



SUOR ORSOLA
BENINCASA
UNIVERSITÀ EDITRICE

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

www.ejplt.tatodpr.eu

2022/1

EUROPEAN JOURNAL OF PRIVACY LAW & TECHNOLOGIES

Directed by Lucilla Gatt

2022/1



SUOR ORSOLA
BENINCASA
UNIVERSITÀ EDITRICE

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223



With the support of the
Erasmus+ Programme
of the European Union

The Journal was born in 2018 as one of the results of the European project “Training Activities to Implement the Data Protection Reform” (TAtoDPR), co-funded by the European Union’s within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191. From 2019-2022, the Journal was supported by the Erasmus+ Programme of the European Commission within the European Project Jean Monnet Chair ‘European Protection Law of Individuals in relation to New Technologies’ (PROTECH) (611876-EPP-1-2019-1-IT-EPPJMO-CHAIR).

In 2022 EJPLT has been further implemented thanks to winning the co-funding for the Jean Monnet Chair project ‘European Green Rights: reshaping fundamental rights for next generations’ (EUGREENEXT) (ERASMUS-JMO-2021-HEI-TCH-RSCH).

The European Commission’s support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

The Issues form 2018/1 to 2020/1 were published by Giappichelli Publisher. From Issue 2020/2 the Publisher is Suor Orsola Benincasa Università editrice.

Editing

Luciana Trama

Design

Flavia Soprani

Development

Emanuele Garzia

© Copyright 2022 by Suor Orsola Benincasa Università Editrice, published in October 2022

ISSN: 2704-8012

The Issue is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND

All the details at: <https://creativecommons.org/licenses/by-nc-nd/4.0>

Free access to the Issue at: www.ejplt.tatodpr.eu

The intellectual property of the individual contributions remain with the authors.

EDITOR IN CHIEF/DIRECTOR

Prof. Avv. Lucilla Gatt – Università degli Studi Suor Orsola Benincasa di Napoli, Italy

VICE-DIRECTOR

Prof. Ilaria A. Caggiano – Università degli Studi Suor Orsola Benincasa di Napoli, Italy

ADVISOR BOARD – SCIENTIFIC COMMITTEE

Prof. Valeria Falce – Università Europea di Roma, Italy

Prof. Toni M. Jaeger-Fine – Fordham University, United States

Prof. Indranath Gupta – O.P. Jindal Global University, India

Prof. Antonios Karaiskos – Kyoto University, Japan

Prof. Roberto Montanari – Università degli Studi Suor Orsola Benincasa di Napoli, Italy

Prof. Roberta Montinaro – Università degli Studi di Napoli l'Orientale, Italy

Prof. Andrew Morris – University of Loughborough, United Kingdom

Prof. Juan Pablo Murga Fernandez – Universidad de Sevilla

Prof. Alex Nunn – University of Derby, United Kingdom

Prof. Avv. Salvatore Orlando – Sapienza Università di Roma, Italy

REFEREES

Prof. Miguel Álvarez Ortega – Kyoto University, Japan and Universidad de Sevilla, Spain

Prof. Carlos Antonio Agurto Gonzáles – Universidad Nacional Mayor de San Marcos, Peru

Prof. Avv. Giuseppina Capaldo – Sapienza Università di Roma, Italy

Prof. Cristina Caricato – Sapienza Università di Roma, Italy

Prof. Roberto Carleo – Università degli Studi di Napoli Parthenope, Italy

Prof. Georges Cavalier – Université de Lyon, France

Prof. María Dolores Cervilla Garzón – Universidad de Cádiz, Spain

Prof. Anna Antonia Ciocia – Università degli Studi della Campania Luigi Vanvitelli, Italy

Prof. Carlos de Cores Helguera – Universidad CLAEH del Uruguay, Uruguay

Prof. Manuel Espejo Lerdo de Tejada – Universidad de Sevilla, Spain

Prof. Elżbieta Feret – Uniwersytet Rzeszowski, Poland

Prof. Giovanni Iorio – Università degli Studi di Milano Bicocca, Italy

Prof. Arndt Künnecke – Hochschule des Bundes für öffentliche Verwaltung, Germany

Prof. Martin Maguire – University of Loughborough, United Kingdom

Prof. Paola Manes – Alma Mater Studiorum Università di Bologna, Italy

Prof. Giovanni Martini – Università degli Studi della Campania Luigi Vanvitelli, Italy

Prof. Michala Meiselles – University of Derby, United Kingdom

Prof. Alessia Mignozzi – Università degli Studi della Campania Luigi Vanvitelli, Italy

Prof. Salvatore Monticelli – Università di Foggia, Italy

Prof. Cinzia Motti – Università di Foggia, Italy

Prof. Nora Ni Loideain – Institute of Advanced Legal Studies of London, United Kingdom

Prof. Taiwo Oriola – University of Derby, United Kingdom

Prof. Francesco Rossi – Università degli Studi di Napoli Federico II, Italy

Prof. Maria A. Scagliusi – Universidad de Sevilla, Spain

Prof. Avv. Laura Valle – Libera Università di Bolzano, Italy

Prof. Isabel Zurita Martin – Universidad de Cádiz, Spain

COORDINATOR OF THE EDITORIAL BOARD

Ph.D. Avv. Maria Cristina Gaeta – Università degli Studi Suor Orsola Benincasa, Italy

MEMBERS OF THE EDITORIAL BOARD

Prof. Sara Lorenzo Cabrera – Universidad de La Laguna, Spain
Prof. Manuel Pereiro Cárceles – University of Valencia, Spain
Prof. David T. Karamanukyan – Siberian University, Russia
Prof. Maria Ioannidou – Queen Mary University of London, United Kingdom
Prof. Jacopo Martire, University of Bristol, United Kingdom
Prof. Avv. Ranieri Razzante – Università degli Studi di Bologna, Italy
Prof. Avv. Alessandra Sardù – Università degli Studi di Modena e Reggio Emilia, Italy
Prof. Hakeem Yusuf – University of Derby, United Kingdom
Ph.D. Avv. Livia Aulino – Università degli Studi di Napoli Federico II, Italy
Ph.D. Avv. Andrea D'Alessio – Università degli Studi di Teramo, Italy
Ph.D. Domenico Fauceglia, Università degli Studi di Roma Tor Vergata, Italy
Ph.D. Avv. Caterina del Federico – Alma Mater Studiorum Università di Bologna, Italy
Ph.D. Matteo Fermiglia – Hasselt University, Belgium
Ph.D. Avv. Paola Grimaldi – Università degli Studi della Campania Luigi Vanvitelli, Italy
Ph.D. Dorota Habrat – Uniwersytet Rzeszowski, Poland
Ph.D. Avv. Anita Mollo – Scuola Superiore Meridionale, Italy
Ph.D. Avv. Michael William Monterossi – Universität Luzern, Switzerland
Ph.D. Sara Saleri – Alma Mater Studiorum Università di Bologna, Italy
Ph.D. Hans Steege – Gottfried Wilhelm Leibniz Universität Hannover, Germany
Ph.D. Kamil Szpyt – Andrzej Frycz Modrzewski Krakow University, Poland
Ph.D. (c) Noel Armas Castilla – Universidad de Sevilla, Spain
Ph.D. (c) Alessandra Fabrocini – Sapienza Università di Roma, Italy
Ph.D. (c) Gabriela García Vera – Uniwersytet Rzeszowski, Poland
Ph.D. (c) Emanuele Garzia – Università degli Studi Suor Orsola Benincasa di Napoli, Italy
Ph.D. (c) Pablo Guédon – Université Jean Moulin Lyon 3, France
Ph.D. (c) Avv. Valeria Manzo – Università degli Studi della Campania Luigi Vanvitelli, Italy
Ph.D. (c) Marie Potus – Université Jean Moulin Lyon 3, France
Ph.D. (c) Michele Scotto di Carlo – Università degli Studi di Napoli Federico II, Italy
Ph.D. (c) Emiliano Troisi – Università degli Studi Suor Orsola Benincasa di Napoli, Italy
Ph.D. (c) Avv. Chiara Vitagliano – Università degli Studi di Napoli l'Orientale, Italy

pp.

Preface

UGO MATTEI - *The Death of Law: a talk by Ugo Mattei.* 8

Section I: Articles

LUCILLA GATT - *Legal anthropocentrism between nature and technology: the new vulnerability of human beings.* 15

ILARIA AMELIA CAGGIANO - *Protecting minors as technologically vulnerable persons through data protection: An analysis on the effectiveness of law.* 27

DIANORA POLETTI - *Gli intermediari dei dati / Data Intermediaries.* 45

MARIA ANTONIA CIOCIA – *Circolarità economica e trasparenza del prodotto / Economic circularity and product transparency.* 57

ROBERTO CARLEO - *Piattaforme digitali e contratto / Digital platforms and contracts.* 73

GIOVANNA D'ALFONSO - *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo" / The regime of liability from things in custody between traditional issues and 'algorithm liability'.* 82

ALESSIO DI AMATO AND VINCENZO ORSINI - *Beyond Bitcoin: Understanding Legal Boundaries of Blockchain Technology.* 110

JEREMY A. ANTIPPAS - *Civil liability and environmental protection: Italian-French looks.* 132

CARLOTTA DE MENECH – *Artificial Intelligence and Self-determination in Medical Field.* 164

EMILIANO TROISI – *Automated Decision Making and right to explanation. The right of access as ex post information.* 181

FEDERICO SERGIO – <i>Riflessioni sul diritto d'accesso agli atti tributari: la dialettica fra la tutela della privacy del contribuente ed il perseguimento dell'interesse fiscale dell'amministrazione finanziaria</i> <i>Considerations on the right of access to tax documents: the relationship between the protection of taxpayer's privacy and the pursuit of the tax administration's fiscal interests.</i>	203
REMO TREZZA – <i>Necro-robotica e circolazione dei dati personali post mortem</i> <i>Necro-robotics and post-mortem circulation of personal data.</i>	219
MARIANA MERIANI – <i>The fascinating theory of common ownership under the lens of competition law practitioners: any needs to rethink the antitrust toolbox?</i>	237

Section II: Focus paper

MARIA CRISTINA GAETA – <i>The regulation of certain aspects of autonomous driving in the Italian legal system.</i>	263
LUCILLA GATT, ILARIA A. CAGGIANO, LIVIA AULINO, EMILIANO TROISI, LUIGI IZZO, DAVIDE SILVIO D'ALOIA - <i>BCI devices and their capacity to express human will having legal value: A model of risk-based classification.</i>	289
LUCILLA GATT, ILARIA A. CAGGIANO, MARIA CRISTINA GAETA, ANNA ANITA MOLLO - <i>BCI devices and their legal compliance: A prototype tool for its evaluation and measurement.</i>	301
SERGIO GUIDA – <i>New machine behavior's evolutionary approaches between AI learning, control and ethics promoting cooperative Human-Machine Intelligence.</i>	315
MARIA GIORGIA CARACENI – <i>Digital surveillance technologies. Ethical, anthropological and political issues.</i>	336
CHIARA VITAGLIANO – <i>Potere di controllo datoriale: nuove tecnologie e tutela dei lavoratori nella società digitale</i> <i>Supervisory power of the employer: new technologies and worker protection in the digital society.</i>	350
IVANA GENESTRONE - <i>The importance of being aware when acting in a commercial world.</i>	365
List of authors	379

The Death of Law: a talk by Ugo Mattei

Summary: [1. Terminologia.](#) – [2. Controlli di razionalità: *Civil Law vs Common Law*.](#) – [3. Entrambi i controlli nel nostro diritto costituzionale.](#) – [4. Cosa intendo per "The Death of Law".](#) – [5. Cattura delle Istituzioni da parte dei poteri privati.](#) – [6. Partigianato.](#) – [7. Aggressione tecnologica.](#) – [8. Prendere o Lasciare!](#) – [9. Accumulo senza bisogno di leggi.](#) – [10. Anni di frontiera e di ritorno a casa.](#) – [11. Condizionalità in patria.](#) – [12. Codici QR O codici legali?](#) – [13. Vittime o complici?](#)

1. Terminologia.

La lingua inglese, per mancanza di sfumature terminologiche, non consente di dare un titolo più preciso a questo intervento. La maggior parte delle altre lingue della tradizione giuridica occidentale include la fondamentale dicotomia sviluppata dal diritto romano tra *ius* e *lex*. In spagnolo si parla di *derecho* e *ley*. In francese, *droit* e *loi*. In italiano, Diritto e Legge. In tedesco, *Recht* e *Gesetz*. In russo, *parvo* e *zako*. . . . Beh, l'idea è chiara. Il primo concetto – *ius* – è il diritto come principio di giustizia e racchiude la morale: qualcosa di retto, di giusto. Il concetto opposto – *lex* – nasce dall'idea di essere legati, con una corda o una catena, "obbligati" come nella nozione giuridica di obbligo; non c'è un giudizio di valore: *lex* è tale perché è vincolante (*dura lex sed lex*). Lo *ius* è il dominio dei giuristi, dove si discute con principi e razionalità; la *lex* è il dominio del potere coercitivo, quello delle manette e dell'incarcerazione dei poliziotti. Il titolo di questo intervento, "The Death of Law", allude al primo concetto.

