Costituisce abuso di posizione dominante sul mercato dei servizi di ricerca generalisti il rifiuto generalizzato da parte di uno dei motori di ricerca più noti al mondo di non riconoscere alcun corrispettivo per la ripresa di contenuti editoriali o dei titoli degli articoli, sfuggendo all'applicazione del nuovo diritto connesso a beneficio degli editori di giornali e agenzie di stampa che conferisce loro il diritto di autorizzare o vietare la riproduzione delle loro pubblicazioni su piattaforme, aggregatori e motori di ricerca.

Sommario

1. Il dilemma del "titolo" degli articoli - 2. Il modello economico di Google. - 3. La posizione delle parti. - 4. La decisione dell'*authority*.

Keywords

stampa - diritto d'autore - diritti connessi - *snippets* - *crawler*

1. Il dilemma del "titolo" degli articoli

Tutela della stampa, dell'editoria, del giornalismo. È ciò che emerge in prima battuta dalla lettura di oltre settanta pagine di provvedimento. L'Antitrust francese - dopo aver esaminato soggetti, mercato[1] e l'operatività tecnica del motore di ricerca più noto al

[1] La Commissione ha ritenuto che la fornitura di servizi di ricerca generalisti (o generali) costituisce un'attività economica e un mercato rilevante. Ha dunque distinto questo mercato da quello dei siti che forniscono contenuti come, ad esempio, Wikipedia, IMDb, The New York Times et Nature. Ha inoltre distinto questo mercato da quello dei servizi di ricerca specializzati e dal mercato dei social media. Infine, ha ritenuto che questo mercato includesse sia i servizi forniti su terminali fissi (computer) sia quelli forniti su terminali mobili (cellulare, tablet). Nelle sue osservazioni, Google non ha mai messo in discussione la definizione di mercato per i servizi di ricerca generalisti, ma ha contestato l'esistenza di un nesso causale tra la posizione dominante che deterrebbe su questo mercato e le pratiche di cui è stato accusato.

mondo[2] - scompone passo dopo passo le difese affrontate nel contradditorio delle parti per giungere ad una decisione che, seppur cautelare (quindi interinale e soggetta ad impugnativa), riconosce in maniera lapidaria che si tratterrebbe di abuso di posizione dominante da parte del motore di ricerca. L'interesse tutelato è la democrazia in una delle sue primarie estrinsecazioni: la libertà di stampa. Protezione ricercata dalla direttiva (UE) 2019/790 (considerando 54 e 55)[3] e perseguita a più riprese dal legislatore francese con la legge n. 2019-775 art. 4, adottata il 24 luglio 2019, che ha recepito l'art. 15 della direttiva, creando un diritto connesso a beneficio delle agenzie di stampa e degli editori.

La scelta francese di un recepimento così rapido - appena tre mesi dopo l'adozione della Direttiva - si spiega con il desiderio dei parlamentari di rispondere a quella che consideravano una situazione di emergenza: risollevare l'industria dell'editoria e della stampa. «I motori di ricerca riproducono e distribuiscono sulle proprie pagine, milioni di testi, fotografie, video senza alcuna licenza, causando danni ingenti alle agenzie di stampa e ai loro autori. Questi motori di ricerca sono diventati delle vere e proprie banche di informazioni e dati, sfruttando contenuti che non hanno né creato né finanziato e per i quali non pagano alcun compenso»[4].

In particolare, le tecniche recenti ("*snippets*") fanno sì che buona parte degli internauti si accontenti di questa modalità di informazione senza la necessità cliccare sul relativo *link* e quindi visitare il sito corrispondente, con conseguente perdita di risorse, sotto forma di abbonamenti o pubblicità.

---

[2] Il report *Brand Finance Global 500 2020*, presentato a Davos durante il World Economic Forum, ha calcolato il valore dei marchi più celebri al mondo. Le società con il valore di mercato più grande al mondo sono le tre società statunitensi Amazon, Google (160 miliardi) ed Apple (140 miliardi di USD).

[3] «Una stampa libera e pluralista è essenziale per garantire un giornalismo di qualità e l'accesso dei cittadini all'informazione e dà un contributo fondamentale al dibattito pubblico e al corretto funzionamento di una società democratica. L'ampia disponibilità di pubblicazioni di carattere giornalistico online ha comportato la nascita di nuovi servizi online, come gli aggregatori di notizie o i servizi di monitoraggio dei media, per i quali il riutilizzo di pubblicazioni di carattere giornalistico costituisce una parte importante dei loro modelli di business e una fonte di introiti. Gli editori di giornali incontrano una serie di problemi nel concedere licenze di utilizzo online delle loro pubblicazioni ai prestatori di questo tipo di servizi, redendo ancora più difficile per loro recuperare gli investimenti effettuati. In assenza del riconoscimento degli editori di giornali quali titolari di diritti, la concessione delle licenze e il rispetto dei diritti nelle pubblicazioni di carattere giornalistico riguardo agli utilizzi online da parte di prestatori» (considerando 54). «Il contributo organizzativo e finanziario degli editori nel produrre pubblicazioni di carattere giornalistico va riconosciuto e ulteriormente incoraggiato per garantire la sostenibilità dell'editoria e favorire in tal modo la disponibilità di informazioni affidabili. È quindi necessario prevedere a livello di Unione una tutela giuridica armonizzata per gli utilizzi online delle pubblicazioni di carattere giornalistico da parte di prestatori di servizi della società dell'informazione, che lasci impregiudicate le vigenti norme sul diritto d'autore nell'ordinamento dell'Unione applicabili agli utilizzi privati o non commerciali delle pubblicazioni di carattere giornalistico da parte di singoli utenti, anche ove tali utenti condividano pubblicazioni di carattere giornalistico online. Tale protezione dovrebbe essere garantita in maniera efficace mediante l'introduzione nell'ordinamento dell'Unione di diritti connessi a quello d'autore per la riproduzione e la messa a disposizione del pubblico di pubblicazioni di carattere giornalistico da editori stabiliti in uno Stato membro nell'ambito di utilizzi digitali da parte di prestatori di servizi della società dell'informazione ai sensi della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio. La tutela giuridica per le pubblicazioni di carattere giornalistico prevista dalla presente direttiva dovrebbe andare a beneficio degli editori stabiliti in uno Stato membro e aventi la sede sociale, l'amministrazione centrale o il centro di attività principale all'interno dell'Unione». (considerando 55).

[4] *Proposition de loi tendant à créer un droit voisin au profit des agences de presse et des éditeurs de presse*, in *senat.fr.*

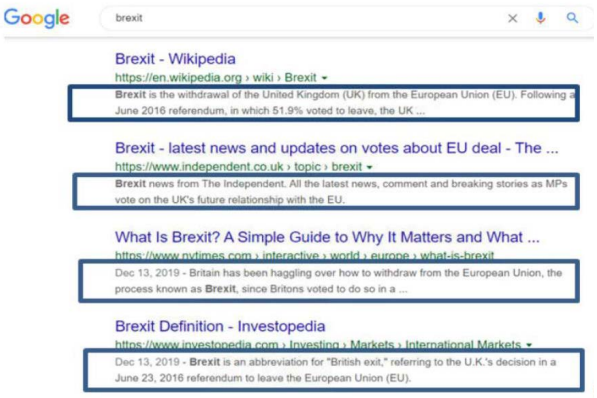
Nell'ordinamento francese è stata avvertita, prima di ogni altro Paese dell'Unione, una reale e concreta urgenza ad intervenire: editori e agenzie di stampa perdono risorse ogni giorno e, ogni giorno, le grandi piattaforme raccolgono profitti usando articoli scritti da giornalisti e foto prodotte dalle agenzie.
Come già accade per altri settori dell'industria culturale (editori di fonogrammi e videogrammi, società di comunicazione audiovisiva), l'istituzione di un diritto connesso a beneficio delle agenzie di stampa e degli editori di stampati dovrebbe, secondo la volontà del legislatore, consentire di ottenere una migliore protezione dei loro contenuti, proteggendo gli investimenti sia umani che finanziari. L'obiettivo di questo nuovo diritto connesso è dunque quello di riequilibrare il potere tra attori digitali e operatori di stampa ridefinendo la condivisione (e la ripartizione) del valore a favore di quest'ultimo.
Google, all'indomani del recepimento da parte dell'ordinamento francese dell'art. 15 della direttiva 2019/790 (avvenuto con la legge n. 2019-775 del 24 luglio 2019), ha cercato di elidere il nuovo diritto connesso forzando la lettera della direttiva, prima, e della legge francese, poi, concentrandosi sulla struttura ed efficacia dei titoli. Ritenendo in linea di principio che i titoli degli articoli di fatto sfuggono all'applicazione del nuovo diritto connesso (per la sintesi della loro formulazione), ha continuato a mostrare solo i titoli degli articoli di stampa all'interno dei vari servizi offerti, pur in assenza di un accordo con editori e agenzie di stampa interessati o a riconoscere il corrispettivo per il loro utilizzo.
L'equazione perseguita è stata quindi la seguente: niente licenza di uso gratuito dei contenuti editoriali, niente anteprima dei contenuti per tutti i servizi di Google. Resta solo il titolo.

2. Il modello economico di Google

L'antitrust francese prima di affrontare le ragioni che hanno portato a ritenere che vi fosse un abuso di posizione dominante da parte del noto motore di ricerca, analizza nel dettaglio il modello economico e le modalità di funzionamento dei servizi di informazione offerti da Google.
Quello informativo è un servizio (sarebbe meglio dire di una pluralità di servizi) offerto gratuitamente agli utenti in connessione al servizio principale di *Google Search* o quale servizio autonomo a cui è sempre possibile accedere senza la corresponsione di alcun compenso. Il modello economico su cui si basa Google riguarda l'interazione tra alcuni servizi forniti gratuitamente agli utilizzatori (che permettono al motore di ricerca di accedere ai dati personali dei fruitori) e i servizi di pubblicità on-line grazie ai quali Google trae la maggior parte dei propri ricavi.
L'attività di Google consiste nel creare prodotti e servizi per gli utenti e offrire agli inserzionisti opportunità pubblicitarie di qualità. Google non vende i dati dell'utente stesso. I dati rappresentano un elemento del processo di generazione degli annunci che consentono di identificare quelli pertinenti per un utente. La pubblicazione di annunci pertinenti aumenta la propria utilità per gli utenti e contestualmente migliora l'efficacia

per gli inserzionisti, poiché incrementa la probabilità che i clic provengano da utenti che sono veramente interessati a quella specifica offerta.
Il servizio "cerca con Google" (*Google Search)* è la funzione di base offerta dal motore di ricerca, accessibile dal sito *www.google.com* o dalle sue declinazioni locali (in Francia *www.google.fr*) e permette agli utilizzatori di cercare qualsiasi informazione all'interno del circuito della rete internet partendo da una o più parole chiave grazie alle quali il servizio di Google propone una serie di risultati.
Per fare ciò, il sistema di *Google Search* esegue una serie di operazioni: *(i)* effettua la scansione dei siti web per raccogliere informazioni sul loro contenuto, il cosiddetto *crawling*[5]; *(ii)* memorizza queste informazioni nel suo indice; *(iii)* classifica questi siti in base alla loro probabile rilevanza e li visualizza nelle pagine dei risultati.
Google non riceve alcun corrispettivo monetario per ordinare i risultai di ricerca; tali risultati, cosiddetti "naturali", sono pertanto una scelta dell'algoritmo di ricerca.
All'interno del sistema di *Google Search* può essere consentito visualizzare i risultati relativi agli avvenimenti di attualità sotto forma di risultati "standard", essi mostrano cioè un titolo, il nome del sito web di origine e un estratto di testo. Questi risultati possono essere arricchiti includendo un'immagine in miniatura. Questi metodi di visualizzazione si applicano indipendentemente dal supporto utilizzato (computer, telefono cellulare, tablet).
Google utilizza il termine inglese "*snippet*" (in francese, "*extrait*") per indicare l'estratto del testo visualizzato nei risultati di ricerca. Il termine "*snippet*", secondo Google, non copre il titolo o alcuna immagine in miniatura che appare nei risultati di ricerca dunque ciò che costituisce uno "*snippet*" il noto motore di ricerca, corrisponde solo agli estratti di testo che nell'immagine che segue compaiono nei riquadri blu.

Capture d'écran - Google Search - Snippets



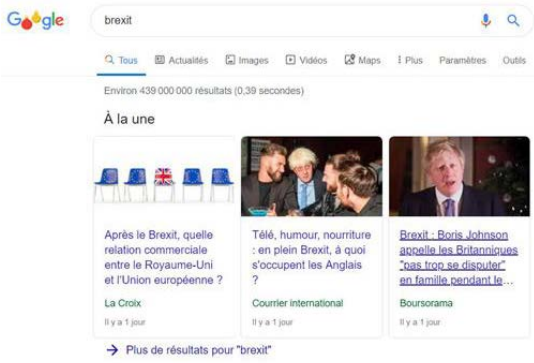
All'interno di *Google Search* ci sono funzioni finalizzate a soddisfare in modo specifico e mirato le ricerche relative ai fatti di attualità, si tratta in particolare:
- delle "notizie principali" ("*À la une*" nella versione francese) che assume la forma di

[5] "*Crawler*" è un termine generico che indica qualsiasi programma (come un robot o uno spider) utilizzato per l'individuazione e la scansione automatiche dei siti web, seguendo i link da una pagina web all'altra. Il *crawler* principale di Google è Googlebot che effettua due tipi di scansione del web: la *deep-crawl* (fatta una volta al mese circa) e la *fresh-crawl (*quasi tutti i giorni).

un carosello di risultati relativi agli avvenimenti di attualità, che possono essere scansionati orizzontalmente e visualizzati sopra i risultati della ricerca. Secondo il parere di Google, "il carosello" di solito visualizza il titolo dell'articolo e il nome dell'editore e spesso è accompagnato da un'immagine in miniatura e dall'indicazione del tempo trascorso dalla pubblicazione dell'articolo (9 ore fa, 20 min fa, etc.);

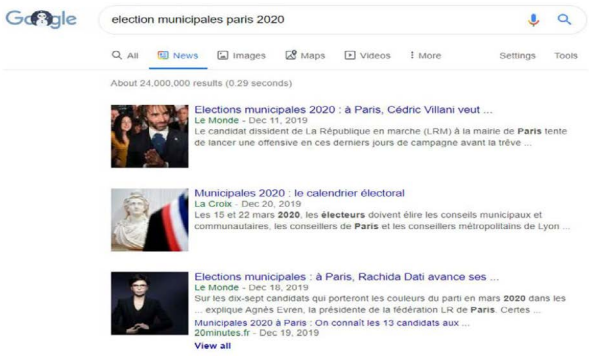
- la pagina delle "Notizie", si tratta di una sezione di ricerca a cui gli utenti possono

Capture d'écran – Google Search – Top Stories



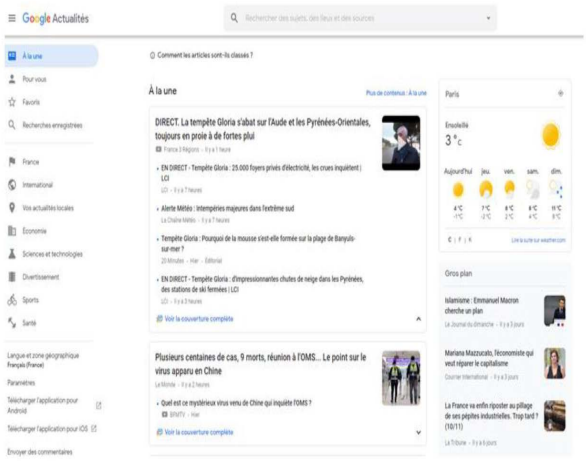
accedere dalla pagina dei risultati e che filtra i risultati per includere solo articoli relativi alle notizie collegate alle parole chiave che sono state inserite in *Google Search*. Tale scheda di solito visualizza il titolo dell'articolo e il nome dell'editore insieme a un'immagine in miniatura e un estratto dell'articolo.
Google offre quindi una vasta gamma di servizi agli utenti in aggiunta e in connessione

Capture d'écran - Google Search - Onglet News



al servizio principale di *Google Search*.
Google News, invece, è un servizio Google separato *Google Search* ed è interamente dedicato alle notizie.
Google News presenta i contenuti di notizie selezionate sulla sua *home page* in base alla lingua e alla regione in cui si trova l'utente.
La visualizzazione dei contenuti in *Google News* differisce da quella *Google Search*. I collegamenti ad articoli e contenuti di notizie sono presentati sotto forma di titolo, accompagnato dal nome dell'editore, un'indicazione relativa alla natura recente o meno del contenuto in questione e talvolta un'immagine in miniatura, generalmente senza

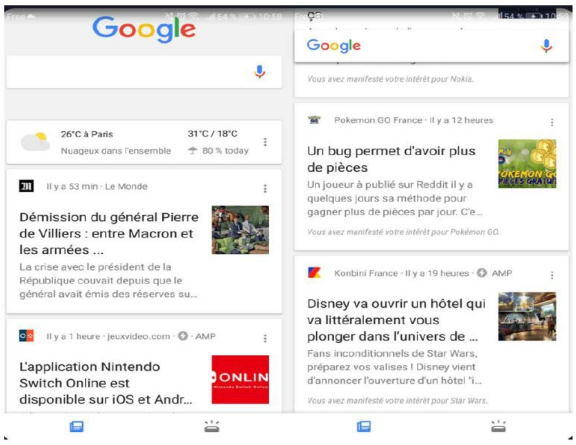
estratti testuali o "*snippet*".