2. Controlli di razionalità: *Civil Law vs Common Law*.

Nella tradizione giuridica occidentale, dopo una lunga evoluzione storica, i giuristi professionisti sono stati in grado di affermarsi non solo come ausilio necessario all'instaurazione del potere sovrano (bisognoso di una burocrazia ordinata), ma anche come controllo professionale del potere arbitrario. Questo è stato il tema del mio discorso di insediamento alla cattedra Fromm, pronunciato quasi 28 anni fa davanti a due colleghi che mi mancano ogni giorno di più: il professor Rudolf Schlesinger e l'allora nuova decana Mary Kay Kane. Il divario tra la tradizione di *civil law* e quella di *common law* si è incentrato sulle posizioni istituzionali di questi guardiani della razionalità del potere (e progressivamente della legalità e dei diritti diversi dalla proprietà). Nel sistema di *civil law*, gli oracoli erano professori; nel sistema di *common law* erano giudici. In entrambe le funzioni, i giuristi svolgevano il ruolo cruciale di controllo del potere arbitrario. Entrambi i circuiti hanno ora abdicato da questo ruolo.

3. Entrambi i controlli nel nostro diritto costituzionale.

I primi teorici espliciti di questo ruolo costituzionale furono i giuristi ugonotti, che fin dal XVI secolo si rifacevano al tirannicidio della tradizione del diritto costituzionale: quando il sovrano porta il popolo alla rovina c'è un diritto di resistenza che include l'uccisione. In Inghilterra, la Gloriosa Rivoluzione, con la sua concessione di un mandato ai giudici, dimostra l'importanza del potere giudiziario nel mantenimento di un equilibrio stabile tra la sovranità e il popolo (all'epoca, ovviamente, i detentori del diritto di proprietà). Grazie all'invenzione delle moderne scuole di legge nel 1870 da parte di Langdell ad Harvard (solo otto anni prima della UC Hastings), gli Stati Uniti sono diventati il primo paese in cui è stato istituito un potente controllo giudiziario e accademico sulla razionalità del potere. Questa potrebbe essere la ragione più importante dell'egemonia del diritto statunitense a partire dal secolo scorso.

4. Cosa intendo per “The Death of Law”.

Il crollo di questo equilibrio storico, che fonda sia l'ideologia sia la prassi dello Stato di diritto, è ciò che chiamo “*The Death of Law*”. Oggi, di fronte alle massicce violazioni e trasformazioni degli standard di decenza giuridica e costituzionali all'interno della tradizione giuridica occidentale, sia i circuiti accademici che giudiziari, hanno fallito. Rinunciando al controllo critico e razionale delle argomentazioni, schierandosi su linee partigiane all'interno di una narrativa di costante emergenza (dalla crisi climatica alla crisi generata dal COVID-19, arrivando alla guerra in Europa), i giuristi si trasformano nel controllo critico e razionale delle argomentazioni, schierandosi su linee partigiane all'interno di una narrativa di costante emergenza (dalla crisi climatica, al COVID-19, alla guerra in Europa), i giuristi si trasformano nel problema piuttosto che nella soluzione. Il risultato è il crollo della reputazione della tradizione giuridica occidentale e la probabile egemonia globale dei sistemi di controllo sociale non intaccati da quella che si riduce a una retorica ipocrita dei diritti. (Ho scritto un paio di articoli su sul vantaggio cinese in questo stato di cose, il secondo recentemente accettato dall'*American Journal of Comparative Law*).

5. Cattura delle istituzioni da parte dei poteri privati.

La prima forza letale che ha accelerato la morte del diritto è stata l'acquisizione da parte delle imprese delle istituzioni occidentali, un'acquisizione silenziosa che si è sviluppata nell'arco di due decenni, tra *The silent takeover* di Noreena Hertz (2001) e *Systemic corruption* di Camila Vergara (2020), due libri che vi raccomando caldamente. Non mi riferisco solo a alla cattura legislativa, ma anche alla presa di possesso di ogni apparato o potere ad impatto politico. Nel libro che ho scritto con Laura Nader, *Plunder: When of the rule of law is illegal* (2008), denunciavamo il movimento corporativo anti-legge che due anni più tardi, con *Citizens United v Fed. Election Commn.*

(2010), è stato incorporato nel diritto costituzionale statunitense.

6. Partigianato.

La partigianeria nella Corte Suprema degli Stati Uniti si è tolta i guanti con *Bush v Gore* (2000), e da allora si è confermata con voti di conferma strettamente di parte. Non ci sono principi più forti di questo: se posso farla franca, lo faccio!, un motto degli anni di Regan. Ciò che ha seguito questo declino della cultura istituzionale è la negazione di ogni principio della privacy che è emersa, su linee bipartisan, con l'annullamento della *Roe v Wade* (1973) (da parte dei conservatori) e le politiche aggressive e discriminatorie di vaccinazione obbligatoria dell'era-COVID (da parte dei liberali).

In entrambi i casi, la persona e il suo corpo non fungono da limite al potere politico delle corporazioni. In tutta l'impronta dell'influenza americana (Stati Uniti, Canada, Australia, Europa occidentale) l'aborto e la vaccinazione - a parte quando sono stati esaminati attraverso una discussione legale di principio sulla portata e sui limiti della scelta individuale - sono diventati un terreno paradossale per il confronto partitico arbitrario e di tifo da stadio. I conservatori radicalizzati: contro la privacy nell'aborto ma a favore della privacy nel mandato vaccinale. I liberali radicalizzati, che si sono schierati a favore della *Roe v Wade* ma hanno mostrato disprezzo per la privacy nelle questioni di vaccinazione in riverenza della scienza aziendale.

I conservatori che rifiutano con fervore i diritti delle donne per la libertà del proprio corpo; i liberali nell'ingenuità della scienza catturata dagli interessi del capitale.

Sia la destra che la sinistra negano la privacy e la logica nelle argomentazioni legali e politiche. *Dobbs v Jackson Women's Health Org.* (2022) rovina delle vite; l'assenza di Novak Djokovic agli US Open danneggia il tennis.

7. Aggressione tecnologica.

L'attacco letale al diritto – già indebolito dal movimento antigiusuriero che ha limitato i danni punitivi, ha reso difficile la certificazione di classe e ha frenato la tutela dei diritti grazie al ricorso ad una varietà di strategie alternative per la risoluzione della controversia – è derivato dalle abitudini tecnologiche apprese dai consumatori domestici oggettivate (conosciute) online come “big data”. La cattura delle istituzioni da parte dei poteri privati e lo Stato di sorveglianza, rapidamente sviluppati all'indomani del 9-11, si sono coniugati nel loro disprezzo per la privacy e per l'autonomia individuale, aprendo la strada all'inquietante *panopticon* in cui viviamo, denunciati da eroi che si sono immolati come Aaron Swartz, Julian Assange, Edward Snowden, Chelsea Manning e altri meno famosi.

8. Prendere o lasciare!

Cinque miliardi di esseri umani sono legati al telefono cellulare, la metà dei quali utilizza i social media. Il tempo medio giornaliero trascorso online è di oltre otto ore, più del sonno. Con questi numeri, che sono in aumento, Internet è diventato la frontiera dell'accumulazione capitalistica. Come le Americhe della prima modernità, chiunque raggiunga questo moderno *Far West* dell'accumulazione aziendale ne impara la logica nel modo più duro: è il proprietario della piattaforma a stabilire le regole. E l'utente deve accettare le regole: prendere o lasciare! Non sei d'accordo con le regole? Allora devi restare fuori. Provate ad accedere a *Facebook*, *Twitter*, *WhatsApp* o *Zoom* senza accettare le loro regole perché, ad esempio, siete preoccupati per la vostra privacy: non è possibile non potete entrare in nessun modo, per quanto importante sia la vostra transazione. Nessun consenso? Niente Zoom! Niente Zoom? Nessun accesso all'istruzione durante il lockdown. Anche un Presidente degli Stati Uniti deve accettare le regole di Twitter o essere bandito almeno per un poco di tempo.

9. Accumulo senza bisogno di leggi.

Prendere o lasciare è una logica *de facto*. Il contrario della legge. È anche conosciuta, nel gergo ipocrita del rapporto Nord-Sud tra potenti e impotenti, come "condizionalità". Un termine eufemistico per indicare il ricatto. Sulla frontiera di Internet (e questa è la principale differenza rispetto all'espansione coloniale) non c'è davvero bisogno di leggi per accumulare capitale. Algoritmi, *smart contract* e *firewall* sono più che sufficienti. Per la prima volta nella storia del capitalismo, la moltitudine di avvocati non è più necessaria. Possono coadiuvare e mantenere alcuni posti di lavoro per un po' di tempo, ma le fondamenta del capitalismo non ne hanno bisogno. La proprietà intellettuale è facilmente sconfitta dall'innovazione tecnologica. E la privacy su Internet, nonostante i tentativi europei come il Regolamento generale sulla protezione dei dati, è una finzione che ha fatto perdere prestigio al diritto.

Chi legge i moduli in un mondo in cui molti sono ansiosi di condividere con la rete i loro segreti intimi?

10. Anni di frontiera e di ritorno a casa.

Tutte le istituzioni capitalistiche di accumulazione sono state utilizzate alla frontiera prima di tornare in patria. La proprietà privata assoluta e la libertà universale di contratto (il dominio unico e dispotico) avevano bisogno di una terra vuota e genocida come laboratorio e, poiché lì si sono dimostrate molto efficienti, sono tornate in Europa. Le istituzioni medievali erano troppo dense di obblighi feudali, beni comuni e doveri collettivi per essere un terreno privilegiato per la sperimentazione di nuovi diritti e strutture di proprietà. Non è un caso che le prime corporazioni olandesi siano state sviluppate per fare affari sul mare *liberum*, per raggiungere nuove terre e saccheggiarle.

Solo dopo aver sperimentato con successo le frontiere del capitalismo, alle nuove istituzioni fu consentito di tornare e rivoluzionare il Vecchio Mondo.