Google Discover, infine, è un servizio collegato a *Google Search*, accessibile su un telefono cellulare o tablet, che presenta agli utenti, senza che questi abbiano effettuato una ricerca specifica, una selezione di contenuti in base alle interazioni con i prodotti Google, o addirittura a seconda delle tematiche che l'utente ha l'abitudine di seguire.
I risultati visualizzati da *Discover* sono principalmente sotto forma di immagini in miniatura, titoli della pagina, nomi delle testate editoriali o nomi a dominio e possibilmente frammenti o anteprime video animati, come mostrato nell'illustrazione seguente.

Durante la sua audizione, Google ha spiegato che il modo in cui gli editori potevano

Capture d'écran - Google Discover



scegliere di apparire o meno in questo servizio è cambiato alla fine del 2019: «Fino alla fine dell'anno scorso (2019), gli editori dovevano compilare un modulo per essere visualizzati in *Google News*. Ora gli editori possono disattivare *Google News* istruendo i robot» (Il termine "robot" si riferisce a *crawler* automatici utilizzati in particolare dai servizi di Google, che consentono la raccolta e l'indicizzazione delle risorse disponibili su Internet).
L'indicizzazione e la visualizzazione dei contenuti editoriali nei servizi di Google ven-

gono quindi effettuati dai crawler istituiti da Google ai quali gli editori possono dare istruzioni. Innanzitutto, è il Robot Exclusion Protocol (REP) che consente agli editori di concedere o negare parti dei loro siti ai *crawler* automatizzati. Successivamente, esistono dei Meta tag che forniscono istruzioni ai robot. Attraverso questi tag, gli editori possono, tra le altre cose, chiedere ai robot di indicizzare o meno le loro pagine web. Gli editori possono anche dare il loro consenso all'indicizzazione e alla visualizzazione dei loro contenuti, attraverso l'uso di strumenti specifici di Google che consentono di personalizzare la presentazione dei loro contenuti in *Google Search* e *Google News*. Infine, grazie al "Publisher Center", gli editori possono gestire la presentazione dei loro contenuti in *Google News*.
Per quanto riguarda le attività pubblicitarie, gli editori e le agenzie di stampa possono agire come venditori di spazi pubblicitari o come inserzionisti.

3. La posizione delle parti

I ricorrenti (gran parte del settore della stampa francese – quotidiana e periodica – nazionale, regionale e dipartimentale) lamentano la modifica della politica di visualizzazione dei contenuti delle notizie all'interno dei vari servizi di Google, in particolare *Google Search*, *Google News* e *Discover* in concomitanza con l'entrata in vigore della legge francese n. 2019-775 art. 4, adottata il 24 luglio 2019 che ha recepito l'art. 15 della direttiva 2019/790.
Si tratta, come anticipato, del riconoscimento di un diritto connesso a beneficio degli editori di giornali e agenzie di stampa che conferisce loro il diritto di autorizzare o vietare la riproduzione delle loro pubblicazioni su piattaforme, aggregatori e motori di ricerca. Un diritto connesso al pari di quelli riconosciuti dalla direttiva 2001/29/CE (Direttiva InfoSoc) che non è limitato alle sole parti testuali delle pubblicazioni ma copre altresì le fotografie e i video e prevede il diritto di ottenere una adeguata remunerazione per l'uso di tali contenuti (considerando 57[6] e 58[7] della direttiva) da parte di prestatori di servizi della società dell'informazione.
Dal 25 settembre 2019, in previsione dell'entrata in vigore della legge francese sul nuovo diritto connesso, Google ha annunciato agli editori e alle agenzie di stampa la nuova

[6] «I diritti concessi agli editori di giornali ai sensi della presente direttiva dovrebbero avere lo stesso ambito di applicazione dei diritti di riproduzione e di messa a disposizione del pubblico di cui alla direttiva 2001/29/CE relativamente agli utilizzi online da parte di prestatori di servizi della società dell'informazione. I diritti concessi agli editori di giornali non dovrebbero essere estesi ai collegamenti ipertestuali, né ai semplici fatti riportati nei giornali. I diritti concessi agli editori di giornali a norma della presente direttiva dovrebbero essere soggetti anche alle stesse disposizioni in materia di eccezioni e limitazioni applicabili ai diritti stabiliti dalla direttiva 2001/29/CE, tra cui l'eccezione in caso di citazioni, per esempio a fini di critica o di rassegna, di cui all'articolo 5, paragrafo 3, lettera d), di tale direttiva».

[7] «L'utilizzo di pubblicazioni di carattere giornalistico da parte di prestatori di servizi della società dell'informazione può consistere nell'utilizzo di intere pubblicazioni o di interi articoli, ma anche di parti di pubblicazioni di carattere giornalistico. Anche l'utilizzo di parti di pubblicazioni di carattere giornalistico ha acquisito una rilevanza economica. Al tempo stesso, l'utilizzo di singole parole o di estratti molto brevi di pubblicazioni di carattere giornalistico da parte di prestatori di servizi della società dell'informazione non compromette necessariamente gli investimenti effettuati dagli editori di pubblicazioni di carattere giornalistico nella produzione di contenuti. È pertanto opportuno prevedere

politica di visualizzazione dei contenuti all'interno dei suoi vari servizi.
In conformità con questo annuncio, Google ha implementato nuovi "tag", frammenti di codice che editori e agenzie di stampa possono inserire nel codice sorgente delle loro pagine web al fine di autorizzare Google a prendere estratti dai loro contenuti editoriali sotto forma di testi, immagini e video. Infine, lo stesso giorno, Google ha precisato che non intendeva remunerare gli editori per la ripresa dei loro contenuti editoriali.
I "nuovi" tag creati da Google che consentono agli editori di dare il proprio consenso si riferiscono solo a "estratti di testo", "immagini in miniatura" e video, ma non riguardano i titoli degli articoli[8].
Quindi Google ha continuato a mostrare i titoli degli articoli all'interno dei suoi vari servizi, senza ottenere l'accordo degli editori e agenzie di stampa interessati, o riconoscendo loro la giusta remunerazione.
Google ha ritenuto che i titoli cadessero in regime di esenzione. Non è tuttavia certo che i titoli degli articoli siano tutti coperti in linea di principio da questa eccezione, poiché il testo si riferisce a parole isolate o estratti molto brevi di pubblicazioni di carattere giornalistico e ciò induce ad una valutazione caso per caso, soprattutto avuto riguardo al contenuto informativo dei titoli degli articoli di stampa e senza dimenticare che il titolo di sé può avere una connotazione creativa e, quindi, ricadere in un regime di protezione autorale. La funzione specifica dei titoli è stata oltretutto riconosciuta dallo stesso Google che ha dichiarato: «*L'utilité d'un snippet varie en fonction de l'origine du contenu et de la nature de l'information. Par exemple, dans le cas d'une recette de cocktail, le snippet peut être utile pour permettre à l'utilisateur de savoir sur quel lien il veut cliquer. En revanche, les contenus d'actualité sont produits par des journalistes professionnels et les titres sont rédigés avec une grande attention pour attirer l'intérêt des utilisateurs et les inciter à cliquer pour aller lire l'article. Dès lors, pour les contenus d'actualité, les snippets ne sont pas en général aussi utile que pour d'autres contenus. En outre, lorsqu'il n'y a pas de snippets, nous pouvons faire apparaître plus de résultats sur une page*» (PV d'audition de Google, cote 4 424).
Google sostiene che, in virtù del principio di neutralità non paga mai per indicizzare i contenuti. A suo parere gli *snippet* remunerativi sarebbero incompatibili con il funzionamento di un motore di ricerca. Google ritiene inoltre che la decisione di chiedere il consenso degli editori per la ripresa degli estratti di testo senza alcun riconoscimento economico non sia un'attività vietata, tenuto conto del contenuto delle nuove disposizioni e delle incertezze interpretative afferenti il testo normativo. Si tratta, quindi, a suo giudizio di una decisione "naturale, prudente e ragionevole". Infine, la decisione del *Bundeskartellamt* nel 2015 riguardo al legittimo rifiuto da parte di Google a riconoscere in favore degli editori una tutela autorale rispetto allo sfruttamento di frammenti dei

che l'utilizzo di singole parole o di estratti molto brevi di pubblicazioni di carattere giornalistico non rientri nell'ambito dei diritti previsti dalla presente direttiva. Tenuto conto della forte aggregazione e dell'utilizzo di pubblicazioni di carattere giornalistico da parte di prestatori di servizi della società dell'informazione, è importante che l'esclusione degli estratti molto brevi sia interpretata in modo da non pregiudicare l'efficacia dei diritti previsti dalla presente direttiva».

[8] Nel servizio di *Google Search*, i link agli articoli giornalistici vengono visualizzati utilizzando tutti o parte dei titoli degli articoli corrispondenti. In *Google News* e *Discover* i collegamenti agli articoli mostrano il titolo dell'articolo (possibilmente accompagnato da un'immagine in miniatura, anche estratti di testo e video nel caso di *Discover*).

loro contenuti costituirebbe, a suo parere, un valido precedente[9].

4. La decisione dell'*authority*

A parere *Autorité de la concurrence* la legge n. 2019-775 non esclude (almeno in linea di principio) la possibilità per un editore di concedere ai prestatori di servizi della società dell'informazione una licenza gratuita per lo sfruttamento dei propri contenuti. Tuttavia, il rifiuto generalizzato di Google rispetto alla remunerazione per l'uso di tali contenuti rappresenta in via cautelare un abuso di posizione dominante sul mercato dei servizi di ricerca generalisti[10], anche se di per sé non costituisce una violazione della legge sul nuovo diritto connesso.

Analogamente, la scelta di Google di includere sistematicamente, senza distinzioni, i titoli degli articoli nel regime di esenzione previsto dall'art. 15 della direttiva è stato ritenuto, a dispetto della rappresentazione offerta dal motore di ricerca, una decisione per nulla "naturale", né "cauta" e neppure "ragionevole".

Al contrario, un comportamento "naturale, prudente e ragionevole", sempre secondo l'opinione dell'antitrust francese, per un operatore dominante come Google, sarebbe potuto consistere nell'avviare i negoziati con gli editori e le agenzie di stampa, atteggiamento che avrebbe consentito a Google di rispettare la volontà del legislatore, proteggendo nel contempo i propri interessi.

Il rifiuto da parte di Google di remunerare gli editori ha avuto un forte impatto nella visualizzazione dei siti internet degli editori e delle agenzie di stampa, che, in caso di rifiuto a concedere licenze gratuite, hanno subito una perdita di traffico e un deterioramento del loro posizionamento nei servizi di ricerca offerti dal portale. Senza dimenticare che la nuova politica di visualizzazione adottata da Google ha imposto agli operatori del settore condizioni di transazione più sfavorevoli. Il perimetro delle licenze gratuite concesse a Google è difatti risultato essere molto più ampio rispetto ad una situazione che sarebbe derivata da una negoziazione. Gli editori che hanno concesso la

[9] Le indagini svolte dal *Bundeskartellamt* hanno fatto seguito ad una denuncia da parte di VG Media nei confronti Google in relazione al riconoscimento di un diritto connesso per gli editori di giornali on line a decorrere dal 1 ° agosto 2013. Tale diritto consente agli editori di vietare ai motori di ricerca di utilizzare gli articoli o altri contenuti, ad eccezione di singole parole o minuscoli testi (frammenti). Nell'estate del 2014, VG Media ha intrapreso un'azione civile contro Google. Di conseguenza, Google ha annunciato che, al fine di evitare contestazioni sullo sfruttamento illeciti di contenuti autorali, avrebbe mostrato i risultati di ricerca relativi ai siti web degli editori di stampa che erano rappresentati da VG Media nella solo in forma ridotta se gli editori non avessero accettato un uso gratuito dei loro contributi.

Il *Bundeskartellamt* ha ritenuto tale decisione legittima considerato che anche una società dominante non può essere costretta in base al diritto della concorrenza ad assumersi un considerevole rischio di contestazione laddove la situazione legale non fosse chiara. Il *Bundeskartellamt* ha quindi deciso di non avviare procedimenti formali contro Google per eventuali discriminazioni nei confronti di VG Media.

[10] Il mercato francese delle ricerche generaliste oscillerebbe a beneficio di Google in una quota pari al 90% del mercato delle ricerche on line. Le prove mostrano che, indipendentemente dall'indicatore utilizzato per valutare la sua quota di mercato, Google ha una grande maggioranza del mercato dei servizi di ricerca generali. In particolare, la sua quota di mercato è di circa il 90% alla fine del 2019 rispetto al 5% del suo principale concorrente Microsoft che utilizza il motore di ricerca Bing.

licenza gratuita (per volontà o necessità) si sono trovati a concedere diritti ben più ampi rispetto a quelli concessi prima dell'entrata in vigore della legge n. 2019-775.
Non solo le pratiche adottate da Google sono risultate dannose per gli editori e le agenzie di stampa ma hanno privato la legge sul nuovo diritto connesso degli effetti previsti. La direttiva (UE) 2019/790 del 17 aprile 2019 sul diritto d'autore e sui diritti connessi nel mercato unico digitale mira infatti a stabilire le condizioni per una negoziazione equilibrata tra editori, agenzie di stampa e servizi di comunicazione al pubblico online, al fine di ridefinire la condivisione di valore tra questi attori e a favore di editori e agenzie di stampa.
L'autorità ha inoltre ritenuto non pertinente al caso concreto il richiamo da parte di Google alla decisione del *Bundeskartellamt* del 2015 (*Bundeskartellamt,* 6th Decision Division, B6-126/14, *Google Inc. vs. Third Parties*, 8 September 2015). Secondo l'antitrust francese si tratterebbe di una circostanza irrilevante rispetto al caso di specie. Come indica il *Bundeskartellamt* nella propria decisione, il caso tedesco rientra in uno specifico contesto giuridico e fattuale che non può costituire un precedente per valutare la natura anticoncorrenziale delle pratiche attuate da Google in un altro contesto.
Il *Bundeskartellamt* si preoccupa inoltre di specificare nella sua decisione che la sua valutazione potrebbe essere diversa in caso di modifica della legge tedesca sui diritti connessi. Le pratiche adottate da Google sono dunque intervenute in un diverso quadro legislativo in seguito all'adozione della direttiva e al suo recepimento nel diritto francese.
Le scelte operate da Google, oltre ad aver ripercussioni negative per editori e agenzie di stampa, inequivocabilmente comportano un deterioramento della qualità delle informazioni, in quanto la mancanza di risorse sufficienti a supportare i costi ha inevitabili riflessi sulla qualità del servizio informativo reso. In tal modo viene minato il rilevante contributo che gli editori forniscono al dibattito pubblico e al corretto funzionamento di una società democratica, la sostenibilità che il legislatore intendeva garantire. Ciò si riflette non solo nelle disposizioni della legge francese ma anche negli obiettivi perseguiti dalla direttiva; il considerando 54 della direttiva sottolinea che la stampa fornisce un contributo fondamentale al dibattito pubblico e al corretto funzionamento di una società democratica («Una stampa libera e pluralista è essenziale per garantire un giornalismo di qualità e l'accesso dei cittadini all'informazione e dà un contributo fondamentale al dibattito pubblico e al corretto funzionamento di una società democratica»). Il pluralismo dei quotidiani di informazione politica e di informazione generale è di per sé un valore che va tutelato.
D'altro canto, queste pratiche sono in grado di produrre effetti distorsivi della concorrenza sul mercato dei servizi di ricerca generali posizionando i concorrenti di Google, in particolare quelli con una piccola quota di mercato e che riconoscono agli editori un congruo compenso per la visualizzazione dei loro contenuti, in una situazione di asimmetria rispetto a Google.
Le pratiche denunciate creano pertanto un grave attacco al settore della stampa in quanto minacciano la redditività degli editori e delle agenzie di stampa a maggior ragione considerato che è lo stesso legislatore(francese) ad aver sottolineato che il nuovo diritto connesso è una fonte di reddito vitale per il settore. A parere dell'Autorità si

tratta di una violazione molto più grave rispetto all'uso fatto da Google nei suoi vari servizi, in particolare in *Google Search*, dei contenuti protetti.
Secondo l'opinione espressa da Google, gli editori non sono mai stati pagati per la visualizzazione di contenuti protetti all'interno dei servizi dalla medesima offerti e la scelta della maggior parte di essi di continuare ad autorizzare la ripresa e la visualizzazione di tali contenuti significa che per tali soggetti non si è verificato nessun cambiamento sostanziale. Google ritiene che non vi sarebbe alcun legame tra la modifica delle condizioni per la ripresa e la visualizzazione di contenuti protetti nei suoi vari servizi e la crisi economica che sta affrontando il settore della stampa, oltretutto preesistente al momento dell'adozione della direttiva e della legge di recepimento francese.
Argomentazioni che, a parere dell'Autorità, non sono state ritenute convincenti anzi si è ritenuto che le scelte operate da Google abbiano addirittura aggravato la situazione di tale settore, ragion per cui l'Autorità ha ritenuto di dover adottare misure urgenti di protezione dopo aver riconosciuto l'esistenza del nesso causale tra le pratiche denunciate e l'attacco al settore stampa.
Da un lato, va notato che l'adozione da parte del Parlamento francese della legge sui diritti connessi costituisce un fatto nuovo che dovrebbe condurre, secondo la volontà del legislatore, a riequilibrare la distribuzione della catena del valore tra servizi comunicazione al pubblico online - come *Google Search* - e gli editori e agenzie di stampa, compresa la remunerazione ai giornalisti per la parte di loro spettanza.
Rispetto alle misure conservative, Google ritiene che le richieste dei ricorrenti sarebbero di natura tale da trasformare un diritto di proprietà intellettuale, limitato a un diritto esclusivo sui contenuti, in una possibilità per il titolare del diritto di imporre ad altre società l'obbligo di acquistare questo diritto. Non solo un tale obbligo di acquisto sarebbe, sempre a parere del noto motore di ricerca, in contraddizione con la legge sulla proprietà intellettuale e i principi del libero mercato, ma sarebbe anche incompatibile con la posizione di Google che non sta chiedendo di acquistare gli *snippets*.
L'Autorità, come anticipato, ha ritenuto necessario adottare, in attesa della decisione sul merito, garanzie relative all'equità delle condizioni di transazione tra Google, gli editori e le agenzie di stampa in merito ai diritti connessi.
Contrariamente a quanto indicato da Google, sia nelle sue osservazioni sia durante la discussione, queste misure sono risultate necessarie e proporzionate alla gravità delle pratiche commesse, capaci quindi di garantire condizioni eque e volte a preservare l'efficacia della legge sui diritti connessi.
Tali misure non implicano l'inserimento di Google in una situazione di obbligo di acquisto di alcun contenuto, ma si limitano a consentire un'equa condivisione delle entrate generate dai contenuti e solo con editori e agenzie di stampa le cui richieste soddisfano i criteri stabiliti dalla legge sui diritti connessi.
Dette misure precauzionali non escludono che determinati contenuti possano essere forniti gratuitamente a Google da editori e agenzie di stampa. Ciò può accadere quando l'editore o l'agenzia di stampa desidera concedere a Google una licenza gratuita o quando i criteri stabiliti dalla legge n. 2019-775 non giustifichino il pagamento della remunerazione.
Google è obbligato a negoziare in buona fede con gli editori e le agenzie di stampa o

le organizzazioni di gestione collettiva la remunerazione ad essi dovuta per la ripresa di contenuti protetti secondo criteri trasparenti, obiettivi e non discriminatori. L'implementazione di questa ingiunzione deve coprire tutti i servizi offerti da Google, in particolare il servizio di ricerca offerto da *Google Search*.
I negoziati relativi a questa ingiunzione riguarderanno, in modo retroattivo, il periodo a partire dall'entrata in vigore della legge 2019-775, ovvero il 24 ottobre 2019.
Si è dunque imposto al motore di ricerca, con un provvedimento cautelare e urgente, di negoziare con gli editori la corresponsione di un equo compenso per l'utilizzazione da parte degli utenti di Google dei contenuti dei giornali on-line.
Al fine di garantire le finalità perseguite da tale ingiunzione, Google dovrà comunicare agli editori e alle agenzie di stampa le informazioni necessarie per una valutazione trasparente della remunerazione ad essi spettante.
Per quanto riguarda gli editori e le agenzie di stampa che a partire dal 24 ottobre 2019 non hanno concesso l'autorizzazione a riprendere i propri contenuti e che hanno chiesto a Google di negoziare, Google durante il periodo di negoziazione non potrà opporsi alla visualizzazione dei loro contenuti secondo le modalità scelte da questi editori e agenzie di stampa.
Google dovrà condurre le trattative per un periodo di tre mesi decorrenti dalla richiesta di apertura di una negoziazione da parte di un editore, un'agenzia di stampa o un organo di gestione collettiva. Questa apertura sarà materializzata dalla data di ricezione di una richiesta a mezzo lettera raccomandata con richiesta di ricevuta di ritorno.
Google è stata esortata ad adottare le misure necessarie per garantire che i negoziati previsti dalle ingiunzioni non incidano sulle altre relazioni economiche esistenti tra Google, gli editori e le agenzie di stampa.
Al fine di controllare l'attuazione delle ingiunzioni, fatta salva in particolare la buona fede di Google nello svolgimento delle negoziazioni, si è ritenuto necessario adottare un meccanismo per monitorare l'osservanza delle ingiunzioni inferte al motore di ricerca. Google dovrà quindi fornire all'Autorità relazioni periodiche sul rispetto della decisione adottata dall'Autorità.
Considerata la natura potenzialmente anticoncorrenziale delle pratiche denunciate e il danno grave e immediato che è stato arrecato al settore della stampa, l'Autorità ha ritenuto necessario mantenere in vigore le predette ingiunzioni fino alla pubblicazione della decisione di merito. Quindi, fino all'esito della chiusura del procedimento, gli editori dovranno ricevere una remunerazione per tutti gli atti di riproduzione dei loro contenuti compiuti dal noto motore di ricerca.

Commenti

Il potere senza responsabilità dei social media nelle campagne elettorali*

Giuseppe Donato

Sommario

1. Il potere dei *social media*: controllo sugli utenti e sugli attori politici. – 2. La responsabilità dei *social media* tra disinformazione e *facilitation* dei contenuti. – 3. Le prospettive di regolamentazione.

Keywords

fake news – libertà di espressione – disinformazione – social media – propaganda

1. Il potere dei *social media:* controllo sugli utenti e sugli attori politici

La rivoluzione tecnologica permanente che ha riscritto le regole della società sotto innumerevoli profili individuali e relazionali ha portato con sé delle nuove sfide rispetto alle quali il diritto – come fenomeno sociale ontologicamente deputato alla tutela delle esigenze della collettività – non sempre ha saputo fornire adeguate risposte. La creazione di uno spazio virtuale senza confini, liberamente accessibile da chiunque, ha originato un nuovo centro di aggregazione di interessi che supera e rompe il modello statuale classico caratterizzato da territorio, popolo e sovranità.

Questo nuovo spazio giuridico, difatti, data la sua natura immateriale, è restio ad essere circoscritto entro i confini nazionali, così come i suoi fruitori non necessitano di alcun riconoscimento di uno *status* di cittadino. Ancor più dirompenti appaiono i riflessi sul piano dell'allocazione della sovranità, specialmente a fronte di una crescente funzione para-pubblicistica svolta dai giganti tecnologici: si manifesta, pertanto, la necessità di individuare adeguate forme di responsabilità, tanto per le azioni che sono ad essi immediatamente riconducibili, quanto per le attività che tramite le loro piattaforme vengono realizzate dai singoli utenti.

Proprio su questo punto di incontro e di scontro fra il vecchio mondo analogico ed il nuovo mondo digitale si attesta la questione dell'influenza dei *social media* sui processi elettorali e, ancor prima, del potere che viene da (o tramite) essi esercitato tanto sui singoli utenti quanto sugli attori politici.

Sotto il primo profilo vanno anzitutto richiamati alcuni dati socio-economici emblematici del ruolo assunto dai *social* nella considerazione dell'opinione pubblica: difatti, anche se oltre la metà degli italiani (59,1%) continua a utilizzare i telegiornali come fon-

te di informazione, il solo Facebook viene utilizzato per questo fine da più di un terzo del campione (31,4%)[1]. L'affidamento riposto dagli utenti nella piattaforma, unito alle basse percentuali di lettori di quotidiani cartacei (17,5%) o online (11,4%), è sintomatico di una società che rigetta in maniera sempre più vistosa i corpi intermedi, siano essi organi di informazione o partiti politici[2].

La tesi che raffigura una cornice favorevole alla fruizione delle informazioni acquisite a mezzo *social* viene ulteriormente suffragata dall'analisi di tre rilevanti elementi: *political advertising*, *micro-targeting*, *social media algorithms*.

La piattaforma di Facebook si è dimostrata un terreno particolarmente appetibile per le pubblicità di stampo politico: secondo il report fornito dall'azienda californiana, nel periodo che intercorre fra marzo e settembre 2019 – e che comprende, quindi, la campagna elettorale per il rinnovo del Parlamento europeo – in Italia sono state acquistate oltre 41.000 pubblicità per una spesa complessiva superiore ai 3 milioni di euro (solo in Germania e Spagna, fra i 27 membri dell'Unione Europea, si è speso di più)[3].

L'efficacia del massiccio investimento su contenuti pubblicitari viene amplificata dal ricorso ad avanzate tecniche di profilazione dell'utente nella sua veste di elettore. In maniera speculare alla progressiva assimilazione tra la presentazione dell'offerta politica e la commercializzazione di un nuovo prodotto, infatti, si registra una sovrapposizione fra elettore e consumatore[4]: le tracce che l'utente lascia in rete sui suoi gusti e le sue preferenze consentono all'inserzionista politico di indirizzargli un contenuto costruito *ad hoc* che, data la sua specificità, gode di maggiori possibilità di essere accolto dall'utente rispetto ad un messaggio generico destinato alla massa indistinta del corpo elettorale.

La capacità di penetrazione delle nuove modalità di proselitismo elettorale viene, infine, ulteriormente rafforzata dagli algoritmi che regolano i *social network*. L'obiettivo delle piattaforme è quello di trattenere gli utenti il più a lungo possibile su di esse, così da potergli offrire un maggior numero di contenuti sponsorizzati e, in un circolo di mutua alimentazione, da poter acquisire il maggior numero di dati. A tal fine l'algoritmo cerca di offrire un'esperienza *web* personalizzata nella quale l'utente possa trovare un ambiente confortevole: si realizza così l'effetto delle *echo chambers*, in cui all'utente viene offerta una continua conferma delle sue opinioni pregresse, portandolo ad assumere posizioni sempre più radicalizzate e meno aperte al confronto[5].

Acclarata la capacità di influenza dei *social* sulle modalità di formazione del convinci-

---

* Il presente contributo rappresenta una rielaborazione della relazione svolta in occasione del Convegno organizzato da ICON-S Italian Chapter su "Le nuove tecnologie e il futuro del diritto pubblico" (Firenze, 22-23 novembre 2019) all'interno del panel n. 5 intitolato "Potere senza responsabilità nella "democrazia" dei social media", presieduto dal Prof. A. Saitta.

1 I dati sono tratti dal 16° Rapporto Censis sulla comunicazione "I media e la costruzione dell'identità".

2 Sembra calzante, a tal proposito, l'analisi condotta da A. Baricco, *The game*, Torino, 2018, 77 sulla distruzione delle élite: «In un ambito che è largamente sopravvalutato, cioè la politica, l'attuale inclinazione degli elettori per una qualche forma di leaderismo populista che tende a saltare la mediazione dei partiti tradizionali, e in fondo anche dei ragionamenti, può dare un'idea particolarmente chiara del fenomeno».

3 I dati sono tratti dal "Facebook report on the implementation of the Code of Practice for Disinformation. Annual Report. 2019", sul quale v. *amplius infra*.

4 Su tale problema v. L. Califano, *Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network*, in *federalismi.it*, 16, 2019, spec. 4 ss.

5 Sui crescenti rischi di una *bubble democracy* v. G. Pitruzzella, *La libertà di informazione nell'era di Internet*,

mento dell'elettore, non meno problematica si prospetta l'analisi del potere che tali piattaforme possono esercitare sull'attività online dei gruppi politici.
La questione è affiorata con tutte le sue criticità a seguito dell'oscuramento, da parte di Facebook, delle pagine ricollegate a CasaPound Italia e a Forza Nuova e dei relativi amministratori[6]: a detta della società tecnologica, infatti, i soggetti coinvolti avrebbero violato le Condizioni d'Uso e gli Standard della Community nella parte in cui vietano espressamente le organizzazioni che incitano all'odio[7].
La mancanza di un chiaro quadro normativo di riferimento – non solo a livello sostanziale, ma anche sul piano processuale[8] – ha fatto emergere la contrapposizione fra le due tesi che si contendono il campo, come dimostrano gli esiti opposti dei ricorsi ex art. 700 c.p.c. presentati dai due gruppi politici.
Nell'ordinanza di accoglimento del ricorso di CasaPound il giudice ha sposato la tesi para-pubblicistica, evidenziando il ruolo assunto da Facebook «con riferimento all'attuazione di principi cardine essenziali dell'ordinamento come quello del pluralismo dei partiti politici (art. 49 Cost.), al punto che il soggetto che non è presente su F. è di fatto escluso (o fortemente limitato) dal dibattito politico italiano»[9].
La valorizzazione dei profili privatistici, invece, ha portato al rigetto del ricorso presentato da Forza Nuova, dal momento che, «pur svolgendo un'attività di indubbio rilievo sociale»[10], Facebook rimane un soggetto privato, onde per cui «il rapporto tra le parti in causa è regolato, oltre che dalla legge, anche dalle condizioni contrattuali alle quali la parte aderisce quando chiede di iscriversi al social network»[11].
L'oscillazione fra le due teorie antitetiche comporta evidenti riflessi sul versante della configurazione della responsabilità dei *social* in merito ai loro interventi *lato sensu* di censura.
Se si accogliesse la prospettiva privatistica, allora la suddetta attività delle piattaforme potrebbe essere contestata solo sotto il profilo della responsabilità da inadempimento, peraltro di difficile accertamento davanti ad una violazione, da parte dell'utente, delle condizioni contrattuali. Se si accentuasse il piano para-pubblicistico del servizio offer-

in *questa Rivista*, 1, 2018, spec. 41 ss. Gli effetti distorsivi prodotti dall'algoritmo di Facebook, quali «l'effetto gregge, il conformismo e le cascate informazionali» sono affrontati da G. Origgi, *La democrazia può sopravvivere a Facebook? Egualitarismo epistemico, vulnerabilità cognitiva e nuove tecnologie*, in *Ragion Pratica*, 51, 2018, 452.

[6] Le due vicende processuali sono analizzate da P. Zicchittu, *I movimenti "antisistema" nell'agorà digitale: alcune tendenze recenti*, in *giurcost.org.*, 2020.