11. Condizionalità in patria.

Con l'emergenza COVID-19 (e altri rischi che creano uno stato di emergenza permanente), le condizioni sono di un ritorno alla logica del "prendere o lasciare" nel mondo offline, che è sempre più difficile tenere separato da quello online nel metaverso del *panopticon*. Non ancora al centro, gli Stati Uniti, dove la cultura della privacy e dei diritti individuali potrebbe ancora reagire. Il trasferimento del *panopticon* condizionato, da Internet al mondo reale, necessita di una sperimentazione in paesi come Israele o l'Italia, dove dispositivi di controllo cinesi sono stati dichiarati obbligatori per la popolazione. Le informazioni sanitarie sensibili per la persona sono contenute in un QR Code che deve essere presentato e scansionato da parte di ristoratori, autisti di autobus, proprietari di strutture per l'esercizio fisico e persino nell'esercizio di strutture per l'esercizio fisico, e persino nell'esercizio di diritti fondamentali, quali recarsi a scuola o agli uffici postali o viaggiare in treno.

Una volta che un diritto è condizionato, cessa di essere: diritto. I controlli sono stati esternalizzati dalle aziende tecnologiche e dalle loro applicazioni.

12. Codici QR o codici legali?

È talmente più economico usare i codici QR piuttosto che la legge come processi di controllo tanto che c'è poca speranza che, sulla scia dei valori neoliberali, il diritto sopravviva ancora a lungo. I tribunali, le facoltà giuridiche, gli avvocati, i notai, i libri di giurisprudenza, i codici e i testi giuridici, le opinioni dissenzianti e le discussioni dottrinali sono sempre più percepiti come sprechi di tempo e denaro, inutili costi di transazione per l'accumulo di capitale. Le stesse funzioni di controllo sociale e di infrastruttura del capitale di controllo sociale e di infrastruttura del capitale possono essere garantite *de facto* da un'app, uno *smart contract* o dalla *blockchain* ad un costo molto inferiore. Perché passare attraverso un processo legale complicato se il vostro cliente non è in regola con il pagamento del *leasing* della sua auto, quando si può semplicemente evitare che l'auto si avvii tramite un programma intelligente a basso costo integrato nell'auto?

Si può fare molto di più per controllare il dissenso attraverso le applicazioni, come già visto in Cina e in Canada (quest'ultimo in occasione degli scioperi dei camionisti, bloccando i conti bancari dei manifestanti ripresi dalle telecamere intelligenti).

13. Vittime o complici?

Senza dubbio, gli avvocati sono professionalmente vulnerabili alla logica “*smart*”, poiché possono essere sostituiti a basso costo dall’automatizzazione, come già avviene nelle compagnie aeree, nelle banche e nelle grandi imprese di distribuzione. La nostra professione, tuttavia, può anche essere passiva, o addirittura complice, della propria scomparsa. L’opposizione professionale da parte della professione legale al suo triste stato di deterioramento è stata nel migliore dei casi inefficace e nel peggiore inesistente. Per motivi di pragmatismo o cinismo, i valori professionali non sono stati difesi. Forse perché il nostro progetto professionale non è più necessario per l’accumulazione del capitale, è più difficile difendere i valori giuridici nelle cittadelle del potere. Gli avvocati hanno solo il potere contrattuale limitato per sostenere i valori dell’integrità e della privacy, rispetto e uguaglianza nei loro servizi al capitale. In effetti, la capitolazione è stata frettolosa: il fascino dei paradigmi dell’economia neoliberale, delle tecnologie della comunicazione e dell’economia neoliberale, della tecnologia delle comunicazioni e delle scienze, ha fatto perdere l’anima al diritto. Per il diritto, rinunciare alla politica è suicidarsi.

Ugo Mattei
Full Professor of Private Law at Università di Torino
Emeritus Professor at University of California

SECTION I

ARTICLES



Legal anthropocentrism between nature and technology: the new vulnerability of human beings.

LUCILLA GATT 

Full Professor of Private Law - ReCEPL Director
Università degli Studi Suor Orsola Benincasa

Abstract

Reflection on the possible reform of the Italian Civil Code requires an analysis of the evolution of the relationship between subject and object of law in the legal systems of the Western area. From this perspective, we note the thrusts toward a recognition of legal subjectivity to nature, animals, but especially to devices endowed with AI. At the same time, on another side, strong tendencies toward objectification/reification of human beings (and animals) emerge, from their origin to the different stages of their development. Anthropocentrism implodes, heading toward a transhumanist drift that only an inclusive humanistic vision of every living being could stem.



Keywords: subject of rights; object of rights; anthropocentrism; legal personality/subjectivity; animals/plants; robots; civil code; novellatation; technology; human beings; objectivity /reification; vulnerability; limit; humanism.

Summary: [Introduction: The CODEX project and the prospects for the novellatation of civil codes in Europe.](#) – [1. Dichotomy between subject and object of law in the current code.](#) – [1.1. Expansion of the categories of subject and object of right in opposite directions.](#) – [2. Nature and natural goods: attribution of legal subjectivity and rights by public and private entities.](#) – [2.1. A critique of the movement for the 'subjectification' of natural goods.](#) – [3. Animals: failure to attribute legal subjectivity and enhancement of the status of object of rights.](#) – [4. Robots: attribution of legal subjectivity and citizenship.](#) – [5. Expansion of the legal objectivity of human \(embryos\) or human-related entities \(synthetic embryos\) as well as living entities, plant or animal.](#) – [Conclusion: Implosion of legal anthropocentrism and the sense of limitation.](#)

Introduction: The CODEX project and the prospects for the novellatation of civil codes in Europe.

The following reflections were expressed years ago at an important discussion of the academic community organized by Ugo Mattei at the University of Turin. For various and inexcusable reasons, they did not see the light of day, but the elapsed time does not seem to have erased their relevance, which - probably - has even increased due to further technological developments. The event from which this contribution draws is part of the broader cultural movement on the revision of the Civil Code.¹

During the days of debate and discussion, and on the strength of Ugo Mattei's solicitation, different positions emerged from those already existing in the Italian academic world on the possible revisions of the Civil Code. Conceptions similar to those that have inspired the novellatation of civil codes in other countries, such as Germany and, more recently, France, no longer appeared current. Instead, in Turin, the way has been opened to ideological reflection that can lead to a real change in the value paradigms underlying positive law choices.

If the theoretical, conceptual and categorical premises formulated during the

¹ It alludes to CODEX Conference - Ideologies and Techniques of the (re)codification of Private Law, 15-17 March 2018, carried out as part of 'Legacy,' i.e., the framework of study dedicated to the memory of Stefano Rodotà, organized by the International University College (of which Rodotà was president from 2008 to 2014) and the Collegio Carlo Alberto at the new headquarters of the University of Turin, under the supervision of prof. Ugo Mattei. Codex will be followed by Civitas, an in-depth study dedicated to the city between social public goods and common goods, according to the well-known taxonomy of the Rodotà Commission. See the Conference brochure to the link: <https://www.dirittieistituzioniphd.unito.it/avvisi/att/121h.allegato.pdf> The conference proceedings collection is available at this link: U Mattei (ed.), *Codex: Ideologie e Tecniche della (Ri) Codificazione del Diritto Privato* (2019) 25(1) The Cardozo Electronic Law Bulletin Review (free pdf https://www.academia.edu/40702536/Vol_25_1_Spring_Summer_2019_Codex_Ideologie_e_Tecniche_della_Ri_Codificazione_del_Diritto_Privato).

days of the Turin conference are to be translated into normative reality, it is necessary to move from thought to action and transform the scientific movement into a political movement, following the example of what Stefano Rodotà did in the past.

1. Dichotomy between subject and object of law in the current code.

This survey adopts a positive law perspective, setting aside broader considerations of philosophical rank. Let it be allowed only to highlight the questions that need to be answered in the effort to elaborate what might be new norms in Book I of the Italian Civil Code. Current legislation undoubtedly reveals a profound inadequacy with respect to the issues that affect both human beings and other living entities in the contemporary world: the gaps that exist today are now too wide and can no longer be ignored.

This perception was already present in Stefano Rodotà, who represents a scholar with the ability to see beyond and ahead because one of his recent works was to promote and edit, together with Paolo Zatti, the 'Treatise on Biolaw', a multi-volume work, including the one on the 'animal question' by Luigi Lombardi Vallauri, and others of fundamental importance such as the two volumes on the 'human body'. Already reading this treatise anticipates questions, anticipates answers, attempts to give guidelines that, today more than ever, deserve to be followed.

We are living what the Italian philosopher of law Enrico Giuseppe Opocher asserted: *'L'indissolubilità tra prospettiva filosofica e mondo dei valori trova la sua radice storica nell'umanesimo classico e più particolarmente in quella rivoluzione antropocentrica, per cui nell'Atene del V secolo a.C. l'uomo cessa di considerarsi come un piccolo anello dell'immensa trama del cosmo, sospinto ad ogni suo passo da una immanente necessità, e si pone arditamente al centro dell'universo, conscio della propria libertà creatrice e della forza oggettivante della sua ragione'*.²

So we are in the fifth century B.C., in the Sophistic revolution, and at that time we became the center of the world. This being at the center of the world, however, came with a very high price. A price that we are paying and that is immediately evident in the dichotomy present both in Book I of our Civil Code between ownership of the personal rights and legal capacity - a category in the process of being overcome as Giorgio Resta has pointed out³ - and in Book III in the definition of property as the object of right.

Thus, the Art 810 c.c. constitutes a rule of foundational value in the Italian legal system and in continental legal systems in general; the distinction between what is a *good*⁴ i.e., an object of law, and what is not, and what, consequently, should

² EG Opocher, *Lezioni di filosofia del diritto*, Padova, 2nd ed., 2000, 27; s. also A Pisanò, *Diritti deumanizzati. Animali, ambiente, generazioni future, specie umana* (Giuffrè Editore, 2012) 22.

³ G Resta, *Le persone, I soggetti, le formazioni sociali: note a margine del pensiero di Stefano Rodotà*, in Mattei (ed.), *Codex: Ideologie e Tecniche della (Ri) Codificazione del Diritto Privato*, cit. sub n 1, 8.

⁴ At present, however, there appears to be consensus on the idea that a good in the legal sense can be defined as any entity, material or immaterial, legally relevant, that is, capable of satisfying (human) interests assessed by the legal system as deserving protection (B Biondi, 'I beni', in *Trattato di diritto civile italiano* directed by F. Vassalli, (4) 1(2nd edn, Giappichelli 1995) 9; CM Bianca, *La proprietà, Diritto civile*, 6 (Giuffrè,

be a subject: it is a conceptual duality, there is no *tertium genus*; there is only the subject of right and the object of right.

Consequently, arguing that we need to eliminate the code is like saying that we need to eliminate the Constitution; in fact, it is necessary to remember that Codes come first, followed by the Constitutions, because the latter contains general declarations of rights that are, of course, very important, but in the day-to-day reality of application practice they play a completely different role than the Code.⁵

That being said, returning to the topic, it has to point out that at the state the distinction between the subject and object of law, as codified and as proclaimed by academic manuals in Italy, has been outlined by Alberto Trabucchi, in whose 'Istituzioni di diritto civile' it is given to read that 'all'uomo per legge suprema fu sottoposto il dominio del mondo esteriore' (page 527 of the 43rd edition, year 2007).

The idea that the object of law is everything that is not human, inasmuch as human being has dominion over everything other than himself, constitutes a traditional element that is now acquired and confirmed by articles 842 and 923 c.c. which sanction the reification of animal being but also the plant world.

On the other hand, however, the above mentioned distinction between human being as subject and all other entity as object no longer appears to be actual, since in the articles 1, 5, 11-14 c.c. the subjectivity of the natural person and also of the legal person is delineated and the last one is not existing, not tangible in real life, but it legally exists instead. In other words, in the Code text not only human beings but also other entities take place as subjects of rights.