[7] In particolare al punto I.2 e al punto III.13 degli Standard.

[8] Sembra emblematico, a tal proposito, il fatto che, nonostante i due procedimenti presentassero caratteri omogenei, il ricorso presentato da CasaPound è stato incardinato presso la Sezione specializzata in materia di impresa del Tribunale di Roma, mentre quello depositato da Forza Nuova è stato trattato da una diversa sezione (diritti della persona e immigrazione civile) della medesima autorità giudiziaria.

[9] Trib. Roma, ord. 12 dicembre 2019, § 3 delle motivazioni.

[10] Trib. Roma, ord. del 23/02/2020, § 2 delle ragioni in diritto.

[11] Il giudice arriva alla conclusione per cui, sulla scorta di fonti internazionali e sovranazionali, grava su Facebook un obbligo di controllo sui contenuti veicolati tramite la propria piattaforma che possano rappresentare fenomeni di *hate speech*. Sul tema, che in parte esula dalle finalità del presente intervento, si rinvia al Codice di condotta per lottare contro le forme illegali di incitamento all'odio *online* approntato dalla Commissione Europea nel 2016 e sottoscritto, fra gli altri, anche da Facebook.

to dai *social network*, invece, i rimedi di diritto comune paleserebbero la loro inadeguatezza: si assisterebbe ad una rottura della dicotomia fra potere e responsabilità, atteso che, nell'attuale contesto, Facebook (al pari degli altri *social*) opera come "*judge, jury and executioner*" senza neppure dover rispettare dei basilari principi processuali come quelli della previa contestazione dell'addebito e della tutela del contraddittorio.

2. La responsabilità dei *social media* tra disinformazione e *facilitation* dei contenuti

Lo snodo fondamentale del rapporto che lega le piattaforme *social* alle competizioni elettorali è plasticamente rappresentato dalla dilagante problematica della disinformazione *online*. La questione è rimasta a lungo sottotraccia, fino ad affacciarsi con vigore all'attenzione del dibattito politico solo a seguito del verificarsi di eventi dalla portata macroscopica quali la Brexit e l'affermazione di movimenti populistici.
La risposta sul piano giuridico si è registrata principalmente sul piano sovranazionale, come dimostra il grande numero di fonti che hanno cercato di tracciare i confini del problema o di avanzare dei rimedi alla sua diffusione.
In una prima Comunicazione[12] la Commissione Europea, dopo aver evidenziato l'incapacità dei *social network* di reagire all'«uso manipolativo delle loro infrastrutture» a fini disinformativi[13], ha individuato nella promozione della trasparenza, diversità e credibilità dell'informazione i possibili rimedi, adeguatamente suffragati da strumenti tecnici quali un vaglio più attento delle pubblicità a carattere politico e una completa identificazione degli inserzionisti.
Le aspettative della Commissione, ulteriormente ribadite in una successiva Raccomandazione[14] rivolta agli Stati membri e ai partiti politici, hanno trovato riscontro nell'adozione di un Codice di buone pratiche[15] – firmato dalle principali compagnie tecnologiche[16] – tramite il quale, seppur nella forma della *soft regulation*, l'Unione Europea ha cercato di regolamentare i doveri delle società firmatarie. Oltre ad una generica enunciazione di scopi, fra i quali si annovera anche quello di «permettere agli utenti di capire perché sono stati oggetto di un determinato messaggio pubblicitario di natura politica o di sensibilizzazione»[17], il Codice prevede numerosi impegni per i firmatari, come quelli di rendere le inserzioni pubblicitarie «chiaramente distinguibili dai conte-

[12] 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, del 26 aprile 2018.

[13] «Per disinformazione si intende un'informazione rivelatasi falsa o fuorviante concepita, presentata e diffusa a scopo di lucro o per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico», ivi, 4.

[14] *Commission Reccomendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament,* del 12 settembre 2018.

[15] Codice di buone pratiche dell'UE sulla disinformazione, del 26 settembre 2018

[16] È stato sottoscritto da Facebook, Google, Microsoft, Mozilla, Twitter.

[17] Punto I, VIII del Codice.

nuti editoriali, ivi comprese le notizie, indipendentemente dalla loro forma e dal supporto utilizzato»[18], di fornire l'indicazione dei promotori e degli importi versati per i contenuti sponsorizzati[19], di «aiutare le persone a prendere decisioni informate quando incappano in notizie online che potrebbero essere false, anche sostenendo gli sforzi intesi a sviluppare e attuare indicatori efficaci di affidabilità in collaborazione con l'ecosistema delle notizie»[20].

Pur rappresentando un importante progresso verso una completa regolamentazione della materia e, in modo specifico, dei compiti che le piattaforme *social* devono assolvere[21], nondimeno il Codice manifesta in maniera evidente i suoi limiti nella misura in cui lascia irrisolto il profilo della responsabilità dei social davanti alla propagazione della disinformazione.

Su questo fronte appare rilevante un recente studio richiesto dalla Commissione LIBE[22] del Parlamento europeo su disinformazione e propaganda[23]. Il documento traccia, anzitutto, una definizione degli operatori tecnologici coinvolti, proponendo di utilizzare il termine *platform providers* per identificare «*those services that convey third-party content with value added services*»[24], rispetto ai quali i *social media* sono soltanto una *species* del più ampio *genus*.

Il dibattito sulla responsabilità di questi soggetti dovrebbe essere risolto, secondo lo studio, in base al principio per cui non possono essere chiamati a rispondere per i contenuti creati dai loro utenti[25], sulla scorta di una responsabilità da posizione, ma solo per le attività di amministrazione su di essi, come quelle esemplificate nel Codice di buone pratiche. Questa peculiare gestione dei contenuti di creazione altrui suggerisce di superare la dicotomia fra «*editorial responsibility*» e «*mediators' distributory responsibility*» in favore di una categoria intermedia identificata nella «*facilitation*»[26] dei contenuti: un'attività che, senza fermarsi al livello di mera intermediazione, non raggiunge comunque la pervasività di un controllo editoriale.

3. Le prospettive di regolamentazione

L'intreccio fra competizioni elettorali e *social media* si inerpica, come si è cercato brevemente di dimostrare, su terreni impervi: *hate speech*, strumenti di disinformazione, abuso di inserzioni pubblicitarie a carattere politico. Il valore primario degli interessi

[18] Punto II.B, 2 del Codice.

[19] Punto II.B, 3 del Codice.

[20] Punto II.D, 7 del Codice.

[21] Si segnala, fra l'altro, che il Codice introduce per i firmatari l'obbligo di pubblicare un report annuale sulle azioni intraprese nella lotta alla disinformazione. I report sono consultabili all'indirizzo *ec.europa.eu*.

[22] Commissione per le libertà civili, la giustizia e gli affari interni.

[23] *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, 2019.

[24] Ivi, 80.

[25] Come, ad esempio, i post di Forza Nuova nel caso sopra esaminato.

[26] *Disinformation and propaganda*, cit., 87.

coinvolti – su tutti, libertà di espressione e pluralismo politico – richiede un preciso intervento di regolamentazione, rispetto al quale gli attori pubblici e privati, pur concordi sotto il profilo dell'*an*, non sono riusciti a trovare una soluzione condivisibile sul *quomodo*. Si delineano, quindi, diverse possibili modalità di azione.

Una prima ipotesi è rappresentata dall'affidamento del compito all'autoregolamentazione delle società tecnologiche, le quali, in assenza di rigidi vincoli legislativi, potrebbero approntare soluzioni veloci ed efficaci di fronte ad un uso distorto delle proprie piattaforme. D'altro canto, il profilo strettamente tecnico non può essere considerato in maniera del tutto avulsa da quello del merito: seguendo tale strada si aprirebbero ampi spazi all'arbitrarietà dei *social media* sui contenuti cui dare accesso, con evidenti conseguenze sul rischio che il suddetto controllo possa essere guidato da interessi di parte[27].

Si potrebbe avanzare, quindi, la prospettiva di una regolazione dal lato pubblico, sul piano nazionale o sovranazionale. L'emanazione di una legislazione statale consentirebbe di affrontare in modo consono al complessivo quadro istituzionale quelle situazioni che, per la loro peculiarità, non sono suscettibili di regolazione secondo canoni generici: si pensi, nel contesto italiano, ai citati casi che hanno interessato l'attività di gruppi di ispirazione neofascista, attività che non può che essere analizzata alla luce del mosaico normativo composto (come minimo) dagli artt. 21, 49 e XII disp. fin.[28] della Costituzione. Gli strumenti di legislazione nazionale, però, pur potendo delimitare in maniera apprezzabile gli obblighi di intervento dei *social* nella lotta alla disinformazione[29], rischiano di rivelarsi inefficaci, sia perché non possono spiegare effetti al di fuori del territorio statale (a fronte della natura intrinsecamente aterritoriale delle piattaforme) sia per le misure predisposte nel caso di inottemperanza delle prescrizioni. Difatti, le sanzioni previste in Germania – fino a 50 milioni secondo il NetzDG – o in Italia – dove Facebook è stata destinataria di un'ingiunzione del Garante per la protezione dei dati personali per una somma pari a 1 milione di euro per il caso Cambridge Analytica e per il prodotto "Candidati"[30] – appaiono del tutto inadeguate a svolgere un effetto deterrente verso dei soggetti che godono di un'ingente disponibilità economica.

Alcune delle criticità riscontrabili sul livello nazionale della legislazione possono essere superate da un approccio di tipo sovranazionale: l'adozione di uno strumento quale

---

[27] Il rischio è ben rappresentato in *Disinformation and propaganda,* cit., spec. 87, dove si sconsiglia l'opzione di affidare ai *platform providers* la possibilità di controllare i contenuti o di deciderne la natura, non potendosi escludere che «*at any time, a competing platform could emerge that would – either openly or covertly – represent a particular ideology*».

[28] Nel dibattito che di recente ha animato la dottrina su quest'ultima norma v., *ex multis*, B. Pezzini, *Il divieto di ricostituzione del partito fascista nella XII disposizione finale*, in M. D'Amico – A. De Francesco – C Siccardi (a cura di), *L'Italia ai tempi del ventennio fascista. A ottant'anni dalle leggi ebraiche: tra storia e diritto*, Milano, 2019, 205 ss. e G.E. Vigevani, *Origine e attualità del dibattito sulla XII disposizione finale della Costituzione: i limiti della tutela della democrazia*, in *questa Rivista*, 1, 2019, 25 ss.

[29] La legge tedesca "*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*" prescrive un obbligo di rimozione dei contenuti manifestamente illegali in un termine di 24 ore o di 7 giorni a seconda dei casi. Per un commento della legge v. V. Claussen, *Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation*, in *questa Rivista*, 3, 2018, 110 ss.

[30] Cfr. ordinanza ingiunzione nei confronti di Facebook Ireland Ltd e Facebook Italy s.r.l. del 14 giugno 2019.

un regolamento europeo sulla lotta alla disinformazione online, ad esempio, assicurerebbe una disciplina uniforme su tutto il territorio dell'Unione, segnando un passo in avanti nella tutela della vita digitale dei cittadini europei ulteriore rispetto a quanto già realizzato con l'adozione del GDPR. Proprio quest'ultimo testo dimostra, inoltre, la capacità delle istituzioni europee di adottare strumenti efficaci anche nei confronti dei colossi tecnologici, come conferma la previsione di sanzioni pecuniarie fino a 10 o 20 milioni di euro o, per le imprese, fino al 2% o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[31]. Peraltro, nemmeno la prospettiva sovranazionale appare esente da rischi di inefficacia dal punto di vista tecnico, atteso che l'opera di delimitazione della responsabilità dei *social media* «*requires technological knowledge from the side of the legislator*»[32].

I requisiti necessari per una regolamentazione funzionale, pertanto, appaiono ben delineati: efficacia dal punto di vista tecnico, garanzia delle peculiarità degli ordinamenti nazionali, applicabilità su scala continentale ed effettività delle sanzioni. A queste molteplici esigenze non sembra potersi rispondere se non adottando la prospettiva di una legislazione concordata fra Unione Europea e società tecnologiche, sulla scia del processo avviato con il Codice di buone pratiche ma col rafforzamento della vincolatività degli impegni. La condivisione del piano di azione fra attori pubblici e privati permetterebbe di relegare ad ipotesi residuali le sanzioni per equivalente, spesso adottate in maniera tardiva e, quindi, inutile, favorendo, invece, l'adozione di misure in forma specifica che garantirebbero delle risposte utili al contrasto alla disinformazione.

[31] Art. 83, cc. 4, 5 e 6.

[32] *Disinformation and propaganda*, cit., 83.

Key findings of the Italian joint sector inquiry into Big Data

Enzo Marasà

Summary

1. Introduction. – 2. Considerations from the Italian Authority for Communications (AGCOM). – 3. Considerations from the Italian Privacy Authority (*Garante* or IPA). – 4. Considerations from the Italian Competition Authority (AGCM or ICA). – 5. Main takeaways from the inquiry and what to expect.

Keywords

Big Data – consumers – competition – data protection – privacy

1. Introduction

On February 10, 2020 the Italian Authorities for Communications[1], Competition[2] and Data Protection[3] published the findings of a joint sector inquiry into the field of Big Data ("Investigation")[4], which lasted almost three years. It was launched on May 30, 2017 to study the functioning and impact of Big Data on the economic, political and social environment and whether the applicable regulatory framework is suitable to address concerns for the protection of privacy, consumers and competition.

Differently from similar studies in other jurisdictions[5] – which have seen the "in silos" involvement of competition authorities separately from other regulators – the Italian Investigation is the first featuring a joint effort of the three regulators of the areas of law mainly affected by the transition from analogical to digital economy. The greater added value of the Investigation rests indeed on its interdisciplinary character and the Italian ability to mix ingredients together, valorizing each one individually and as a whole.

Definition

The expression "Big Data" is used to describe the collection, analysis and storage of a vast quantity of personal and non-personal data generated from different sources. They are characterized by four main features (referred to as "the four Vs"):

1 *Autorità per le Garanzie nelle Comunicazioni* (AGCOM).

2 *Autorità Garante della Concorrenza e del Mercato* (AGCM).

3 *Garante per la Protezione dei Dati Personali* (*Garante*).

4 Published on the AGCM's website (at this link).

5 Including, inter alia, in UK, Germany, France, Spain and Benelux countries.

Volume of the enormous quantities of data collected and processed
Variety of the many different types and sources of data gathered
Velocity of the processing and elaboration activities
Value acquired by processed and elaborated data.

Value chain
The Investigation has portrayed the value chain of Big Data as structured along three levels: *(i)* data collection (further divided by data generation, collection and retention); *(ii)* data elaboration (extrapolation, integration, analysis); *(iii)* data interpretation and decision-making.
The content of the Investigation (122 pages) is vast and articulated and it is thus impossible to thoroughly address all the issues raised in a brief format. In subsequent sections A, B and C we have distilled the key findings of each of the three authorities in their respective remits. In the final section D, we wrap up with a few conclusive observations.

2. Considerations from the Italian Authority for Communications (AGCOM)

The development of digital markets and powerful platforms does not only involve the need to investigate Big Data from a competition and regulatory standpoint but also requires analysis from a constitutional perspective. AGCOM addresses Big Data from that angle too. It also observes that market failures in the context of Big Data do not only depend from the structure of markets and dynamics of supply (e.g. market power, network externalities, economics of scale) but also from certain distorted dynamics of demand of digital content/services stemming from users (as influenced by framing, prominence, self-confirmation bias, default-bias etc.). As illustrated by studies on behavioral economics, these novel distortions may too negatively compromise a competitive environment in digital markets to the detriment of consumer choice and pluralism.
Considering its competences, the analysis of the AGCOM focuses on the impact of Big Data on: (i) the dissemination of information and the protection of fundamental rights; (ii) the functioning and role of online advertising in driving consumers' information and preferences; (iii) the regulatory framework for audiovisual services and electronic communications, with a focus on regulatory asymmetries between "over the top" players (OTTs) and traditional operators.