1999) 49-50, 52, 54; F Bocchini, E Quadri, *Diritto privato* (4th edn, Giappichelli, 2011) 79. In case law, it has been clarified that if the interest that the entity satisfies is contrary to the law, it is not deserving of protection and the entity, which came into existence to satisfy an interest contrary to the law, is not and cannot be a legal good: the works that arose as a result of unauthorized allotment, inasmuch as its demolition is *ipso iure* presupposed by the system, cannot be objects of rights and are not, therefore, legal goods (s. Trib. Bari, 9 February 2005). The interest is identified with the content of the right that has the good as its object. More than one interest can be satisfied on the same good and, therefore, more than one right can exist on the same good (e.g.: think of the hypothesis of a land owned by Titius, object of the usufruct of Caius, leased to Mevius, on which Sempronius exercises a right of way (A Trabucchi, cit., 527). Similarly, it has been clarified that, since both public and private interests may concur on the same thing, the same thing can take on the configuration of different legal goods and be subject to a disciplinary regime that is both private and public (e.g., the so-called environmental goods for reasons of art, history or ecology: A Trabucchi, cit., 528 nt. 3; CM Bianca, cit., 51). The qualification of legal good is attributed by the legal system (legally or judicially); this qualification is independent of natural reality and does not consider the tangibility in the strict sense of what is identified as a legal good, being able to extend to anything, understood in the broadest and most abstract sense possible, which satisfies an interest worthy of protection of one or more subjects, private and/or public, who benefit from it, and this regardless of the utility in the economic sense that may derive from the use itself. Scholarly reflection has come to focus that they satisfy a (human) interest deserving of private and/or public protection and are, therefore, goods in the legal sense all 'things': patrimonial or non-patrimonial (e.g., life, liberty physical integrity, honor).

⁵ This should be kept in mind not only for those who are legal scientists but also for those who actually practice law and necessarily have to interpret it, because only the text of the code allows for a truly democratic interpretation as it is made widely by all legal professionals, while similar exegesis is not possible for constitutional text, interpreted by about 15 people.

1.1 Expansion of the categories of subject and object of right in opposite directions.

Instead, we are currently witnessing an expansion of legal subjectivity and legal objectivity, i.e. of the elements that are part of the category of subjects and the elements that are part of the category of objects; this is a two-way expansion, profoundly contradictory, which must be analysed for the purpose of formulating rules that are suitable for protecting the interests at stake.

What is happening is that on the one hand there is a tendency to subjectivise natural elements, and there is a strong movement for the recognition of a new legal status for the animal, but at the same time there is a strong tendency towards the *subjectivisation* of humanoid robots or in general of embodied algorithms that represent expressions of the highest levels of artificial intelligence, anthropomorphic machines that represent the pinnacle of anthropocentrism not only legal but philosophical and ontological in general, in the sense that everything that resembles man is supposed to become a legal subject.⁶

This tendency towards the *subjectivisation* of robots is very strong because there are movements headed by the strong economic interests of the companies that produce these machines, but above all, there is also a very strong academic movement headed by very well-known scholars from US and even Asian universities who, with a series of papers and conferences, are predicting and promoting the recognition of the legal personality of robots, which would not only penetrate human life on a massive scale in the next half-century, but would (in many respects, it is already a reality) establish emotional relationships with human beings, to the point of *institutionalising* relationships such as marriage or other kinds of relationships that all these anthropomorphic robots are ready to satisfy.⁷

The situation is very complex; it is a reality that we smile about but instead has a planetary spread, around which very strong economic interests revolve. Here, the so called 'rampant capitalism' finds its most obvious manifestation.⁸

2. Nature and natural goods: attribution of legal subjectivity and rights by public and private entities.

The contradiction that emerges from this view of legal anthropocentrism that is imploding is the tendency of some areas of the planet (the first ones are not from the Western area) to recognize natural goods (rivers, mountains, forests) as legal subjects, i.e., as subjects holding rights such as, for example, the right of

⁶ U Ruffolo, *Intelligenza artificiale e responsabilità* (Giuffrè Editore, 2018) who fully addresses the theme of the personification of machines together with that of their responsibility; MC Gaeta, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies* (ESI, 2019). See also at web context, D Alesso, 'Robot e A.I.: questioni di soggettività giuridica', [2018] *Cyber Laws*; S Carunchi, 'Robot e soggettività giuridica' [2018] *Fiscalfocus*; M Iaselli, 'Robot con intelligenza artificiale, verso una soggettività giuridica?', [2017] *Altalex*; C Trevisi., 'La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo' [2018] *Medialaws*.

⁷ Already years ago on the point s. L Gatt, 'Sub art. 810', in L. Gatt, S. Troiano (eds.), *Commentario al Libro III del Codice Civile, Collana I codici d'Autore, Commentario* directed by CM Bianca (Dike, 2014) 6-7.

⁸ U Mattei, L Nader, *Il saccheggio. Regime di legalità e trasformazioni globali* (Mondadori Bruno, 2010).

being protected from the destructive action of human beings. The reasons behind these positions are of different kinds and cover different areas, going from religious to ethics ones. They reflect the specific relationship between nature and humanity existing in some civilities/populations.⁹

This very recent phenomenon is also present in the Western area, but it is different from previous ones mentioned above in which the States are that recognized legal subjectivity; in this case, however, it is a private law entity - precisely: the Scottish JMT (John Muir Trust) Foundation¹⁰ - which has recognized the highest mountain in Scotland, the United Kingdom and the British Isles, the Ben Nevis, as having legal subjectivity, and so the right to remain wild as a place and therefore to be protected as such.

In Italy only at the beginning of this year (Constitutional Law Feb. 11, 2022 No. 1) were Articles 9 and 41 of the Constitution amended and the protection of the environment, biodiversity and ecosystems was introduced among the fundamental principles of our legal system. In 2001 (Constitutional Law Oct. 18, 2001 No. 3), we had merely established a reservation of State law on the environment (art. 117 Cost.). With the above mentioned 2022 constitutional reform, the State law reservation was extended to animals.

The question remains whether the latter choice was reasonable and actually protective. On the other hand, it resonates in a positive sense that the protection of biodiversity (that is, of the animal and plant worlds), has been established as a constitutional principle.

Anyway, the Italian choice does not go in the direction of attributing legal subjectivity to natural and/or animal entities but - more correctly in the opinion of the writer (s. furthermore) - goes in the direction of recognizing special protection of these realities that therefore remain objects but become inviolable in the interest of future generations.¹¹

2.1 A critique of the movement for the 'subjectification' of natural goods

The diffused trend of personhood attribution to nature should give pause for thought about whether the ownership of subjective rights and the recognition of personhood/legal personality to natural goods actually constitutes protection, as this puts them on a par with other private entities.

It has to ask if, in a hypothetical lawsuit filed by a company with an interest in establishing an industry at Ben Nevis, Ben Nevis would prevail. Wouldn't there

⁹ Cf. R Míguez Núñez, *Le avventure del soggetto. Contributo teorico-comparativo sulle nuove forme di soggettività giuridica* (Mimesis, 2018) and R Míguez Núñez, 'Una nuova frontiera della soggettività: i diritti degli enti naturali', available at: [Una nuova frontiera della soggettività: i diritti degli enti naturali \(lindiceonline.com\)](https://www.lindiceonline.com/it/articolo/una-nuova-frontiera-della-soggettivita-i-diritti-degli-enti-naturali). With regard to the initiatives of Ecuador and Bolivia s. also L Perra, 'L'affermazione giuridica dei diritti della natura', available to this link: <https://www.filodiritto.com/laffermazione-giuridica-dei-diritti-della-natura>

¹⁰ Cf. https://en.wikipedia.org/wiki/John_Muir_Trust

¹¹ Very interesting the article of MC Gaeta, 'Il problema della tutela giuridica della natura: un'analisi comparata tra Italia e Stati dell'America Latina' (2020) 4 Nuovo Diritto Civile, 313 – 343; more in details on the protection of future generation with regard to green technologies in transport sector M.C. Gaeta, 'Green and Sustainable Mobility in Road Transport. How Private Law Can Guarantee the Right Balance Between Environmentally Sustainable Development and Digital Transformation', *European Business Law Review*, Special Issue (forthcoming).

be better protection if instead States were more responsible and declared these natural areas protected independently of legal personality?

If we were to get out of this typically anthropocentric and Grotian-derived category of the subjectivization of law and of the legal personality (which, because of what has just been said, turn out in reality, to be a kind of double-edged sword) theoretically, States should protect certain goods as themselves, regardless of the attribution of subjectivity and parity to the legal subject intended as a human subject.

Another important point is that in the Ben Nevis case it is a private actor that recognizes legal personality to natural property. In this case, the court could also ridicule it and argue that there is no basis for this kind of operation; if, on the other hand, the courts recognize this power to private actors, it opens up important and 'disturbing' scenarios for the future.¹²

From this point of view, the Italian choice briefly described above, even with all its limitations, appears more supportable.

3. Animals: failure to attribute legal subjectivity and enhancement of the status of object of rights.

While we are seeing the recognition of legal personality to natural goods by some legal systems, especially non-European ones, the situation for animals appears more complex.

Indeed, there is a very strong academic movement pushing for an improvement in the legal status of animals¹³. Nonetheless, at the regulatory level, this recognition, or rather equalization between animals and humans in terms of legal subjectivity, has not yet happened, even in states such as Germany and Austria that have included animal protection at the constitutional level.¹⁴ The same consideration can be made for Italy and its recent constitutional reform. The recently introduced reservation of state law for the protection of animals in Article 9 of the Italian Constitution - as mentioned above - does not recognize the personhood of animals, which remain objects, but above all does not recognize their dignity as living beings to be placed on the same level as human beings.¹⁵

¹² About that s. the short but incisive consideration of the blog part of the research project 'Judges in Utopia. Judicial law-making in European private law', funded by the Netherlands Organisation for Scientific Research (NWO Vidi scheme). It aims to inform practitioners, policymakers, academics and law students of developments in European case law on private legal relationships, with a particular focus on the influence of fundamental rights and public policy. Particularly interesting the article titled '*Anthropocentrism in European Private Law and the Case of Ben Nevis*' available at this link: [Judges in Utopia: Anthropocentrism in European Private Law and the Case of Ben Nevis](#)

¹³ Citing some important scholars among others who have dealt with this issue, we can remember: Luigi Lombardi Vallauri, Luisella Battaglia, Francesca Rescigno, Diana Cerini, Margherita Pittalis and, first of all, Stefano Rodotà.

¹⁴ Similar choices have been made in Switzerland and India. In France in October 2013, a *bipartisan* appeal in favour of the animal cause was published by twenty-four intellectuals, calling for an amendment to the French *civil code* so that animals are no longer simply defined as 'things'. The state, according to the proposers, must finally recognise that they are 'living and sensitive beings'. These movements aim to bring Member States' laws into line with what has long been written in art. 13 of the Lisbon Treaty, which defines animals as 'sentient' beings.

¹⁵ L. Lombardi Vallauri, S. Castignone, '*La questione animale*', in Trattato di Biodiritto a cura di Stefano Rodotà e Paolo Zatti (Giuffrè, 2012), with particular regard to the chapter written by F. Rescigno, '*L'inserimento della dignità animale in Costituzione: uno scenario di fantadiritto?*', 267 ff.

At present, in Western legal systems, subjectification and thus the equating of animal being with sentient being has not yet fully taken place.¹⁶

In any case, the crucial point is that this equalization has not only not taken place, but, contrary to what is said and written by academics, right now the reification of the animal is reinforced by the use of new technologies. And, on closer inspection, a similar fate befalls the human being-as will be said in a moment.

4. Robots: attribution of legal subjectivity and citizenship.

Nature and animals are involved in this attempt to expand subjectivity, that is, by this attempt to equate them or, more or less, to make them close to the legal level of human beings. This trend is going slightly better for nature (although it is a double-edged sword, as mentioned above), but it is going significantly worse for animals.