2.1. Dissemination of distorted and biased information and threats to democratic process

The creation and supply of informative content is deeply impacted by the advent of Big Data. The Investigation highlights that the traditional journalistic and scientific cri-

teria, which before the digital era worked as gatekeepers of objective criticism, are losing this fundamental role in the society along with their ability to curb disinformation. The concentration of digital markets in the hands of a few platforms (GAFA[6]), which in large part distribute informative content generated by a great number and variety of non-professional editors (often users themselves, or even bots and algorithms), brings to a new paradox: the great increase of sources of information caused by the digital revolution does not lead to an increase of quality and variety of information but rather the opposite. The reality is that it seems to increase polarization of views while lessening the ability of consumers to distinguish between objective information, opinion and fake news.

The AGCOM warns that these factors threaten fundamental freedoms at the very founding of the democratic process and must therefore be tackled as a priority through strong policy initiatives and – possibly – new regulatory tools.

The basic concept is that data-driven, zero-pricing digital businesses aim at capturing as much consumer attention as they possibly can (generating so called "attention markets"). Digital platforms push consumers to produce a vast array of data through proposition of attractive content and interactive functions (*like*, *scroll*, *search, etc.*). As a result, platforms profile users and provide customized content strictly related to their online "history". This may severely affect the quality and neutrality of information received by users as it leads to circular mechanisms (e.g. filter bubbles, self-confirmation bias, anchor effects, echo chambers, group thinking, etc.) in which individual users reveal the information they are prone towards through their actions. The platform's algorithm then circularly re-proposes content to the same user (or clusters of users) which confirms their opinions and beliefs.

These mechanisms isolate discussion environments and predispose favorable conditions for microtargeting disinformation campaigns on aspects which have deep political and cultural impacts. Ultimately, these campaigns would allow – through the massive collection and exploitation of data – to actively influence voters, threatening the functioning of democracy. AGCOM thus rightly observes that in the digital era effective competition and differentiation of sources in the media markets (external pluralism) is no longer enough to ensure real information pluralism and quality. To the contrary, uncontrolled multiplication of sources might even accentuate auto-selection and polarization in the research and dissemination of information (*backfire effect*) if these issues are not properly addressed.

So far, to counter these practices the AGCOM has implemented and is further promoting co-regulatory initiatives with digital operators' associations and experts aimed at setting best practices codes, creating *ex ante* quality benchmarks combined with enhanced transparency obligations, *ex post* monitoring and fact-checking, and initiatives of "digital literacy" against disinformation and hate speech. Regulatory tools already exist in the weaponry of the AGCOM[7] and are being updated to also enable monitoring and tracking of ownerships and corporate links between platforms and websites/

[6] Common acronym to refer to Google, Apple, Facebook and Amazon. GAFA(M) includes Microsoft.

[7] Like the "*Informativa Economica di Sistema*" (IES) – a mandatory monitoring system provided for by national law.

brands, including sources of financing of fake contents by online advertising. The AGCOM also warns that the contrast to disinformation online requires that similar and other regulatory initiatives be tackled at EU level; and is proactively cooperating with the European Commission and the EU network of national regulatory authorities to that end.

2.2. Big Data & Online advertising: concerns for competition and pluralism

The crucial value of data for advertising purposes, which is functional to creating specific profiles on consumption habits, pushes online platforms to capture as much consumer attention as possible through the promotion and proposition of appealing content. The data so gathered are then marketed to advertisers or intermediaries and monetized, sometimes by breaching privacy rules and fundamental rights of individuals.

Against this backdrop, in July 2019 the AGCOM, in the context of the competences assigned by sectoral legislation[8], initiated proceedings aimed at assessing the existence of dominant positions in relevant markets within the online advertising sector, as capable of hindering pluralism in the wider "Integrated System of Communications" (ISC)[9]. It is the first proceeding directly involving online platforms and the correlation between collection and profiling of data for commercial purposes. The AGCOM has wide statutory powers to impose structural remedies to remove dominant positions within the ISC (for purpose of pluralism)[10] and it intends to use it to address competitive concerns at various levels of online advertising' value chain, including collection and profiling of data.

In addition to the aspects of competition and pluralism, the AGCOM points out that the dynamics of the collection of data for advertising purposes can lead to production and dissemination of disinformation and content contrary to human dignity (hate speech, racial or sexual discrimination, violence etc.).

2.3. Regulatory asymmetries and the pursue of a level playing field between OTTs and offline players

Zero-pricing digital businesses, combined with Big Data and the high level of concentration in digital markets, may enable certain platforms to aggressively expand into traditional markets with potentially disruptive consequences. Regulatory asymmetries between OTTs and "offline" players is often a perceived cause of unfair competition as it may unlevel the playing field between them. The Investigation shows that regula-

[8] Legislative Decree no. 177/2005 (as amended from time to time) and Art. 1 of Law no. 249/97.

[9] It is a bundle of media, tlc, publishing, and advertising markets statutorily defined by Legislative Decree no. 177/2005.

[10] Art. 43 of Legislative Decree no. 177/2005.

tory asymmetry is particularly problematic for competition in the electronic communications and audiovisual services sectors. Indeed, traditional operators of these sectors are since long calling for approximation of their regulatory and liability regime to that applicable to OTTs.

Electronic communications services

According to the AGCOM's findings, the need to approximate regulatory regimes in this sector has emerged mostly with respect to the following aspects.

-Safeguarding open internet and net neutrality. The rules provided by EU Regulation 2015/2120[11] to safeguard net neutrality principles, which so far have been applied solely towards internet access providers, might have to be extended to "algorithmic" platforms operating in highly concentrated markets to guarantee transparency, fairness and neutrality in the provision of strategic digital services to other businesses[12].

-Number-based interpersonal communications. The most widely diffused interpersonal communications and messaging services using the internet (e.g. WhatsApp, Messenger, etc.) require the indirect use of a mobile number as an identifier. This feature makes their functioning in the substance equivalent to traditional telephone/SMS services, whilst according to the EU regulatory framework they cannot be characterized as electronic communications. Certain measures have been introduced at EU and national level to reduce this regulatory asymmetry[13], though OTTs still escape from general authorization's requirements and thus from access and interconnection obligations applicable to traditional telephone and networks operators.

-Data protection/retention asymmetry. The pervasive diffusion of powerful OTT platforms, combined with Big Data, has unveiled a source of competitive distortion relating to differences in the applicable data protection regimes. Stakeholders from the electronic communications industry complain that traditional operators are subject to more stringent obligations on data collection and processing compared to OTTs, disadvantaging the dynamism and quality of their offering. For instance, while traditional telephone operators are subject to new consent requirements to provide enhanced data-driven services (e.g. based on geo-localization) to their customers, OTTs may request a unique consent for a bundle of digital services including interpersonal communications.

Audiovisual services

Audiovisual operators have highlighted regulatory asymmetries with respect to OTT content aggregation or hosting platforms, which do not have editorial responsibility

[11] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015.

[12] The AGCOM notes however that Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 may have addressed some of the concerns in this respect.

[13] AGCOM refers to: (i) the introduction by Art. 1(44) of law no. 124/2017 of the obligation for operators that indirectly use national plan's numbering resources to subscribe with the Register of Operators of Communications (ROC) managed by the AGCOM; and (ii) the possibility introduced by the new EU Electronic Communications Code for Member States to impose interconnection obligations to OTTs in limited cases an under the principle of proportionality (Recitals 16, 18, 149 and Art. 61.2.*c* of EU Directive 2018/1972 of 11 December 2018).

and do not own the content (e.g. platforms like Youtube, social networks and other hosting providers).

-Access to users' data and issues of data ownership. Traditional audiovisual service/content providers, unlike OTTs, find difficult to access data generated by consumers viewing their original content through the OTTs' platforms. Such data remain in the OTT's exclusive availability even without owning and having invested in content production. This puts traditional audiovisual content providers, unless vertically integrated with OTTs, at a competitive disadvantage vis-à-vis digital platforms in acquiring new customers' data and improving content accordingly. OTTs may leverage on this advantage to enter and quickly displace traditional players in the upstream content markets. The AGCOM suggests this concern may be addressed by introducing interoperability and data portability procedures by means of contract between content providers and OTTs, provided that the contractual solution complies with GDPR's consent or legitimate interest requirements. However, considering that market forces in the digital environment may not bring to solve this concern by contractual autonomy, the AGCOM evokes the possible introduction of new regulation on ownership and control of viewers' data.

-Editorial liability of OTTs over hosted content. The AGCOM considers that by organizing, promoting and ranking aggregated content based on Big Data analytics and algorithms, OTTs may harm democracy and human dignity if not held liable for the illegal content they may diffuse. Several stakeholders have complained that the e-commerce directive[14] exempts hosting platforms from prior monitoring obligation and liability on the illegal or dangerous content they may host (unless for not removing it *ex post* once identified). The new Audiovisual Service Directive[15] recognizes in part the growing competitive pressure of OTTs (in terms of audience and advertising revenues) towards traditional audiovisual service providers in this respect. In particular, it extends certain rules typically applied to the "offline" audiovisual world – namely on protection of underaged people and wider public from violent, offensive or anyhow criminal audiovisual content – to social media and video-sharing platforms if the platforms' "essential functionality" is the provision (even by mere automatic means or algorithms) of entertainment programmes and user-generated videos[16].

3. Considerations from the Italian Privacy Authority (*Garante* or IPA)

From a privacy perspective, the IPA stresses that its task is to limit the possible impact of Big Data on people's fundamental rights by, at the same time, preserving the benefits that may come from them.

[14] Directive 2000/31/EC (see Arts. 12-15).

[15] As amended by Directive (EU) 1808/2018.

[16] See Recital 5 and the new Art. 28.*b* in Directive (EU) 1808/2018.

3.1. To what extent GDPR may help handling data protection concerns raised by Big Data

The IPA notes that the GDPR[17] does not expressly deal with, and is not entirely fit to tackle, all the issues arising from across the whole value chain of Big Data. Certain provisions applicable to the collection phase may nonetheless effectively protect data subjects from information asymmetries and, indirectly, from the risks related to profiling and automated decisions. Further, the entire processing of personal data must be carried out in compliance (*by default and by design*) with the principles of lawfulness (consent/legitimate interest), fairness, transparency, purpose/data/storage minimization, accuracy and security, which are at the foundation of the GDPR (Arts. 5-6). Nevertheless, the IPA provides no straight answers to the question whether and how the GDPR may make massive volume of data collection and processing through automated techniques, which intrinsically characterizes Big Data, compliant with these fundamental principles.

3.2. The importance of preserving quality of Big Data to ensure fair and transparent profiling

The requisites of "trustfulness" and "quality" of personal data play a decisive role to a GDPR-compliant use of Big Data in profiling individuals. In this regard, the IPA invokes effective enforcement of Recital 71 of GDPR[18]. Indeed, the added value of Big Data, compared to traditional data, consists in the possibility to extract from personal data more meaningful information to identify behavioral trends, address people's needs and predict their future decisions. This is made possible by the combined use of tracking and analytics technologies (e.g. cookies and IoTs combined with AI/algorithms) enabling the direct observations of data subjects and the automated collection of related data to infer other data/information from various datasets (e.g., by identifying recurrent statistical-probabilistic correlations). The level of accuracy in processing personal data may therefore significantly condition the digital and non-digital behavior of data subjects.

3.3. The importance to comply with transparency requirements when processing Big Data

Big Data analytics techniques are frequently accused to be opaque: often users are not

[17] Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation).

[18] Recital 71 of GDPR states that «the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons […]».

aware of which data are collected and for what purposes. Therefore, the IPA highlights the paramount relevance of the GDPR's provisions aiming at ensuring transparency, particularly those requiring to inform data subjects «of the existence of automated decision-making, including profiling, referred to in Arts. 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject». In this regard, the IPA notes that a correct enforcement of the principle of transparency may also significantly affect competition in digital markets, considering that the information given to data subjects may influence consumer choice in the same way as labels on goods may do.

3.4. Complexities with anonymization and pseudonymization of Big Data

Big Data often do not involve personal data. However, the IPA stresses that it is difficult to draw a hard line between personal and non-personal data as this dichotomy does not correspond to the actual complexity of the processing of Big Data. For instance, even though the processing starts from anonymized (i.e. non-personal) data, data outputs may lead to re-identify (*singleouting*) a person by combining different datasets – and this may also occur unpredictably. In other words, Big Data widen and blur the category of personal data. It is thus crucial that data controllers implement (by default and by design) "dynamic" technical and organizational measures[19] to: (i) accurately assess whether collected data are personal; and (ii) organize processing systems to preserve from voluntary or accidental re-identification. In this regard, the IPA examines the differences between existing techniques of data *anonymization*[20] and data *pseudonymization*[21].

Anonymization seeks to prevent from: (a) isolating a person from a group; (b) linking data to a certain person in a different database; and (c) inferring new personal information from another dataset. It can be achieved by combining techniques of "randomization" (e.g. *shuffling*) and "generalization" (e.g. *crowding*). However, one must find the right trade-off to preserve the utility and value of the anonymized data[22].

Pseudonymization is a less incisive and radical measure than anonymization as it allows to keep ono-to-one correspondence of the pseudonymized data with the originator. This way, while the immediate identification of data subjects is prevented in the first instance, the collected data keep their statistical and informative value intact. However, the IPA warns that pseudonymized data are still personal data (subject to the GDPR) and therefore pseudonymization cannot substitute anonymization.

[19] As opposed to "static" ore on-off measures, "dynamic" measures entail a systematic assessment at different moments in time and scope of the processing of data.

[20] Recital 26 of GDPR sets the principle that GDPR should not apply to anonymized data.

[21] See Recital 28 and Arts. 4(5), 6(3)(e), 25 and 32(1) (a) of GDPR.

[22] The IPA makes the example of an epidemic study, which is more valuable the less the data are randomized or generalized

3.5. Application to Big Data of the principles of purpose limitation and data minimization

The Investigation highlights that the enforcement of the principles of purpose limitation and data minimization is particularly challenging in the digital era. While the GDPR expressly sets out these principles and the related obligations, it is difficult in practice to apply them to massive data collection and processing through automated techniques, which is typical of Big Data.

Purpose limitation

The IPA warns that anonymization cannot be an *escamotage* to carry out processing activities incompatible with the purpose initially declared to data subjects. Enforcing the requirement to set the initial purpose as precisely as possible may help curbing arbitrary and uncontrolled use of Big Data (i.e. without renewed data subject's consent). However, the IPA recognizes that the added value of Big Data largely relies on the possibility to use data for purposes that cannot be precisely foreseen from the outset.

Data (including risk) minimization

To address this issue, the IPA invokes the strict application the "accountability" principle[23] based on a "by design approach". Data controllers should implement appropriate policies and checking systems to ensure quality, accuracy and minimized collection of data throughout the processing and against a case-by-case analysis. To this end, the IPA recommends that controllers systematically precede the processing of Big Data by a "data processing impact assessment"[24] ("DPIA") and make the DPIA publicly available. Further, controllers should adopt "dynamic" techniques to systematically check over time whether the solutions in force are still appropriate and improve them where necessary.

4. Considerations from the Italian Competition Authority (AGCM or ICA)

The ICA first provides an overview of the structure and main characteristics of data-driven markets. It then analyses various aspects of the complex interplay between use of personal data and privacy rules with market power, consumer protection and competition law, also pointing to the role and impact of public policy on the functioning of digital markets.

[23] Accountability in the framework of the GDPR requires that data controllers must not only be responsible for, but also be able to demonstrate compliance with the principles set forth in the GDPR (Art. 5.2).

[24] Art. 35 GDPR.

4.1. Structure and main characteristics of digital, data-driven markets

The ICA observes that the need to factor Big Data in the antitrust analysis mostly arises for services that either play a central role in the digital ecosystem, to the extent that could not be provided without the use of Big Data (e.g. online advertising), or are characterized by relevant information asymmetries and by distribution and intermediation activities (e.g. financial and insurance markets, with growing relevance of automotive). While these services are usually provided in highly concentrated markets also featuring dominant players, accumulation of Big Data is only one of the several factors which contribute to such characteristics. The following factors – which are not new to antitrust analysis but have become more relevant in the digital economy – still play a critical role in explaining market power of digital platforms:

- the distinctive multi-sided structure of digital markets;
- strong investments in innovative data analytics and interpretation technologies (i.e. AI and algorithms)
- economics of scale and scope;
- network effects; and
- switching costs.

The ICA stresses that it is the cumulated effect of Big Data with all these factors that is capable of strongly conditioning the competitive dynamics of digital markets, leading to "winner takes all" or "market tipping" effects, which ultimately tend to strongly benefit first movers while disincentivizing new entrants.

4.2. Big Data as a barrier to entry

Considering the above, personal data can be characterized as a barrier to entry, according to the ICA. However, the extent to which data constitute a barrier to entry must be measured case-by-case against: (i) actual relevance of Big Data for the service in question; (ii) nature, quality and quantity of data needed to compete effectively; and most importantly (iii) number and variety of sources available to attain the information and knowledge generated by such data and which is required to compete effectively.

The Investigation indicates that, in principle, what causes grater competitive strength is not data themselves but the additional information and knowledge which is possible to extract from data. In certain markets (e.g. online search) the competitive advantage may depend on the availability of a greater volume and variety of data, which combined with well-established algorithmic and machine learning technologies generate new knowledge and improved services[25]. However, the ICA notes that in digital advertising the greater value of real-time data, which can be sourced and replicated indefinitely from various sources, may make barriers for new entrants less significant

[25] Referring to online search, the ICA also mentions the need to consider increasing and decreasing economics of scale generated by the ratio between quantity, variety and frequency of data collection, citing in this respect the European Commission's *Google Search (Shopping)* case (AT.39740).

and thus incumbent's advantage deriving from Big Data less sensitive for competition. In other contexts, raw data may be easily available in large quantity and variety and the crucial factor for gaining a competitive edge is the possession of superior and proprietary AI technologies developed through important investments in innovation. Further, some markets require both data and innovation, whilst others need data of a certain quality over quantity[26].

Overall, the ICA highlights that most datasets are somehow replicable as there are countless online and offline data available on the market for different uses, often publicly accessible[27]. Hence, it concludes that only exceptionally Big Data may constitute an "essential input" to operate on a market.

4.3. Novel characteristics of market power and new challenges for antitrust in the digital ecosystem

The ICA takes as a fact that certain strategic digital services are today controlled by dominant companies, expressly pointing to markets for online search and mobile operating systems, social networks and intermediation services in e-commerce. More in general, it points to "systemic" market power caused by the global dimension and the strategic role of *gateways* played by these services. Such role would give certain platforms a "decisive influence" on social and economic dynamics of the Internet by managing access to digital markets, visibility and reputation of third-party undertakings. In particular, the Investigation identifies the following key contributors to market power of digital platforms:

-Vertical and conglomerate integration. It is considered a distinctive characteristic of leading platforms across the Big Data value chain. Supplying a whole range of services allows these platforms to combine data generated by the same subjects from different digital sources and behaviors, and thus better profiling. This integration of data and services is deemed to entrench the power these platforms hold in every market where they operate. This feedback mechanism enables certain platforms to provide an even greater range of services and to enter new markets, gaining a competitive edge from the outset. Further, the ICA points to the strategic position held by certain platforms in supplying crucial intermediate services for acquisition and elaboration of data (e.g. hosting, cloud, analytics etc.); and to the lock-in and lock-out effects that the integration of all these services, combined with limited interoperability, may have on customers and potential competitors respectively.

-Persistency of market power. Network externalities typical of multi-sided digital platforms, combined with the availability of a large volume of detailed data on users' behaviors, apparently make the market power of certain big players difficult to contend

[26] The ICA refers digital agriculture as example of a sector where data are a key competition driver and may require all the listed characteristics. See European Commission's decision in *Bayern/Monsanto*, Case M.8084 (2018).

[27] ICA refers to European Commission's merger cases *Facebook/WhatsApp* (M.7217) and *Apple/Shazam* (M.8788), in addition to hearings of Big Tech companies.

for an indefinite timeframe, according to the ICA's findings. Such perceived persistency of market power makes the high concentration level of digital markets even more problematic, as it risks discouraging investments in innovation and preventing future market entry.

-Novelty of market power. The ICA stresses that digital economic is challenging basic and consolidated antirust concepts such as the notion of undertaking, relevant market and market power. It points to the paradox that incumbents in traditional/offline markets (e.g. physical banks or insurance companies) seem to attribute actual market power to digital operators that yet have not entered their markets. Indeed, thanks to the greater availability of Big Data and the unmatchable technical capabilities to pool and exploit data to their advantage in potentially any sector, certain platforms are perceived as being able to disrupt the existing positions and become dominant immediately after entry. Competition authorities are worried that, lacking ad hoc powers and regulatory tools to intervene before conduct being occurred, they may lose momentum to prevent the creation or strengthening of persistent dominant positions in digital markets that could be extremely difficult or too late to remedy *ex post* by means of the existing antitrust toolkit.

4.4. Market power and control of concentrations

The ICA shares with other competition authorities the concern for a gap in merger control legislation, which allows digital incumbents to acquire innovative start-up platforms or technologies before they can thrive and threaten the persistency of their market power. The targets are businesses with yet a tiny or no turnover that are however very valuable for incumbent platforms because of the strategic value of their data and their innovative potential. Where the aim of such acquisitions is not to give a chance to thrive to an innovative business, which otherwise would not have a similar growth potential, but rather to impede effective competition in digital services, they are called "killer acquisitions".

killer acquisitions may escape antitrust scrutiny because the prior notification and authorization system of most merger control regimes globally is based on market turnover thresholds, which trigger mandatory notification if exceeded by the parties of the concentration. These thresholds were set in a time where market turnover was a reasonable proxy of size and power of firms, whilst the speed of innovation of digital economy and the value of data generated by zero-pricing services was not even conceivable. The target of a killer acquisition will often not exceed the minimum turnover threshold which triggers prior notification obligation with any competition authority and will thus escape scrutiny altogether. It may also be impracticable to calculate market shares in the digital sector, considering that target's activity could be an innovative service or platform with yet no market presence.

From the substantive viewpoint, increasing market power by means of mergers and acquisitions in the digital sector poses new concerns for competition, going beyond effects of the concentration on prices. The ICA warns that, in a digital economy boosted

by zero-pricing services, quality or innovation and privacy seem the most important competition drivers, which are mostly affected by market power. Analyzing these types of effects in concentrations indeed creates new challenges for the antitrust analysis: it is not only exponentially more complicated to assess the likelihood of a harm to competition; it is also difficult to distinguish between effects on competition, which is the object of antitrust law, and effects on public objectives assigned to other authorities, e.g. the protection of privacy and of other fundamental rights.

In line with similar stances expressed by public institutions globally, the ICA pushes for both procedural and substantive changes to merger control regimes at both national and international level. First, it supports the introduction of value-based thresholds (i.e. purchase price or assets' value) in merger control regimes to detect killer acquisitions. Secondly, it calls for reviewing European Commission's criteria for the antitrust analysis of concentrations by giving greater relevance and clarity to "conglomerate effects" on competition in the digital sector (e.g. with respect to powerful platforms' ability to leverage on Big Data generated by various services to create or entrench dominance across markets).

New guidance is also needed to make complicated analysis on potential effects of mergers on non-price parameters (e.g. innovation, quality, privacy level) or on the collusive potential of pricing algorithms in concentrated digital markets. All these complications are enhanced by the difficulty of defining relevant markets in the digital economy: in this respect, the Investigation suggests that the centrality of market definition in EU competition law should not prevent or make excessively complicated to stop conducts clearly producing exclusionary effects[28].

4.5. Characterizing personal data as commodity, price or quality: impact on competitive analysis

The ICA recognizes that while characterizing personal data as price or quality may – theoretically – help assessing the effects of Big Data on competition and consumers, it is exceptionally complicated to determine a minimum benchmark or expected competitive level of privacy and thus whether platforms' conducts may cause harm to competition or consumers (e.g. by unfair "prices" or degradation of quality).

Interestingly, while the ICA observes that personal data do not usually constitute autonomous object of trade but rather an ancillary good in the demand or supply of products/services, it nonetheless analyzes the features of demand and supply of personal data as they were the autonomous object of a relevant product market. By contrast, it warns that considering personal data themselves as "commodity" or "currency" might conflict with the philosophy underlying the protection of privacy as a fundamental right.

However, considering personal data as a component of the price or, in the alternative,

[28] European Commission's top officials reported to press they are about to launch a public consultation for reviewing the 1997 Market Definition Notice to respond to the new challenges of digitization and globalization.

as a quality feature of digital products/services is deemed a helpful means to address by law the impact of the merchandise of personal data on consumer welfare and competition. Characterizing personal data as (non-monetary) price highpoints that they are often the sole economic consideration in exchange of a product/service, and this enables authorities to use EU law to protect competition and consumers in "zero-pricing" digital markets.

Nevertheless, the ICA recognizes that the relationship between quality or price and the level of privacy is not univocal. For several services and consumers, a greater collection and matching of data means a more efficient service. Further, the Investigation shows that it is difficult for consumers to assign a specific value to their personal data since it is often hidden or unpredictable. The real value of personal data may be only revealed when combined with other datasets at a given point in time, acknowledgeable only by data controllers.

Further, the "negotiability" of privacy is at odds with the low level of differentiation of privacy conditions in digital platforms' offering as well with fundamental rights relating to protection of personal data (e.g. the need to comply with Arts. 5-6 GDPR). In addition, assigning the role of price or quality to personal data may "backfire" as it entails that digital players – assuming they would differentiate their offering based on the level of privacy – could charge real money for "premium", more data-protective services, thus making privacy a "luxury for a few". In this respect, the Investigation illustrates a "privacy paradox": while the very large majority of respondents to the ICA's surveys declared their strong interest in protecting their personal data, a mere third of it refuses to give whatever requested consent – a distortion attributed to the "free effect" of the offering of digital services.

4.6. The (ambivalent) effects of privacy policy on competition

Along this line, the ICA indicates that privacy rules may have an ambivalent impact on competition. A restrictive approach to data protection may curb digital incumbent's market power but also hamper the circulation and use of data across multiple sources and thus strengthen barriers to entry. However, national experience has shown that a coordinated application of sector regulation (e.g. energy and financial) with privacy rules can lead to identify the right balance to use access to data to support the dynamics of competition[29]. A full application and enforcement of the GDPRS' provisions may thus contribute to level the playing field between digital incumbents and new entrants.

The Investigation points to three topics in privacy enforcement having a crucial impact on competition: (i) portability; (ii) ownership/management of data; and (iii) purpose limitation combined with consent requirements.

(i) Data portability. The introduction of data portability by the GDPR (Art. 20) is deemed in principle a fundamental step to reduce switching costs (i.e. lock-in risks for

[29] See in this regard Decision of the *Garante* no. 39 of 25 July 2007.

users deriving from accumulation of data with one's platform) and to incentivize "multihoming" across platforms. However, the ICA observes a few potential obstacles to full exploitation of portability. Firstly, surveys sent to consumers have revealed scarce awareness of this right and on how to use it (up to 91%). Secondly, around 40% of users show low propension to multihoming for certain services (e.g. social networks) because of the time/effort it would take or lack of real alternatives. Thirdly, different standards often cause the transfer of datasets across platform technically unfeasible or unhelpful. In this respect, the principle of portability of the GDPR applies to users' raw datasets, and not to information extracted therefrom. Indeed, the GDPR only requires interoperability of platforms' data transfer systems, which does not necessarily entail compatibility of transferor's data with the transferee's services.
(ii.) Ownership and management of data. Some experts heard by the ICA suggest that market dynamics in connection with circulation of personal data may be improved by defining property rights over personal data. Similarly, other have suggested to develop alternative legal and technical architectures for managing personal data, e.g. by passing from the current system based on "centralized" management of data by platforms to a "decentralized" system based on users' control. However, the feasibility of such a solution is conditioned by the ability of users to identify the value of their personal data, which is often not foreseeable *ex ante*.
(iii.) Data minimization, purpose limitation and consent requirements. The Investigation highlights that the massive and generalized collection of Big Data inherently conflicts with the principles of data minimization and purpose limitation, which require controllers to obtain new consent from data subjects to use their data for purposes exceeding that initially communicated. Nonetheless, it may be impossible to foresee from the outset how collected data might be used and the utility they may have. Therefore, how the consent requirement is applied in relation with the principles in question may crucially impact competition by significantly affecting the ability of digital operators to promptly expand into new services and markets. Innovative solutions like "dynamic consent" (by which data subjects should be requested to confirm or retrieve their consent based on actual use of data by controllers over time) may favor the participation of individuals in processing their personal data, reduce information asymmetries enhancing "consumers empowerment" and thus improve competitive dynamics. Dynamic consent may however require alternative architectures for ownership and management of data as well as a functional separation of platforms' activities.

4.7. Possible scope of intervention of the AGCM

The ICA Investigation confirms the ICA's determination to make any possible legal use of its wide powers to enforce competition and consumer protection law to prevent the harmful consequences that may derive by misuse or strengthening of market power in the digital environment.

Consumer protection

In the recent years the ICA has fined leading digital, zero-pricing platforms for allegedly misleading and aggressive practices on the grounds that they collected personal data of consumers in exchange of services promoted as "free", without however correctly informing on how personal data are used and monetized, irrespective of a breach of the consent requirements set forth in the GDPR[30]. It now seems also willing to monitor personalization of prices and discriminatory conducts based on tracking consumers' spending behaviors and preferences by using algorithms and Big Data techniques[31]. Personalization of services may be greatly beneficial to individual consumers and consumer welfare, though it may also become unfair if leads to harmful or obscure discrimination based on use of personal data unknown to consumers and which obstructs their ability to make informed commercial choices. Notably, to effectively pursuing and enforcing consumer protection in digital markets, the ICA calls for legislative interventions to increasing maximum fines and investigative powers in the field.

Competition law

The ICA indicates that conducts entailing the use of Big Data may constitute antirust infringements (Arts. 101 and 102 TFEU or the national equivalent) in several circumstances:

-Abusive conducts. According to the ICA, the three abuse investigations carried out by the European Commission against Google in the recent years are perfectly consistent with traditional abusive conduct. The Commission has framed the peculiarities of a digital commercial practice (e.g. discriminatory use of search algorithms) within a traditional theory of harm based on exclusionary effects. This considered, the ICA deems antitrust law sufficiently flexible to address a whole set of conducts in digital markets through an evolutionary application of existing rules and theories of harm.

Notably, while recognizing the greater complexities connected with defining relevant markets in digital economy, the ICA suggests that antitrust enforcement policy could focus more on exclusionary effects than on rigorous market definition. In the ICA's opinion, this would particularly make sense for conducts leveraging on the central role of "irreplicable" Big Data in possession of a dominant platform that could simultaneously affect a variety of markets. It however stresses that refusal to deal or provide access with respect to data must in any case satisfy the "exceptional" conditions set forth by the case law on "essential facilities" to constitute an abuse. In particular, the following aspects are indicated as relevant to assess the "indispensability" of data to compete on a certain market: (i) the personal or non-personal nature of data; (ii) whether data have been collected by the dominant undertakings with the consent of data subjects rather than generated by data analytics operations or integration of various datasets;

[30] Decision of the AGCM no. 27432 in Case PS/11112 (*Facebook-sharing data with third parties*) of 29 November 2018 (as partially upheld in appeal by the first instance administrative court TAR Lazio). A precedent in line is Decision no. 26597 in Case PS/10601 (*Whatsapp – transfer of data to Facebook*) of 11 May 2017.

[31] A trend that may be confirmed during the COVID emergency with aggressive and frequent use of interim measures by the ICA (including obscuration of websites) to stop misleading practices or price gauging by digital merchants and platforms in the e-retail of essential product or services.

and (iii) the impact of GDPR or other regulations to portability and circulation of the data concerned.

Finally, the ICA speculates on hypothetical exclusionary conducts consisting in "reducing rivals' data" (as mirroring more traditional "increasing rivals' costs"). Examples refer to making more difficult for competitors to access customers' data by imposing contractual limitations to use certain services or by means of exclusivity agreements with third parties; or other obstacles imposed to customers to use competitors' services. Exploitative abuses, though more complicated to find, are deemed to possibly arise in connection with imposition by dominant platforms of unfair or "excessive" collection of personal data. Despite admitting that it is problematic to assess the competitive level beyond which collection of personal data may be deemed unfair or excessive, the ICA indicates that exploitative abuses may apply to a broader set of circumstances in digital markets than in traditional markets.