What is going well, however, is the subjectification of robots. Just think of 'Sophia' a robot created by the Hong Kong Company Hanson Robotics, with advanced AI and, above all, with accentuated anthropomorphic features, which, just before the end of 2017 was declared a citizen of Saudi Arabia.

It is evident how this choice has first and foremost an economic significance: Saudi Arabia aspires to become a center for the development of artificial intelligence and the planetary scale realization of these so-called humanoid-robots devices.

This episode can be analyzed from several perspectives. On the socio-political level, the granting of citizenship to Sophia created a series of protests: women rebelled as well as migrants due to the fact that Saudi Arabia sent a very specific message by granting citizenship to a robot while it has not yet granted full subjectivity to women nor citizenship rights to migrants.

Secondly, and from a different perspective, it can be noted that Sophia's case and, more generally, the tendency to grant legal subjectivity to the robot is not isolated: the subjectivization of robots was already being talked about in 2006 in the United Kingdom where a study was commissioned by the government on what human society will be with the arrival of robots. Reading the report reveals a society in which robots are regarded as subjects like the humans with whom they mix and even have the same rights.¹⁷

Thirdly Europe, at the legislative level, is proposing regulation of artificial intelligence, including the anthropomorphic robots. The proposal for the Artificial Intelligence Regulation (AIA) of April 2021 has recently been accompanied by the proposal for a directive on liability for damage deriving from artificial intelligence

¹⁶ G Shyam, 'Is The Classification Of Animals As Property Consistent With Modern Community Attitudes?', (2018) 41(4) UNSWLawJl, 47; 1418, available at [Shyam, Geeta --- 'Is The Classification Of Animals As Property Consistent With Modern Community Attitudes?' \[2018\] UNSWLawJl 47; \(2018\) 41\(4\) UNSW Law Journal 1418 \(austlii.edu.au\)](#)

¹⁷ Reference is made to the Report 'Robo-rights: Utopian dream or rise of the machines?', the result of the study commissioned back in 2006 by the British government to the company Ipsos-MORI, Outsights and Institute for The Future, and in which it analyzes a scenario in which robots could enfranchise humans and lead a life as private citizens with all that comes with regard to the protections to be provided including social security(!). Cf. L Gatt, 'sub art. 810', in *Commentario al Libro III del Codice Civile*, n. 7.

systems (AI Liability Directive) of September 2022, aimed at establishing uniform rules for the access to information and the easing of the burden of proof in relation to the harm caused by AI systems, ensuring wider protection for victims (whether individuals or businesses) and promoting the AI sector through an increase of guarantees. But the most relevant act about the examined issue (the subjectivization of robots) is the resolution of the European Parliament of 16 February 2017 with recommendations to the Commission concerning civil law rules on robotics¹⁸ in which space is given to different approaches to the question of the complex attribution of liability for damage caused by a robot: from the application of strict liability institutions, to risk management, to the establishment of a compulsory insurance regime and, finally, the establishment of an ad hoc legal status: the *electronic personality*, which makes it possible to hold the most sophisticated robots accountable for their harmful actions.

In the end, it is therefore clearly seen how at the European level the scenario is decidedly still open and the tendencies¹⁹ to recognize full legal subjectivity to robots are decidedly consistent.²⁰

5. Expansion of the legal objectivity of human (embryos) or human-related entities (synthetic embryos) as well as living entities, plant or animal.

What is happening is incredible: while we try to subjectify robots, and - perhaps - nature, what instead is objectified/resined at the highest level are not only animals but also human beings in their initial stage of life: human embryos, ova, gametes are now at the mercy of any type of experimentation that generates subjects without genetic identity or with untraceable identities²¹.

¹⁸ Available at: [Texts adopted - Civil Law Rules on Robotics - Thursday, 16 February 2017 \(europa.eu\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0243)

¹⁹ Cf. a Symposia titled 'Regulating intelligence: the challenge of consciousness in new forms of life', 27th April 2018, Centre for Life, Newcastle upon Tyne. This symposium seeks to highlight the difficulties in the interplay between consciousness, responsibility, and liability, and attempt to provide a basis for developing workable legal definitions of consciousness that may be applicable in many fields of law. More precisely it deals of a research project 'Regulating the Tyrell Corporation: Company Law and the Emergence of Novel Beings'. Biotechnology and advances in AI promise the advent of new forms of life, maybe even 'conscious', reasoning creatures as intelligent and as sapient as Homo sapiens. Dr David Lawrence and Dr Sarah Morley have received funding from the Wellcome Trust to conduct a project of research into this area, with a specific focus on controlling companies' development of these beings via regulation. Through a number of events, as outlined below, a new network of expertise will be created in order to consider these future technological developments and suggest practical legal definitions for the status of both conscious and unconscious novel beings, in service of later developing and providing proposals for appropriate regulation for the responsible development, operation, and disposal of the technologies.

²⁰ Some reactions to the Parliament Resolution mentioned above: L. Berti, 'La responsabilità civile dei robot: dalla risoluzione del Parlamento Europeo all'art. 2043 c.c.' [2017], available at: <https://www.iusinitinere.it/responsabilita-civile-dei-robot-risoluzione-parlamento-europeo-art-2043-cc-6626>; D. Alesso, *Robot e AI: questioni di soggettività giuridica*, 2018, available at: <https://www.cyberlaws.it/2018/robot-e-ai-soggettivita-giuridica/>. See also, S Thanopulos and M La Torre, *Il Manifesto La soggettività e la responsabilità nel mondo dei 'robot'*, available at: <https://www.spiweb.it/cultura-e-societa/stampa/rassegna-stampa-2/rassegna-stampa-italiana/il-manifesto-11-ottobre-2019-la-soggettivita-e-la-responsabilita-nel-mondo-dei-robot-di-s-thanopulos-e-m-la-torre/>

²¹ But even when genetic identity is traceable, very complex scenarios open up, such as that of "embryo exchange" analysed by IA Caggiano, *Veridicità della filiazione ed errore nella procreazione assistita. Un rapporto possibile tra interpretazione della legge e studi empirici* (Pacini, 2018). Not to mention the very difficult compensation scenario resulting from malfunctioning medical artificial procreation facilities: cf. F. Di Lella, *Le attività pericolose nel settore bio-medico. Spunti per una rilettura dell'art. 2050 c.c.* (Pacini, 2020).

All this seems to be a contradiction and an implosion of juridical anthropocentrism.

Let's consider supernumerary embryos:²² in Italy they are still an unsolved problem. The Italian Ministry of Health with a decree of 2004 imposes their conservation indefinitely at a national central bank but it is doubtful that they are actually constantly transferred to this bank. An empirical analysis conducted in the public and private hospitals and similar structures of the Italian territory shows that health professionals often ignore this transfer obligation. In Italy, voices have emerged from the National Bioethics Committee (CNB) which have proposed making cryopreserved embryos adoptable but this proposal, however, has not yet been accepted.

What will be done with these supernumerary human embryos produced by medically assisted procreation? This is not known. Law No. 40 of 2004 banned experimentation on embryos but it is still done because this ban is not punished and there are no controls.

Currently gene editing operations are being done on human embryos, but the most serious thing is that we have *SHEEF* - 'Synthetic Human Entities with Embryo-like Features' - that is, artificially created embryos by assembling cells²³ that are not necessarily only human²⁴, so there are questions about what they are and how to regulate them. There are questions about whether to extend to them the regulatory status of human embryos, and there are doubts because there is no clarity about the nature of these new organisms.

On February 18, 2018, for the first time, a human-sheep hybrid embryo, in which one out of every 10,000 cells is human, was created in the laboratory to explant organs to be given to humans.

Case law had already reached the idea that if a good is functional to an unlawful interest²⁵ it is not a legal good: for example, think of unauthorized buildings. A year earlier an embryo of man and pig had been made for the same

In this context, the contract becomes the only instrument for protecting the individual: on this point see the important study by L. Valle, *Il contratto e la realizzazione dei diritti della persona* (Giappichelli, 2020).

²² The current legislation provides an ambiguous discipline in which the indicated elements are considered both as objects and as subjects of rights (see Articles 8, 9, 13 L. 40/2004). It is not easy to identify the boundary of the legal configuration and this leads to great uncertainties in terms of protection, especially in case of abuse by health professionals but also by those (would-be parents) who resort to the aforementioned techniques. The complexity of the problem was recently attested in the ruling of the EC Court of Justice, October 18, 2011, C-34/10, *Olivier Brüstle v. Greenpeace e. V.*, which, having to identify the scope of application of Directive 98/44/EC, ruled out the patentability of an invention if it requires the destruction of human embryos or their use as source material. The conclusion is even more interesting where attention is paid to the very broad notion of embryo elaborated by the Court, according to which it constitutes a 'human embryo' any human ovum from fertilization, any unfertilized human ovum into which the nucleus of a mature human cell has been implanted, and any unfertilized human ovum which, through parthenogenesis, has been induced to divide and develop. The decision appears, however, contradictory where it separates industrial and commercial purposes from research purposes, appearing to allow for the latter what is prohibited for the former.

²³ One very similar to a mouse embryo was recently described in *Science*, consisting of two types of stem cells supported by a three-dimensional 'scaffold.' In a report in *eLife*, scientists from Harvard Medical School discussed the criteria for testing these new entities, which, if they cannot be considered true embryos, might nevertheless in the future look very much like them and display some characteristics of sentient beings, for example, feeling pain. In essence, the researchers wonder whether it is reasonable to place the same research rules for these new entities as for human embryos generated by gamete fertilization.

²⁴ D Joy Riley, 'What Is a SHEEF, and Why Should We Care?', available at: <https://tennesseecbc.org/2017/04/28/what-is-a-sheef-and-why-should-we-care/>

²⁵ See above note n. 4.

purpose, now with sheep; this is contrary to the protection of animals, which are used and killed to explant organs: why should this not also be possible with human beings?

Cloning and hybridization are illegal in our legal system, but they are actually done everywhere in the world without relevant obstacles.

It can be seen, therefore, how the lack of control and the absence of shared regulation even at the European level has generated a structural vulnerability of human beings (but also of other living beings) in the face of technological applications that, currently, are capable, on the one hand, to artificially reproduce living beings of all species and to mix their genes without particular substantial limitations, and, on the other hand, favor the progressive affirmation of the non-living object; of the anthropomorphic artifice as a subject equated with the living subject, which results in a decay of the latter to the level of *object*. Not only SHEEFS but also synthetic human embryos (the so-called blastoids²⁶) enter the circuit of genetic modifications and experiments.

Similarly, the so-called organoids provoke a complex and at present unresolved series of ethical-legal reflections. They are in the midst of development in the name of personalized medicine and are proposed as a neutral solution to problems of cloning and hybridization or creation of synthetic embryos for research and experimentation aimed at the creation and marketing of new drugs. However, the organoid, as a human-derived entity, also presents legal problems of qualification, regulation and destination, and this particularly in the case of organoid masses or brain organoids with respect to which a delicate problem of identifying the level of consciousness arises. On the subject, jurists are silent while only moral philosophers question themselves²⁷.

This extremely dangerous circular process on the level of the preservation of human being as such, is now underway and aggravated by the trends of 'legal conformism'²⁸ that are widespread on a planetary level. This process appears, moreover, to be unstoppable and has generated an ontological vulnerability²⁹ of the living being (human and animal) in relation to technological evolution that now unequivocally presents a dark side that must be tackled with determination on the level of both strictly legal rules and strictly ethical rules. Although, in the writer's opinion, a proximity, if not even, where possible, an intersection of the two realms, would be desirable.

Conclusion: Implosion of legal anthropocentrism and the sense of limitation.

²⁶ DG Alberti, 'Embrioni umani sintetici/ Creati da cellule modificate: come funzionano e perché' available at: <https://www.ilsussidiario.net/news/embrioni-umani-sintetici-creati-da-cellule-modificate-come-funzionano-e-perche/2144917/>

²⁷ Cf. the presentation of F. Battaglia, *Do ethical issues regarding brain organoids rely on the metaphysics of the mind-brain identity theory?*, Seminars cycle "JM Chair PROTECH Debates "Studies on the legal aspects of medically assisted procreation and intersection between Ethics and Sciences - 14 April 2022, available at: <https://www.protech-jeanmonnet.eu/event/the-question-of-sheefs-synthetic-human-entities-with-embryo-like-features-and-similarities-what-are-the-new-forms-of-life-created-in-the-laboratory/>

²⁸ L. Gatt, *Problema dei minori senza identità genetica nei (vecchi e) nuovi modelli di famiglia: il conflitto tra ordine pubblico interno e c.d. ordine pubblico internazionale* (2017) 2 *Famiglia*, 271-272.

²⁹ The concept of human vulnerability in the technological environment has been analysed during the PROTECH- Jean Monnet Chair project activity: <https://www.protech-jeanmonnet.eu/>.

It is necessary to mention Hans Jonas, who belongs to a particular historical period such as that of Nazism, who already in a 'dramatic epoch of human history had long reflected on the relationship between ethics and technology, focusing lucidly on the problem of the limit [of human action], and who wrote in fact about acting in such a way that the consequences of one's actions are compatible with the survival of authentic human life on earth.³⁰

It appears to this writer that today Jonas's warning is not heeded at all and that this is leading to an irreversible loss of the centrality of the human being to the advantage of a transhumanist vision completely detached from any ethical substratum.

And, even more, it seems more persuasive in a modern eco-dynamic approach³¹ the position of those who speak³² of liberation from the now imploded anthropocentric paradigm must be married today, to promote a dialectic of humanism as a form of awareness of the limit that is inherent in every entity, event and process, including the human event. This means recognizing the common structure of finitude that every mortal shares. The process of emancipation cannot stop at gender, ethnicity, class. It will have some chance of being fulfilled only when it becomes a process shared with the animal and vegetable nature of which we are part and manifestation.

³⁰ H Jonas, *Das Prinzip Verantwortung. Versuch einer Ethik für die technologische Zivilisation*, Frankfurt/M., 1979, Translation ed. by PP Portinaro, Torino, 1990, 15.

³¹ P.P. Franzese, A. Riccio, A. Scopa, *Valutazione della sostenibilità ambientale: verso un approccio ecodinamico*, in *Biologi italiani*, 7/2003, 60, available at: [\(PDF\) VALUTAZIONE DELLA SOSTENIBILITÀ AMBIENTALE: VERSO UN APPROCCIO ECODINAMICO \(researchgate.net\)](#).

³² AG Biuso, *Dialettica dell'Umanesimo*, in *Liberazioni. Rivista di critica antispecista*, IX/ 34, 2018,26-37.



***Protecting minors as technologically vulnerable persons through data protection:
An analysis on the effectiveness of law.***

ILARIA AMELIA CAGGIANO 
Full professor of Private Law

Abstract

The article aims to address the issue of the protection of personal data regarding the only category of vulnerable subjects specifically provided by Regulation (EU) 2016/679 (GDPR): minors. Corresponding attention is dedicated to the Italian legislation (legislative decree 10 August 2018, n.101) enacted to adapt Italian law (the code regarding the protection of personal data referred to in legislative decree 30 June 2003, n. 196) to the GDPR.

I will analyze the provisions referred to minors (e.g., articles 8, 12 GDPR as well as art. 2-quinquies of Legislative Decree 2003/196), as well as the principles and rules provided in general terms, which indeed need to be tailored where applicable to the processing of personal data involving minors. Positive aspects as well as critical issues are highlighted in the light of effectiveness, that is to verify if the objectives set out by law (rectius ratio legis) are put in place through rules able to realize them.

With particular attention to privacy policies and effective application in digital contexts, the presentation aims to submit issues and proposals for solutions from both a de iure condito and de iure condendo perspective.

Keywords: minors; data protection; vulnerable people; effectiveness; regulation; GDPR.

Summary: [Introduction: Minors as vulnerable persons in the age of technology: a quest of data protection.](#) – [1. The data protection system as the controller's "tailor-made suit": principles of the GDPR applied to the processing of minors' data.](#) – [2. The rules of the GDPR for the protection of minors: the data controller – data subject relation.](#) – [3. GDPR and Italian rules: an assessment of adequacy and effectiveness.](#) – [3.1. The age threshold.](#) – [3.2. The exercise of parental responsibility.](#) – [3.3. Methods of verification.](#) – [Conclusion: The effectiveness assessment in light of the negotiation practice.](#)

Introduction: Minors as vulnerable persons in the age of technology: a quest of data protection. *

The issue of children's personal data protection must be tackled on a twofold level of understanding: one that looks at the children's needs to have their data protected, which are stated in specific rules; the other – a contextual one - that considers the domain of application of those rules, as the virtual environment¹.

In fact, this double level of analysis draws upon the awareness of the pitfalls posed by automation and artificial intelligence and the consequent needs of protection, in every area of human activity.

The notion of vulnerability that tends to be increasingly common in the social sciences and legal thought has been broadened in the last century and tend to move away from an exclusively ontological significance to embrace a relational one².

Vulnerability is no longer just the subjective category to qualify fragility of individuals: minors, people with disabilities, elderly, characterized by personal or life conditions, subjective characteristics (frailty, mental or physical infirmity) that make vulnerability a stable feature in different life contexts (the minor, the elderly, the immigrant, the incapacitated) - [subjective vulnerability].

It is also a *relational fragility*, related to the occasional relationship with an environment-as the technological environment- even if it does not necessarily permanently affect the individual's condition. We can all be vulnerable in a given context [relational vulnerability]. In this sense, vulnerability becomes a diffuse but abstractly reversible state, being possible to operate with a series of actions to

* I thank Emiliano Troisi for able assistance and correction of the draft of this work.

¹ This approach has been developed within the activities of Jean Monnet Chair PROTECH (on *European Protection of Individuals in relation to New Technologies* – prof. L. Gatt), online here <https://www.protech-jeanmonnet.eu>, 2019 - 22.

² In this sense, see P Stanzione, 'Data protection and vulnerability' (2020) 2 EJPLT 1, online here <http://www.ejplt.tatodpr.eu>; G Maltieri, J Niklas, 'Vulnerable data subjects' (2020) 37 CSLR 1. See also, P Corrias, E Piras, *I soggetti vulnerabili nell'economia, nel diritto e nelle istituzioni* (ESI 2021); L Didonai, *La vulnerabilità alla prova dell'argomentazione giuridica* (ESI 2021); C Faralli, 'Vulnerabilità e nuove tecnologie' (2019) 136 Politeia 5, 108; D Poletti, 'Vulnerabilità e atti personalissimi' (2020) DQP 11, 28; L Re, 'Introduzione: la vulnerabilità tra etica, politica e diritto', in MG Bernardini, B Casalini, O Giolo, L Re (eds.), *Vulnerabilità: etica, politica e diritto* (IF Press 2018); A Furia, S Zullo, *La vulnerabilità come metodo* (Carrocci Editore 2020).

get out of that environment³, or in any case not a necessarily permanent one.

Moreover, it is possible that the two conditions occur jointly, as is the case in minors, or, in a different sense, in the elderly. For the former ones, having regard to the technological vulnerability, digital nativity in the use of devices tends, in fact, to amplify the occasions of risks arising from an incomplete awareness of themselves and the world, as it occurs in childhood and adolescence. For the latter, technological illiteracy can be the cause of lack of access to services or goods, for which they are otherwise vulnerable to technology.

In this article, these two aspects of vulnerability will be considered, the one that looks at subjective notion and the other that looks at the relational notion, with regards to minors and their personal data.

Regulation (EU) 2016/679 – GDPR sees minors as the only category of vulnerable subjects specifically regulated whose ontological vulnerability increases in the technological world⁴.

This perspective is aimed at bringing out the actual protection needs for interpreting law.

1. The data protection system as the controller's "tailor-made suit": principles of the GDPR applied to the processing of minors' data.

Moving from the perspectives of analysis related to the levels of vulnerability, to the investigation of existing law, one must consider both the special rules provided in the case of processing concerning minors, and the general ones, which most likely impact or put minors at risk.

Indeed, any law organized by principles can differently affect the different classes of individuals subject to it.

Within this framework, the protection of fragile subjects (including minors) in the general data protection regulation cannot be entrusted exclusively to specific provisions (yet laid down to a minimal extent), but to the backbone of the regulation itself, general rules and principles, where emerges the principle of controller responsibility, a scheme that transfers the risk of choices to the organization.

It is, in fact, the *principle of accountability* of the data controller, which, by entrusting him or her with deciding the methods, guarantees and limits of the processing of personal data (i.e., the proactive behaviors that ensure compliance with the regulations), constitutes the fundamental safeguard for the protection of the interests of minors.

Thus, effective protection of children's data does not lie in the granting of special rights to the child involved, or to his or her representatives, according to the right-duty scheme (data subject - data controller relationship), but in the data controller's choices to adopt the most protective measures for data concerning children. Therefore, the data protection system, which the data controller chooses

³ It is therefore (in the proper sense) a potentially transient *quality*

⁴ Unlike the first meaning, relational vulnerability is not expressly indicated in the GDPR but it can be argued that it underlies the system and can be found in specific provisions (e.g. Article 22), if it is understood as a subjective projection of particularly risky activities.

to adopt, constitutes the first safeguard for the protection of minors.

The *accountability* principle governs a number of choices and activities of the controller that can affect the processing of minors' data.

First, one must take the case of processing involving automated decisions, as profiling. Under the GDPR, no preclusion of this type of processing is foreseen, not even in the case of processing of children's data, but, here, in addition to general requirements, there are mere recommendations to protect data subjects.

The GDPR recommends that decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects should not affect children (recital 71).

However, the non-binding nature of the recitals does impede risks for minors, as in case of *marketing* purposes.

In this regard, the guidelines adopted by the competent authority recommend that organizations should refrain from profiling *for marketing purposes*, in particular in the digital environment, due to the fact that « *children can be particularly susceptible in the online environment and more easily influenced by behavioural advertising. For example, in online gaming, profiling can be used to target players that the algorithm considers are more likely to spend money on the game as well as providing more personalized adverts* »⁵.

However, it must be pointed out that minor age and lack of maturity is relevant not only for the purchase of goods or services. Profiling may direct education, choices and behavior along the child's growth and identity formation process ⁶. Therefore, this risk should be kept in mind and weighed when undertaking profiling activities on minors for any purpose ⁷.

Protection of children in processing relies also in the principle of "*data protection by default and by design*" (Art. 25 GDPR), i.e., the need to design the processing by providing from the outset the essential safeguards "in order to meet the requirements" of the regulation and protect the rights of the data subjects. Implementation of this principle requires a prior analysis and an enforcement commitment on the part of data controllers through a series of specific and demonstrable activities such as pseudonymization, minimization, the possible

⁵ See, WP29 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018*, 31 (from which the quotation marks in the text corresponding to this note are taken), approved by the European Committee for the protection of personal data (EDPB). GDPR replaced the recommendations of Article 29 Data Protection Working Party (independent advisory body set up in accordance with Article 29 of Directive 95/46 / EC on the protection of personal data - "Working Party"), with the guidelines provided by the European Data Protection Committee, which play the role of proof of compliance with the Regulation. This role has been strengthened and confirmed in the changed framework in the event of company policies compliant with aforementioned guidelines (cons. 77 GDPR). With regard to the profiling provided for by the GDPR, WP 29 had clarified that since there was an express prohibition, the indications contained in the recitals could only be ascribed to a recommendation, not an absolute prohibition. The guidelines of WP 29 on profiling, as mentioned above, have been adopted by the European Committee.