-Restrictive agreements. The ICA reminds to mainstream theories about the potential anti-competitive effects of pricing software or algorithms used by vendors or platforms to monitor and set prices of goods and services on the Internet[32]. Such algorithms may be designed or operated by competitors with the object or effect of automatically colluding on higher resale prices, in which case traditional case law on cartels may apply unproblematically. If, otherwise, such effect were the result of tacit, anti-competitive interaction between sophisticated algorithms without human intervention and awareness (so called "robot collusion"), it could become extremely complicated to construe a "meeting of minds" or "common understanding" between competitors, as required by the established case law to find an infringement of Art. 101 TFEU.

5. Main takeaways from the inquiry and what to expect

The Investigation shows that, in the field of Big Data, privacy law and policy represent the cornerstone to the main issues affecting the protection of competition, consumers and fundamental rights (including ultimately democracy). However, privacy law has ambivalent effects on these issues and may cut both ways depending on the specific circumstances. A restrictive enforcement of data protection may raise barriers to circulation of data and competition to the detriment of new entrants, while a loosen enforcement may favor digital incumbents. There is indeed no straightforward relation between competition and use of personal data and no one-size-fits-all solution.

This said, the Investigation seems to suggest that "dynamic consent" requirements may be a possible means to address a few crucial concerns in the field of competition, media pluralism and privacy. From the perspective of privacy, dynamic consent would help restituting control of personal data to data subjects and enforcing the principle of purpose limitation. From the perspective of media regulation, it would help leveling the playing field between OTTs and traditional players by approximating regulatory asymmetries on use of customers' data. From the perspective of antitrust, dynamic

[32] One of the basic texts cited on this topic is A. Ezrachi - M.E. Stucke, *Virtual Competition – The Promise and Perils of the Algorithm-driven Economy*, London, 2016.

consent could curb market power of digital incumbents by constraining their ability to leverage on Big Data accumulated across a variety of sources and services to cement their dominance into existing or new markets.

Further, dynamic consent architectures, by giving consumers better control on their data, may raise a barrier to supply-side substitutability between different digital services, thus contributing to functional separation of platform's activities. This in turn would help shaping and distinguishing relevant markets in the digital ecosystem, thus preserving rigorous market definition as a foundation of EU antitrust analysis. In this respect, various authorities across the EU, including the ICA, have proposed to loosen the centrality of market definition to better address abuse and concentration cases in digital markets. However, this stance could undermine certainty and predictability of antitrust law, ultimately making it prone towards non-economic or political considerations.

In the field of media and communications, coordinated legislative and regulatory updates along with changes to the GDPR may be necessary to develop new data ownership's architectures, which in turn would help level the playing field between OTTs and "offline" operators. For example, the rules on portability and circulation of data must be coordinated with consent and purpose limitation requirements as well as with specific consent requirements prescribed by sector regulation.

The Investigation makes evident that in-silos application of sectoral legislations by different authorities and countries is an obstacle to effectively remedy to concerns raised by Big Data on competition, consumer welfare and data protection. Given the global scale of digital players and the imperative of the Single Market within the EU, the raised issues cannot be tackled through a fragmented approach along sectoral or national lines. A holistic, synergic and harmonized application of different fields of law across jurisdictions, which combines sector regulation and common constitutional principles, has become increasingly indispensable. A few months after the conclusion of the Investigation, the European Commission launched public consultations on new ex ante regulatory measures and a New Competition Tool[33], which seem to address these concerns within such a perspective.

At the same time, competition law has its own limits and should not be used to achieve public goals that pertain to other legislative fields or political objectives. Arbitrarily using competition, consumer protection or privacy law to address one another's concerns may indeed cause conflicts of competences between authorities and the risk of double jeopardy [34]. To avoid the risk of conflicts of competences and double jeopardy in the field of Big Data, undertakings should be given the opportunity to defend within

[33] A high level and neutral summary of the rationale and possible content of the proposed measures is available in this article from the author. Another independent, academic analysis of the scope and purpose of the measures was published by Prof. Pablo Ibanez Colomo on the *Chilling Competition* blog (at this link).

[34] n the 2012 Toshiba judgment (Case C-17/10), the ECJ set out three cumulative conditions for the *ne bis in idem* principle to apply in the competition field, in contrast with the two applying to criminal matters. Accordingly, two prosecution cases have to cover the same facts, the same offender and the "same protected legal interest". However, in its Opinion rendered in a subsequent case (C-617/17), AG Wahl took the view that including the identity of the legal interest as a requisite to apply the *ne bis in idem* principle to the competition field is no longer justified.

a single proceeding from interconnected allegations investing multiple infringements potentially falling under the remits of two or more authorities. In this perspective, procedural reforms in the direction of further integrating the complementary competences and skills of competition, consumer and privacy authorities, without depriving each of their own competences, may make sense.

The ability to make case-by-case analysis also seems increasingly indispensable to avoid mistakes in the assessment of infringements. This requires that competent authorities be equipped with the right technical expertise (e.g. data scientists and analysts) to make complex analysis. Certainty of law, and thus consistency and predictability, must be safeguarded too as a fundamental right to be preserved – and this is probably the real challenge posed by Big Data.

Currently, the ICA is investigating Amazon and Google for anticompetitive practices in the markets of e-commerce intermediation services and e-mobility services respectively. It alleges – inter alia – that the two platforms may be leveraging on Big Data acquired on dominated markets to preserve prominence of their own or affiliated partners' products, thus marginalizing potential competitors[35]. For the upcoming future, the AGCM is studying competitive threats raised by Big Data in the banking, insurance and automotive sector. In addition, the Authority for Communications (AGCOM) has strong *ex ante* regulatory powers in the field of control of media and pluralism by which, theoretically, it could impose structural or behavioral remedies in the online advertising sector, which is currently under inquiry by the same AGCOM. These are crucial cases to understand future competition enforcement policy in Italy on matters such as market definition and remedies in the field of Big Data.

The impact of COVID-19 on digital economy/Big Data was not considered by the Investigation as it was closed before the outbreak. Community lockdowns are likely to further increase the importance of digital services and Big Data, thus enhancing market power of digital platforms. However, competition authorities may adapt their enforcement policy accordingly. It is conceivable that the urgent and overriding objective to protect health, safety and the well-being of the general public – particularly vulnerable peoples – may extend the scope and reach of antitrust enforcement by inflating the concept of consumer welfare, pushing competition authorities to pursue conduct that otherwise would be at the boundaries of its remit.

Hence, while waiting for the New Competition Tool, and by making a virtue of necessity, the ICA may be more resolute in testing aggressive theories of harm and enforcement against market power of digital incumbents, including by resorting to interim measures any time an immediate threat to weakened businesses or consumers is detected.

[35] A summary of the ICA's preliminary concerns is available here and here.

Recensioni

Per chi vuol sapere tutto di un reato, "La diffamazione", di Vincenzo Pezzella

Carlo Melzi d'Eril

Certi titoli dicono molto dei libri che presentano, come certe facce delle persone che le portano in giro. Un titolo come "La diffamazione", al lettore che lo nota, trasmette questo messaggio: il volume che battezzo tratterà tutti gli aspetti del delitto contro la reputazione, senza tralasciarne nessuno, circostanza che, a chi un po' conosce la materia, fa subito storcere il naso, poiché le questioni e i problemi, teorici e pratici, a cui ha dato luogo l'interpretazione e l'applicazione dell'art. 595 c.p. sono davvero numerosissimi.

Come certe facce, anche certi titoli, però, possono ingannare, e dare quindi impressioni sbagliate, oppure essere sinceri e non tradire le aspettative.

Il caso de "La diffamazione", di Vincenzo Pezzella, giunto alla seconda edizione, fa parte di questa seconda categoria. Il poderoso volume, di ben 1232 pagine, passa in rassegna pressoché ogni tema che dottrina e giurisprudenza hanno evidenziato in ordine al reato in parola. Da "vecchio" (potrei anche evitare le virgolette, in effetti) frequentatore di librerie e compulsivo acquirente di ciò che vi si vende, sono abituato a sfogliare gli indici dei testi: quando sono ben fatti aiutano a capire velocemente se ciò che hai in mano è di interesse o meno.

Qui la struttura del lavoro, ben descritta appunto nell'indice, fa subito capire che il contenuto della monografia ha quelle caratteristiche di completezza di cui si diceva appena sopra. Lo schema è, per così dire, classico: prima si tratta dei reati, poi delle scriminanti, quindi della peculiare casistica portata dalla modernità con i problemi sorti a causa della diffamazione on-line, infine dei profili risarcitori specifici del danno da diffamazione.

Nella prima parte, così, l'Autore dà conto del reato di diffamazione semplice, di quella aggravata, delle cause di giustificazioni comuni, delle cause di non punibilità (art. 598 c.p.) e della insindacabilità (art. 68 Cost.), nonché della prova liberatoria e della responsabilità per omesso controllo del direttore. L'ordine espositivo della materia è, anche qui, amico del lettore: per fare solo un esempio tratto dalle prime pagine, il primo punto della "diffamazione semplice" è l'analisi del bene giuridico, cui subito segue un paragrafo sulla "reputazione minima" e quella già compromessa, come quella del caso del boss pluriomicida. Questa struttura si replica per ogni argomento: di ciascuno viene prima descritta in generale la disciplina, per poi approfondire l'analisi, spesso utilizzando casi pratici, menzionati già nell'indice, particolarmente ricco e dettagliato.

La seconda parte è dedicata alle scriminanti tipiche del diritto di cronaca, di critica e di satira, con uno sguardo attento alla giurisprudenza nazionale ed europea. Qui si affrontano, tra gli altri, temi come la contrarietà della Corte europea dei diritti dell'uomo alla sanzione detentiva per la diffamazione, le peculiarità dell'intervista, la cronaca declinata per il mezzo radiotelevisivo e in argomento giudiziario, senza dimenticare di descrivere come i presupposti del diritto di critica siano stati interpretati a seconda

della materia a cui questa specifica scriminante deve essere applicata. Nell'esaminare il diritto di cronaca l'Autore non si limita a riproporre i temi classici del fondamento costituzionale, della titolarità del diritto e dei presupposti di matrice giurisprudenziale, bensì estende il proprio sguardo al diritto alla riservatezza, la cui disciplina ha più di un punto di contatto con quella della diffamazione.

La terza parte riguarda, come anticipato, il delitto commesso in rete, passando dalla discussa applicabilità delle disposizioni per la stampa alla rete, alla responsabilità dei provider, alle nuove forme di comunicazione, che inevitabilmente pongono inedite frontiere all'applicazione del delitto in questione. Facebook, Twitter, WhatsApp, Trip Advisor, in generale chat e social forum, sono tutti contesti da conoscere con attenzione per capire in che termini può essere ad essi applicata una normativa la cui radice nasce negli anni Trenta del secolo passato. Qui l'Autore sceglie felicemente il metodo casistico, ancor più che in altri punti del libro, circostanza che consente di spiegare nel dettaglio le soluzioni adottate in passato e quando tali soluzioni possono essere richiamate come precedente, per individuare magari gli anelli di una catena che configuri un filone giurisprudenziale in grado di tracciare un sentiero in una materia così sconnessa e poco arata.

L'ultima parte del tomo ha ad oggetto i profili risarcitori specifici del delitto in questione. E anche qui le questioni relative alla liquidazione e alla quantificazione del danno si snodano tra i rapporti fra azione civile e azione penale, la disciplina relativa alla pronuncia sui danni in sede penale e la provvisionale con i relativi problemi applicativi nei gradi successivi al primo. Anche in questi passaggi l'occhio dell'Autore passa con penna agile dalle architetture dei principi e delle regole ai problemi sollevati dalla applicazione pratica della disciplina, come quando dà spazio al rilievo formulato dai giudici civili, secondo cui spesso i colleghi penalisti emettono sentenze di condanna generica quando vi sarebbero tutti i presupposti per una quantificazione più precisa.

Roland Barthes sosteneva: «dimmi come categorizzi e ti dirò chi sei». Anche solo il modo con cui le questioni e gli argomenti sono presentati in questa importante monografia, ci dice che l'Autore conosce la materia e la sa rendere fruibile a chi, esperto o novizio dei temi in questione, ha bisogno di uno strumento per approfondire o per avvicinarsi a questo reato la cui disciplina ha molti addentellati e numerose sfaccettature.

La lettura del volume, poi, convince come un tale imponente lavoro ricostruttivo della materia nel suo complesso, non possa mancare nella biblioteca del giurista che ambisce a possedere uno strumento per conoscere la materia o che si imbatte per la prima volta in essa e ha bisogno di un "Virgilio" che lo conduce negli anfratti, a volte non semplici da percorrere della disciplina, soprattutto di ultimo "conio".

La diffamazione
Vincenzo Pezzella

Utet Giuridica
Anno di edizione: 2020
Pagine: 1280
ISBN: 978-8859822301

Recensione a Emilio Tosi (a cura di), *Privacy Digitale*, Giuffré Lefebvre, 2019

Giovanni Stella

Si tratta del ventunesimo volume pubblicato nella rinomata *Collana di Studi Diritto delle Nuove Tecnologie®*.

La corposa raccolta dedicata all'analisi giuridica complessa ed attuale del tema affascinante della *Privacy Digitale* dopo la rivoluzione copernicana del GDPR si apre con l'Introduzione del Curatore, la Prefazione di Antonello Soro *Garante per la Protezione dei dati Personali,* la *Premessa* di Vincenzo Franceschelli e si chiude con la *Postfazione* del compianto Giovanni Buttarelli *European Data Protection Supervisor UE*.

Nell'introduzione Emilio Tosi - *Professore Associato Abilitato di Diritto Privato nell'Università di Milano Bicocca* e *Direttore Esecutivo di Diritto delle Nuove Tecnologie® - Studi Giuridici per l'Innovazione®* fondata nel 2003 - Curatore della completa e approfondita raccolta di studi così suggestivamente rileva:

> «Privacy digitale potrebbe sembrare una contraddizione in termini, un singolare ossimoro giuridico, ma così non è.
>
> La data simbolica del 25 maggio 2018 segna la piena applicazione della nuova disciplina uniforme in materia di tutela della riservatezza e protezione dei dati personali delle persone fisiche introdotta dal Regolamento 27 aprile 2016, n. 679 — meglio noto come General Data Protection Regulation (GDPR) UE — che ha abrogato la storica Direttiva CE 95/46.
>
> Tale rilevante novità normativa per la tutela dei diritti fondamentali della persona alla riservatezza e alla protezione dei dati personali (art. 2 Costituzione e artt. 7 e 8 Carta dei diritti fondamentali UE) ha richiesto l'armonizzazione ad opera del D.Lgs. 10 agosto 2018, n. 101 — entrato in vigore il 19 settembre 2018 — del Codice Privacy ora novellato.
>
> Il GDPR in forza della sua intrinseca vocazione transnazionale può nel contesto complesso e mutevole dei mercati digitali ben svolgere funzione di legal benchmark globale».

Nel volume in recensione vengono affrontati temi e problemi della privacy digitale con rigorosa analisi giuridica e interpretazione assiologica, costituzionalmente orientata, attraverso il prisma della normativa comunitaria e interna.

Il volume è ricco di spunti di riflessione e approfondimenti sui profili giuridici controversi che spaziano da *Social Network, Cloud Computing, Internet of Things, Smartphone, Smart Cars, Droni, Fintech, Blockchain, Big Data e Artificial Intelligence.*

Si studiano, quindi, le principali temibili variabili socio-economiche e tecnologiche – naturalmente antagoniste della tutela della riservatezza e della protezione dei dati personali – che occorre disciplinare in modo equilibrato, bilanciando contrapposti interessi.