⁶ In this sense, M Bianca, 'La filter bubble e il problema dell'identità digitale' (2019) 2 RDM, 1 ff.

⁷ With regard to the use of *social media*, EDPB, *Guidelines 8/2020 on the targeting of social media users*, 7: «*The potential adverse impact of targeting may be considerably greater where vulnerable categories of individuals are concerned, such as children. Targeting can influence the shaping of children's personal preferences and interests, ultimately affecting their autonomy and their right to development*». S., in addition, with regard to behavioral advertising, the WORKING GROUP WP 29, *Opinion 02/2013 on apps on smart devices* (27 feb 2013), sec. 3.10, p. 23, «*data controllers should not process children's data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing* ».

adoption of a certification mechanism, the very limitation of profiling. When it comes to processing concerning data of minors of age, this means to have the processing of children's data in mind from the beginning⁸, having regard, for example, to the transparency of the information according to the recipients of the information, calibrating the following elements: clarity, semantics, accessibility, contextuality, relevance, universal design, comprehensibility, multichannel presence.

Among *accountability* activities, are crucial those related to the *identification and management of the risks* inherent in the processing for the data subject. Risk is to be understood as the danger of negative impacts on the freedoms and rights of data subjects (recitals 75- 77); these impacts have to be analyzed through an appropriate assessment process (Art. 35-36) taking into account the known or apparent risks and the technical and organizational measures (including security measures) that the data controller considers it necessary to take to effectively mitigate them such. Risks to the rights and freedoms of natural persons include when personal data of vulnerable natural persons, especially minors, are processed (recital 75).

For this reason, when processing minors' data, one must consider to always carry out a data protection impact assessment, although not mandatory⁹, due to the fact that the processing of data of vulnerable subjects is a criterion for "increase in the imbalance of power between the data subjects and the data controller, an aspect which means that people may not be able to consent or oppose the processing of their data or to exercise their rights¹⁰.

2. The rules of the GDPR for the protection of minors: the data controller – data subject relation.

The need of protecting minors, as particularly fragile data subjects, appears in the GDPR through references and special provisions. It is specified (Recital 38) that: "*Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and*

⁸ EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* Adopted on 13 November 2019 focus on transparency in the case of children or other vulnerable individuals (p.14).

⁹ Article 35 *Data protection impact assessment* «1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks [...]».

¹⁰ In this sense, WP 29, *Guidelines 248 rev.01 2017* (explicitly approved by the EDPB): «*Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data)*. The WP29 identifies some specific criteria in this regard, including:

- Evaluation or scoring, including profiling;
- Automated-decision making with legal or similar significant effect;
- Data processed on a large scale
- Data concerning vulnerable data subjects (minors, mentally ill persons, asylum seekers, or the elderly, patients, etc.);

The DPIA is required if at least two of these criteria are met, but - taking into account the circumstances - the data controller can decide to conduct a DPIA even if only one of the above criteria is met. For the DPIA, the Italian DPA has adopted, by providing an Italian version, the *software* of the CNIL (French Authority), that can be freely downloaded from the site.

their rights in relation to the processing of personal data", but also, that such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

Within the GDPR, *three special rules* concern minors, however, as we have already seen, they do not exhaust the profiles that the data controller and the Authority must take into account when a minor is concerned¹¹. They affect the *direct relationships between the data controller and the data subject*, as for the information duties, the subject's consent, requests for deletion of the processed data.

More specifically, with regard to the information to be provided to the data subject, the Regulation requires that it must be communicated in a *concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child* (Art. 12). In this regard, it is clarified that *any information addressed to the public or to the data subject should be concise, easily accessible and easy to understand* (cons. 58).

Where consent is the legal basis for processing, such subsequent (to information) and possible authorization, is regulated with respect to minors only in the case of direct offerings of information society services, thereby highlighting how the European legislator had in mind the areas of greater operativity (and risk) for minors represented by the *digital environment*¹².

With respect to this rule, one can point out that the choice of identifying an age threshold as a requirement of capacity not only acknowledges the existence of a minor's online identity (which cannot be compressed)¹³, but also implements the need for a certain rule, which reduces litigation and favors the development of industry (unlike what would have allowed the introduction of a principle based on the capacity of discernment).

I will return to these aspects shortly, as they can be treated together along with some reflections on the regulatory choices made.

Finally, with regard to the rights of the data subject in the course of the processing, the interest of the minor as a binding request for protection is found in the discipline of the so-called right to be forgotten, according to which: «1. *The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: [...] f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)*» (Art. 17). In

¹¹ In addition to art. 57 already mentioned, *supra* nt. 4.

¹² Art. 8 states: «1. *Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years [...]*.

¹³ Referable to art. 13, paragraph 1, of the Convention on the Rights of the Child, which establishes for children «the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.».

this regard, the Regulation clarifies that the right to be forgotten of personal data no longer processed for which consent has been revoked or the right to object has been exercised « *That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.* » (Recital 65).

It is clear that this provision assumes that the minor might be not aware at the time of the consent about the consequences of his acting in the long run, but also that processing, and spread, of personal data over time can interfere with the digital identity of the minor (the representation *online* emerging from data and information that allow him to be identified) as an expression of his personal identity, that is his representation in social relationships¹⁴.

Also with regard to the *right to be forgotten*, the vulnerabilities that the legislator considers are in the pair: child (as placed in the) - technological environment.

The protection *ratio* underlying the right to be forgotten is that the information (affected by the erasure request) as historically outdated, therefore partial, inaccurate, substantially no longer true, may not represent the data subject and for this very reason may cause harm. In case of minors, there is also the risk that such data will insist on a personal identity in the making or on an identity of an adult who does not find (or does not want to rediscover) aspects of him/herself, as represented in the data processed. It then becomes necessary to provide for safeguards against any possible injury¹⁵.

As it is well known, the main contribution of the new regulation is certainly not represented by the right to the erasure of personal data, but by the standardization of a right to de-indexation¹⁶, which, however, appears to be mobile, and with a number of criticalities, highlighted by scholarly opinions and jurisprudence, mainly linked to the impossibility of hypothesizing a real

¹⁴ Lastly M Tampieri, 'L'identità personale: il nostro documento esistenziale' (2019) 4 EDP, 1195; F Scia, 'Riservatezza e oblio: diritti dei minori e servizi della società dell'informazione' (2019) 2 EJPLT, 16 ff., online version here <http://www.ejplt.tatodpr.eu>.

¹⁵ Cass., SS. UU., 22 July 2019, n. 19681 in the database *De jure* focused on the balance between the right to be forgotten and the right to report (*rectius* to historical re-enactment) by a newspaper, of a murder that took place twenty-seven years earlier, whose perpetrator had served the relative prison sentence and had re-entered positively in the social context: "in terms of the relationship between the right to privacy (in its particular connotation of the so-called right to be forgotten) and the right to historical re-enactment of facts and events concerning past events, the trial judge - without prejudice to the freedom of editorial choice in relation to this recall, which is an expression of the freedom of the press and information protected and guaranteed by art. 21 of the Constitution - has to assess the public, concrete and current interest in mentioning the identifying elements of the people who were protagonists of those facts and events. This mention must be considered lawful only if it refers to characters who in the present moment attract the interest of the community, both for reasons of notoriety and for the public role covered. Otherwise, the right of those concerned to privacy prevails over past events that hurt their dignity and honor and whose collective memory is now extinguished". For comments, *ex multis*: VMF Cocuccio, 'Deindicizzare per non censurare: il Ragionevole compromesso tra diritto all'oblio e diritto di cronaca' (2021) RCP 175; V Amendolagine 'Il diritto all'oblio tra rievocazione storiografica on line e cronaca giudiziaria' (2020) on GiustiziaCivile.com

¹⁶ The new form of the right to be forgotten includes the (old) right to erasure, together with the (new) right to de-indexation, the clarification of which goes back to the well-known Google Spain ruling (EU Court of Justice 13.5.2014, case C-131/12, in *Dir. Inf.*, 2014, 353 ss., As well as in *Foro it.*, 2014, IV, 295), and appears - timidly - reproduced by art. 17, par. 2, GDPR: "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.».

disappearance of the originally disseminated news, which ends up being persistently stored in web archives.

Therefore, not considering the oscillations on the content of the right to de-indexing in Court of Justice's case law, now broad,¹⁷ now with a more limited scope to the point of being considered a substantial step backwards on this point¹⁸, the mechanism provided by Article 17, i.e., of the recognition to the data subject of the right to erasure, may appear inadequate.

Probably, it could find more effective protection through an interpretation of the duty to erase (of the oldest information), in a perspective of effectiveness, as a positive duty to update information with obligations of greater dissemination than the old news, so to realize through this additional obligation the updating of the initially reported information.

3. GDPR and Italian rules: an assessment of adequacy and effectiveness.

On a more detailed level of analysis, it is worth noting to examine the special rule governing data processing of who is in a condition of subjective and relational vulnerability and its effectiveness: the rule on consent in the processing of data

¹⁷ As reported in the cd. Google Spain ruling: "The operator of a search engine is obliged to delete, from the list of results that appears following a search carried out starting from the name of a person, the links to web pages published by third parties and containing related information to this person, even if this name or such information is not previously or simultaneously deleted from the web pages in question, and this possibly even when their publication on such web pages is in itself lawful ", where the processing is not is more compliant.

¹⁸ CGUE, 24 sept 2019, C-507/17 (Google/CNIL) with comment by A Iannotti della Valle, 'Il diritto all'oblio "preso meno sul serio" alla luce della sentenza Google/CNIL della Corte di Giustizia dell'Unione europea' (2020) 2 AIC 495. According to that ruling, the operator of a search engine is not required to de-index in all versions of its search engine, being obliged to carry it out in the versions of that search engine corresponding to all Member States and to implement measures that discourage Internet users from having access, from one of the Member States, to the links in question contained in the non-EU versions of that engine.

The Court emphasizes that, in a globalized world, access by Internet users, in particular those located outside the Union, to the indexing of a link that refers to information concerning a person whose center of interest is located in the Union, can produce immediate and substantial effects on the person in question within the Union itself, which is why a worldwide de-indexing would fully achieve the protection objective pursued by Union law. However, it specifies that many third-party States do not recognize the right to de-index or in any case adopt a different approach to this right. The Court adds that the right to the protection of personal data is not an absolute prerogative, but must be considered in the light of its social function and must be reconciled with other fundamental rights, in compliance with the principle of proportionality. Furthermore, the balance between the right to respect for private life and the protection of personal data, on the one hand, and the freedom of information of Internet users, on the other, can vary considerably around the world. This approach, however, was deemed insufficient in terms of protection of the data subject in a stringent sense, where this protection is intended against the (potential) totality of network users: «it is true that typing google.com.br or google.co.jp will not be enough to display the results that would appear from Brazil or Japan, thus circumventing the limits imposed by territoriality. However, even if it is not enough to directly enter the URL of a different version of Google, with the use of a proxy server it is still very easy to view a site from Italy as if we were in Brazil or Japan, hypotheses that it has been possible to verify personally managing in a few minutes to view Google 'from abroad' while remaining in Italy. This means that it will always be possible, for those who are really interested in carrying out a 360-degree search on a person, to also trace the results for which the right to be forgotten has been recognized, [...] The protection would remain effective, therefore, only in front of the average user and not so interested at all in the search for information, which will make only a quick search on his local version of the search engine, without further deepening. On the other hand, the right to be forgotten would be ineffective for all those really interested in finding out who they are dealing with» (A Iannotti della Valle, 'Il diritto all'oblio "preso meno sul serio" alla luce della sentenza Google/CNIL della Corte di Giustizia dell'Unione europea' (n. 18).

of minors.¹⁹

By Italian law, art. 8 of the GDPR has been subject to adaptation and modification, according to the margins of intervention allowed by the European legislator, as represented by the following table.