Qui di seguito, in sintesi, i principali saggi raccolti nel volume e firmati da autorevoli

giuristi: Emanuele Lucchini Guastalla su *Privacy e data protection: principi generali*; Teresa Pasquino, *Identità digitale della persona, diritto all'immagine e reputazione*; Nicola BRUTTI, *Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer*; Pieremilio Sammarco, *Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblìo condizionato;* Ettore Battelli e Guido d'Ippolito, *Il diritto alla portabilità dei dati personali;* Alberto M. Gambino e Rosaria Petti, *Privacy e proprietà intellettuale;* Pier Filippo Giuggioli, *Privacy e consumatore;* Giuliano Lemme, *Blockchain, smart contracts, privacy o del nuovo manifestarsi della volontà contrattuale;* Anna Carla Nazzaro, *Privacy, smart cities e smart cars;* Sara Landini, *Privacy, rischio informatico e assicurazioni;* Dianora Poletti, e Concetta Causarano, *Privacy e autoregolamentazione tra codici di condotta e certificazione;* Enza Pellecchia, *Privacy, decisioni automatizzate e algoritmi;* Raffale Torino e Giovanni De Gregorio, *Privacy, protezione dei dati personali e Big Data;* Dario Farace, *Privacy by design e privacy by default;* Laura Valle et alii, *Privacy e contratti di cloud computing;* Irma Sasso, *Privacy e successione digitale;* Giovanni M. Riccio e Federica Pezza, *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali.*

E ancora il Curatore della raccolta ammonisce il lettore rammentando che nonostante la complessità della sfida regolatoria digitale e la tensione intrinseca tra tutela dei diritti fondamentali della persona, libera circolazione dei dati personali e in ultima istanza tutela del mercato:

«Occorre scongiurare il progressivo, quanto incontrollato e scarsamente trasparente per non dire opaco, *dominio dell'algoritmo*.

Non ci sono più limiti insuperabili né ostacoli alla volizione umana nella *modernità liquida* di Zygmut Bauman (*Liquid Modernity,* Cambridge, 2000): spingersi oltre nella società digitale, superare il limite, appunto, proiettandosi verso l'ignoto non appare deprecabile *hybris* — l'umana tracotanza dell'antica Grecia — ma diviene, pericolosamente, per usare le parole del filosofo Remo Bodei il «maggior vanto dell'età moderna» (*Limite*, Bologna, 2015).

La *Silicolonisation du monde* teorizzata dal filosofo francese Eric Sadin (*Silicolonisation du monde. L'irrésistible expansion du libéralisme numerique,* Paris, 2016) che stigmatizza l'espansione incontrollata del liberismo digitale peculiare della nuova *economia della conoscenza* — dei nostri comportamenti e dei nostri dati personali — oltre che del *global silicon dream*».

Emilio Tosi, oltre ad aver sapientemente curato la raccolta, è anche autore di due fondamentali contributi: il primo dedicato a *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice Privacy*; il secondo a *Responsabilità civile per trattamento illecito dei dati personali.*

Proprio il tema della responsabilizzazione e della responsabilità – profondamente riformato dal GDPR – risulta centrale nella corretta attuazione della nuova normativa comunitaria armonizzata.

La riforma comunitaria introduce, tra le tante novità, anche il nuovo fondamentale *principio dell'accountability* (art. 5, par. 2 — GDPR), della responsabilizzazione del Titolare.

Sul punto Tosi ci ricorda che «In base alle regole di *accountability* — che segnano il passaggio dalla responsabilità *ex post* alla responsabilizzazione consapevole e documentata *ex ante* — i principi posti dalla nuova disciplina divengono adattabile e flessibili alle effettive esigenze, emerse all'esito della doverosa analisi preliminare e autodiagnosi,

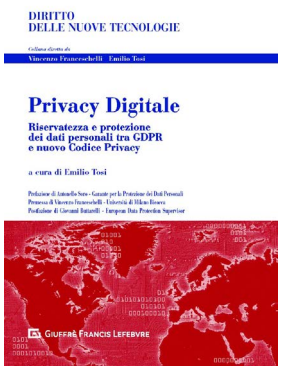
del singolo Titolare e verificabili in concreto, non meri obblighi formali ed astratti. Il concetto di *accountability* risulta, in particolare, delineato dal combinato disposto degli artt. 24, 25 e 35 del GPDR: principio innovativo e al tempo stesso insidioso sotto il profilo della *compliance* in quanto flessibile, caso per caso, in relazione alla tipologia dei dati trattati, alle modalità e alla struttura organizzativa del Titolare».

Come ci ricorda il Presidente dell'Autorità Garante per la Protezione dei Dati Personali Antonello Soro – Autore della Prefazione al volume – «ciò che, più di ogni altra misura, garantirà l'effettività dei diritti sanciti sarà la diffusione di quella "cultura della protezione dati" necessaria per promuovere, a un tempo, sviluppo economico e libertà, efficienza amministrativa e dignità della persona. Opere giuridiche, come quella curata dal Prof. Emilio Tosi, che non si limitano a descrivere la cornice in cui ci si muove, ma indicano anche la strada da percorrere e gli ostacoli da evitare, sono indubbiamente contributi essenziali e determinanti per costruire questa cultura e renderla patrimonio comune».

E ancora il compianto Giovanni Buttarelli all'epoca *European Data Protection Supervisor* – Autore della Postfazione al volume – rileva che ancora manca per completare il quadro regolatorio comunitario l'ultimo — essenziale — tassello normativo della proposta di Regolamento *e-privacy* relativo alla tutela della vita privata e dei dati personali nelle comunicazioni elettroniche sia delle persone fisiche che delle persone giuridiche, abrogativo della Direttiva 2002/58/CE: «*The GDPR and Regulation 2018/1725, along with the Data Protection Law Enforcement Directive, reinforce the EU's position as a global leader in data protection and privacy practice. They also go a long way towards helping us to achieve the strategic objective of opening a new chapter for EU data protection, set out in the EDPS Strategy 2015-2019. However, one piece of this regulatory puzzle is still missing. Only by concluding a new ePrivacy Regulation, which accurately reflects and supports the principles outlined in the GDPR, can we ensure that the fundamental rights of data protection and privacy are fully respected*».

Si tratta, in conclusione, di un'opera accurata che riesce a lumeggiare con efficacia, metodo scientifico rigoroso - pur nel rispetto della sensibilità e degli stili, necessariamente diversi, degli Autori che hanno contribuito alla raccolta - e profondità di indagine, una materia complessa e sempre più centrale nella vita non solo delle persone fisiche ma anche nelle scelte strategiche di imprenditori e Stati.

Privacy Digitale
Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy
Emilio Tosi (a cura di)



Giuffré Lefebvre
Anno di edizione: 2019
Pagine: XLVIII-686
ISBN: 9788828811381

A proposito di *fake news*: analisi e proposte per contrastare il dilagare del fenomeno. Recensione a Tommaso Guerini, *Fake news e diritto penale*

Giuseppina Ferro

"La manipolazione digitale del consenso nelle democrazie liberali" è il sottotitolo esplicativo del bel volume di Tommaso Guerini, "*Fake News e diritto penale*": un'indagine svolta tra strumenti di informazione tradizionali e cyberspazio.

L'intento della ricerca è dichiarato sin dalle primissime pagine: in una epoca di diritto penale totale non esistono fenomeni sociali che non interagiscano con il sistema punitivo. E nell'attuale contesto di grandi trasformazioni l'autore punta la lente sul rapporto tra sistema penale e forme massive di alterazione digitale del consenso mediante la diffusione tramite rete di notizie manipolate.

All'interno di una architettura argomentativa impeccabile Tommaso Guerini conduce la propria analisi muovendo dalla definizione penalisticamente orientata dell'espressione "*fake news*", quale fenomeno in grado di alterare i meccanismi di funzionamento delle istituzioni democratiche, in particolare manipolando il processo di formazione del consenso nel corso delle campagne elettorali: "un'informazione in parte o del tutto non corrispondente al vero, prodotta e divulgata intenzionalmente o inintenzionalmente attraverso il web, i media o le tecnologie digitali di comunicazione, e caratterizzata da un'apparente plausibilità, quest'ultima alimentata da un sistema distorto di aspettative dell'opinione pubblica e da un'amplificazione dei pregiudizi che ne sono alla base, che ne agevola la condivisione e la diffusione pur in assenza di una verifica delle fonti, tale da ledere beni giuridici individuali, come l'onore e la reputazione ovvero finalizzata a incidere, direttamente o indirettamente, sulla libertà dei cittadini di esercitare il diritto di voto e ad incidere sul corretto funzionamento delle istituzioni democratiche".

L'autore traccia per cenni fulminei la storia di Internet da Alan Turing ai giorni nostri, non trascurando di evidenziare come attualmente il core business dei Giganti del web sia da individuare nella raccolta sistematica dei dati, cui consegue la capacità di offrire agli utenti un mondo virtuale cucito su misura, grazie al lavoro di *profiling* costante. Conseguenza ne è il mutamento del sistema informativo che non è più monopolio dei media tradizionali. Dunque, occorre trovare strumenti capaci di contemperare la libera manifestazione del pensiero e il diritto a non vedere inquinata la corretta formazione del consenso. Il tema è caldo, come dimostrano i *case study* richiamati (tra gli altri, la campagna elettorale negli USA conclusa con l'elezione di Trump e il referendum in Gran Bretagna per la Brexit) quanto all'utilizzo dei social network nella competizione politica. Non manca, e non avrebbe potuto essere diversamente, un riferimento all'Associazione Rousseau, esperimento italiano di eliminazione dei corpi intermedi in ambito politico.

Le dimensioni epidemiche del fenomeno analizzato comportano ricadute tali da met-

tere in pericolo la genuinità della formazione del consenso, soprattutto in occasione dell'espressione della volontà politica in termini elettorali da parte della cittadinanza. Da qui la necessità di verificare il panorama normativo esistente, sia sul piano del diritto interno che sovranazionale per misurarne l'efficacia. Vengono presi in esame gli ordinamenti che hanno introdotto una legislazione dedicata alla disinformazione e/o *fake news*, distinti in tre quadranti geopolitici: Europa, Russia, Asia. Il quadro risultante in termini comparatistici evidenzia come nel panorama europeo i paesi che si sono determinati ad un intervento normativo del fenomeno hanno posto l'accento sul contemperamento dei valori in gioco, tra necessità di limitare la diffusione di *fake news* e la tutela della libera manifestazione del pensiero. Il modello russo pur apparendo assonante con l'impostazione europea alla prova pratica non risulta convincente per la vaghezza delle espressioni utilizzate (e per la posizione occupata nei rapporti internazionali sulla libertà di stampa e sui diritti politici), così finendo per essere assimilato invece al quadrante asiatico, le cui norme sono emblematicamente definite dall'autore "bavaglio asiatico".

Sul fronte del diritto interno, Tommaso Guerini ripercorre lo strumentario approntato dal diritto penale italiano a tutela dei beni giuridici che entrano in gioco, partendo dalla evoluzione del delitto di diffamazione, utilizzato com'è noto dal legislatore anche per sanzionare le relative violazioni perpetrate tramite l'utilizzo di social network, come pure dei concetti di diritto di cronaca e diritto di critica al tempo della "post-verità". La diffamazione, come le ulteriori fattispecie esistenti, astrattamente applicabili al fenomeno della manipolazione digitale dell'informazione, escono malconce dall'attenta analisi svolta dall'autore. Che si tratti di diffamazione, di pubblicazione di notizie false esagerate o tendenziose, atte a turbale l'ordine pubblico; o ancora di procurato allarme, o più specificamente di fattispecie attinenti i reati elettorali o della sostituzione di persona nel cyberspazio: tutti gli istituti presi in esame patiscono l'essere strutturati su categorie novecentesche e risultano inidonei a fronteggiare efficacemente la diffusione di *fake news*.

Lo sforzo di dare conto dello stato dell'arte in tema *fake news* si spinge fino all'esame dei progetti di legge esistenti per arginarne il dilagare. Le proposte si articolano su direttrici diverse: il primo affonda le radici nel populismo penale di questi tempi e propone l'introduzione di ulteriori fattispecie penali, unitamente all'obbligo di importanti oneri di monitoraggio e rettifica in capo agli amministratori; un altro è ispirato alla disciplina tedesca e immagina di sanzionare amministrativamente la *disinformation*, prediligendo il momento preventivo a quello repressivo. Alcune proposte si caratterizzano invece per la sollecitazione ad abolire il diritto all'anonimato on line, altre infine invocano l'opportunità dell'istituzione di una commissione di inchiesta.

Tirando le fila della ricerca, si arriva all'ultimo capitolo con la suspense di scoprire la soluzione, e Tommaso Guerini non si sottrae all'aspettativa alimentata: anche traendo spunto delle esperienze di altri paesi europei, propone una riposta alla domanda che introduce la conclusione del volume: (in)formare o punire? Si rinvia alla lettura per non svelare del tutto la soluzione proposta che ha il pregio di provare a fare una sintesi che contemperi i valori in gioco in un'ottica complessiva di strumenti di tutela in grado di ridurre le distanze attualmente esistenti tra mezzi tradizionali di informazione e social network.

Infine, va reso merito alla capacità di coniugare l'accuratezza con cui sono trattati i vari aspetti che emergono nella ricerca con la piacevolezza della lettura di un testo in cui l'autore inserisce molti spunti di riflessione interdisciplinari senza mai sacrificarne la vocazione scientifica. Il tutto con una sintesi stringente che consente anche al lettore meno attrezzato di seguire compiutamente le implicazioni della problematica affrontata.

Fake news e diritto penale.
La manipolazione digitale del consenso nelle democrazie liberali
Tommaso Guerini

Giappichelli
Anno di edizione: 2020
Pagine: X-230
ISBN: 9788892132405

Elenco autori

Jacopo Antonelli Dudan
avvocato in Milano
Cristiana Benetazzo
professore associato di diritto amministrativo, Università di Padova
Chantal Bomprezzi
dottoranda in Law, Science and Technology, Università di Bologna
Luigi Briguglio
Senior Researcher, CyberEthics Lab.
Riccardo Cabazzi
dottore di ricerca in diritto dell'Unione europea e ordinamenti nazionali, Università di Ferrara
Federico Ceci
dottorando in diritto internazionale e dell'Unione europea, Università di Bari
Giuseppe Donato
dottorando di ricerca in scienze giuridiche, Università di Messina
Giuseppina Ferro
avvocato in Roma
Giusella Finocchiaro
professore ordinario di diritto privato, Università di Bologna
Mirko Forti
assegnista di ricerca, Scuola Superiore Sant'Anna
Alice Fratti
avvocato in Milano
Maurizio Fumo
già presidente della V sezione penale, Corte di Cassazione
Sara Gobbato
avvocato in Milano
Iván Gutiérrez Agüero
researcher & developer, Tecnalia
Pietro Insolera
avvocato in Bologna, dottore di ricerca in diritto penale
Fabiola Iraci
dottoressa in scienze giuridiche
Lubos Kuklis
Chief Executive, The Office of the Council for Broadcasting and Retransmision
Michela Manetti
professore ordinario di diritto costituzionale, Università di Siena
Enzo Marasà
avvocato in Milano
Emiliano Marchisio
professore associato di diritto commerciale, Università "Giustino Fortunato"
Paola Marsocci
professore ordinario di diritto costituzionale, La Sapienza – Università di Roma
Carlo Melzi d'Eril
avvocato in Milano

Elenco autori

Domenico Natale
dirigente, Ministero dell'Economia e delle Finanze
Carmela Occhipinti
Managing Director, CyberEthics Lab.
Adriana Peduto
avvocato in Roma
Francesco Pizzetti
già professore ordinario di diritto costituzionale, Università di Torino; già Presidente dell'Autorità garante per la protezione dei dati personali
Marco Plutino
professore associato di diritto costituzionale, Università di Cassino e del Lazio Meridionale
Giovanni Maria Riccio
professore associato di diritto privato comparato, Università di Salerno
Stella Romano
avvocato in Verona, dottore europeo di ricerca in diritto costituzionale
Elena Sartini
avvocato; legal researcher - CyberEthics Lab.
Giovanni Stella
professore ordinario di diritto privato, Università di Pavia
Palmina Tanzarella
ricercatrice di diritto costituzionale, Università di Milano – Bicocca
Riccardo Traina Chiarini
avvocato in Milano
Cecilia Trevisi
avvocato in Milano
Scilla Vernile
ricercatrice di diritto amministrativo, Università di Sassari
Davide Zecca
dottorando in diritto pubblico comparato e diritto costituzionale, Università di Pavia
Paolo Zicchittu
ricercatore di diritto costituzionale, Università di Milano – Bicocca

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 2020 - CODICE ISSN 2532-9146