Art. 8 GDPR <i>Conditions applicable to child's consent in relation to information society services</i>	Art. 2-quinquies (<i>Minor's consent in relation to information society services</i>), cod. privacy (<i>our translation</i>)
1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. 2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. 3. Paragraph 1 shall not affect the general contract law of Member	1. <i>In implementation of Article 8(1) of the Regulations, a child who is fourteen years old or older may consent to the processing of his or her personal data in connection with the direct provision of information society services. With respect to such services, the processing of personal data of a child under the age of fourteen, based on Article 6(1)(a) of the Regulations, is lawful on condition that it is given by the person exercising parental responsibility.</i> 2. <i>In connection with the direct offer to minors of the services referred to in paragraph 1, the data controller shall draw up in particularly clear and simple, concise and comprehensive language, easily accessible and understandable by the minor, in order to make the consent given by the minor meaningful, information and communications relating to the processing concerning the minor.</i>

¹⁹ In previous studies we have clarified the perspective of analysis based on evaluations of regulatory effectiveness (of the ability of legal norms to achieve their intended purposes) and effectiveness of protection. This evaluation criterion is also part of the approach that the European institutions (the Commission) have adopted in the *ex post* evaluation policies of better regulation, and in particular through the *Regulatory Fitness and Performance Program* (REFIT) which verifies, through a continuous and *evidence-based* process, the adequacy and effectiveness of the Union standard, to assess the adequacy of EU actions with respect to the objectives of the standards and the effective achievement of the same. The *ex post* evaluation criteria consist of: effectiveness (if the EU action has achieved its objectives); efficiency (what are the costs and benefits); relevance (if it responds to the needs of stakeholders); consistency (with respect to other actions); EU added value (what are the benefits of operating at EU level). This notion departs from the strict notion of effectiveness in sociology of law that equates effectiveness with legal compliance (recently in J Hahn, 'The Effectiveness of the Law', in *Foundations of a Sociology of Canon Law* (Springer, 2022), 179 -2022 https://doi.org/10.1007/978-3-031-01791-9_6). For a notion of effectiveness focused at the core of the problematics of legal consequence Leroy, 'The Concept of the Law's Effectiveness', in *Droit et société*, 2011/3 (No 79), 715-732. Available at: <https://www.cairn-int.info/journal-droit-et-societe1-2011-3-page-715.htm>.

States such as the rules on the validity, formation or effect of a contract in relation to a child.	

Technological vulnerability can be said to be taken into consideration as the rule limits the scope to information society services, as a context within which the minor operates more widely and freely, thus requiring greater protection.

The objective scope is in fact limited to online transactions, relating to contracts or services that are concluded or transmitted online, being aimed primarily at minors. Technological vulnerability is understood in a restrictive sense, looking at the moment of authorization for the provision of data and not also at the fact that the data, once collected, will be processed in a digital environment (which would make the rule - *a posteriori* - of general application).

In this regard, the European Data Protection Committee has clarified how the presence of an offer aimed at minors must be inferred from the statements of the controller/ professional or from an objective criterion, inferable from the substantial characteristics of the offer, such as the marketing plan.²⁰ This clarification leads to consider how, beyond the formal declarations, also the actual dissemination of an offer to the public (although not formally budgeted in the marketing plan, where easily detectable by the controller in the plan of his own market analyzes, and detectable by the Guarantor Authorities during their inspections also on the treatment registers) imposes specific obligations to adopt measures to protect the rights of the interested parties (art.25 GDPR).²¹

On the other hand, the processing of data conveyed by products that use advanced technologies and computerized data processing (e. g. smart toys), appears to fall within the scope of the rule, where the authorization to process data takes place online (as in the creation of ID profiles connected to the services provided by the products). This is a sector that deserves attention, to the extent that the use of smart toys involves effective digital surveillance profiles on the activities of the child, through continuous interaction with the robot, which, for its characteristics, is able to attract the child in numerous acts of daily life.²²

In the rule under examination, the protection mechanism adopted towards *vulnerable subjects / minors* is that to establish an age threshold for the autonomous consent of the minor, but only in the cases in which consent constitutes the legal basis for the processing of data, or the hypothesis referred to in art. 6, paragraph 1, letter a) of the GDPR, the age of the contractual consent being valid for the other hypotheses (arg. Ex art. 8 par. 3).

²⁰ «In this respect, if an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence (such as the content of the site or marketing plans) then the service will not be considered to be 'offered directly to a child' and Article 8 will not apply». [EDPB, Guidelines on consent 05/2020]

²¹ In this sense, it must be interpreted the provision of the Italian Data Protection Authority which in February 2021 ordered the blocking of the social network Tik Tok for disputes relating to the legal basis, not being clear the methods of ascertaining the age. On this point, Personal Data Protection Authority, prov. n. 20 of 22 January 2021 (web doc. 952419).

²² On the multiple risks of smart toys under legal, sociological and behavioral profiles, see the open access publication, S Chaudron, R Di Gioia, M Gemo, D Holloway, J Marsh, G Mascheroni, J Peter, D Yamada-Rice *Kaleidoscope on the Internet of Toys: Safety, security, privacy and societal insights*, EUR 28397 EN (Publications Office of the European Union, Luxembourg, 2016), JRC105061.

Therefore, the hypothesis of data acquired at the time of signing a sales contract or online service, of which the interested party is a party and whose processing is necessary for the execution or execution of pre-contractual measures adopted on request for the same (Article 6, paragraph 1, letter b) GDPR) is out of the scope of this article.²³

In other cases, the mere validity of a contract does not imply the lawfulness of unnecessary processing (e.g. for profiling, often not lawful as occurs in the most common social networks (see cons. 38), where there is no privacy consent regularly expressed, as with regard to the processing of particular categories of data²⁴.

3.1 The age threshold.

Art. 8 of the GDPR protects the *subjective and relational vulnerability of the minor* by requiring a prior consent mechanism, given by the holder of parental responsibility, when it concerns minors under the age of fourteen.

The national legislator has decided to lower the age threshold provided for by the GDPR, for reasons of systematic consistency with a series of national rules that recognize to those minors special capacity to carry out acts, including the legislation on cyberbullying and adoptions.

These are choices cannot be exempt from some criticisms in terms of systematic coherence, upon closer examination.

First, the rule that allows the ultra-fourteen-year-old child to request the removal of his/her data from the Internet manager on whose website they are published, to apply to the Guarantor Privacy Authority (Article 2, Law 71/2017) refers to a different protection rationale, in which the exercise of the right follows the harmful event that has already occurred (*ex post* protection).

Secondly, with regard to the regime of adoptions, the use of the *a maiori* argument, as a declination of the analogy, appears to be equally critical, where, in the case of authorization to process data, the choice, apparently less radical, but more complex to understand in its implications and dangers, can be not understood or even overlooked. The absence of salient stimuli is a problem that

²³ However, it should be noted that even if there is a case in which consent to the processing of data, connected to the execution of a contract is in any case required (e.g. sensitive data), it must be considered whether the data processing has been programmed by the controller as a condition for the execution of the contract even if it is not necessary. In this case, this will affect the requirement of the freedom of consent to the processing of data in a way affecting the validity of the processing (Article 7, paragraph 4, GDPR: In assessing whether the consent has been freely given, the utmost consideration is taken the possibility, among others, that the execution of a contract, including the provision of a service, is conditional on the provision of consent to the processing of personal data not necessary for the execution of this contract).

²⁴ With reference to the home automation sector, the main legal basis for the processing of personal data is represented by the execution of the purchase / supply contract of the home automation product / service concluded with the interested party, and in addition the consent for secondary uses or specific purposes not included in the first hypothesis, such as the processing of data of minors pursuant to art. 8, or profiling, in accordance with the EDPB Guidelines on online services, dated 9 April 2019, which specify that if you want to process the personal data of the interested party for purposes other than those strictly connected to the execution of the contract between the data controller and data subject, it is necessary that the controller, also taking into account the principles of lawfulness, correctness and transparency stated in art. 5, par. 1, and the principle of purpose specified in art. 5, par. 2, GDPR, identifies other bases of legitimacy, other than the contract. On this point, see L. Vizzoni, 'Dispositivi domotici e dati personali: dalle difficoltà applicative del GDPR alla prospettiva del futuro regolamento e-privacy, (2020), NGCC, 1032 ff.

also concerns informative self-determination of adults.

3.2 The exercise of parental responsibility.

Moreover, it should be considered the implementation of art. 8 GDPR in the national law, according to which: «*the processing of personal data of the minor under the age of fourteen [...] is lawful on condition that it is performed by the person exercising parental responsibility*. It provides for a substitution of the *incapable minor*, which seems to exceed the scope of derogation provided by the GDPR art. 8, limited to the age threshold, not also to the modalities of consensus for minors under- threshold «*Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years*» (art. 8, par. 1). The national choice of providing for the total replacement of the will of the minor is not justifiable even by virtue of the compatibility rule (not to prejudice the general provisions of the contract law of the Member States - par. 4)²⁵, for representing a limitation on the free exercise of a fundamental freedom, and as such, not compressible even in minors.²⁶

It therefore appears consistent to argue the disapplication of the national rule because of the provision of the regulatory rule, with regard the method of providing consent for the adolescent under the age of 14: authorization (as an alternative to the substitution) by the holder of parental responsibility, since it is a provision that is not in contrast with the general rules on contracts (Article 8, last paragraph, GDPR), applicable to unilateral acts, including those with non-patrimonial content.

Yet, pursuant to the general legislation of domestic law, prior listening to the minor (listening from 12 years or earlier where capable of discernment) must in any case be guaranteed (art. 315 *bis* c.c.). Therefore, this interpretation is consistent with the national legislation.

Such a regulatory system may be able to enhance the educational function of the parents in the construction of the personality of the minor, protagonist and / or participant in the acts he performs, without mortifying his decision-making freedom and the expression of personality in an intermediate regime between representation and autonomy.

Finally, in terms of applicability of the general legislation, it can be noted that the rules on the exercise of *parental responsibility* and the need for *mutual agreement* apply to the case in question, certainly in relation to issues of greatest interest, such as registration to websites or social networks, creation of personal

²⁵ A preventive control by authorization and not only by substitution (which is the rule of legal representation) had already been considered admissible in general in the Italian legal system by the most authoritative scholars, with reference to the action of the incapable, on the basis of a functional interpretation of the law on the legal representation of the minor which requires that the act fall within the sphere of control of the parent or guardian for protection needs, and which therefore can make this requirement satisfied even when the legal representative authorizes the act in advance. CM Bianca, *Diritto civile. La norma giuridica* (Giffrè, 2022) 238. Furthermore, in this case, the compatibility with an integrative and not substitutive intervention on the part of the operator of parental responsibility is justified by the relevance to the exercise of a right of personality.

²⁶ See art. 5 l. 22 dicembre 2017, n. 219.

accounts (316 e 337 *ter*, co. 3 c.c.)²⁷.

3.3 Methods of verification.

Art 8 GDPR, paragraph 2, requires the data controller *shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology*.

The rule, according to the regulatory technique of the GDPR for general principles and rules, in compliance with the technological neutrality clause (cons. 15), does not suggest particular methods of verification of the consent author. US legislation and experience have suggested a series of verification mechanisms: the use of a credit card that provides for a notification to its holder for each individual operation; the parent's connection with the app / program / platform staff via video conference; the verification of the parent's identity with an identity document²⁸, and, more recently, a matching system between a personal identification photo, for example that of the driving license, first verified through technological practices.²⁹

In this regard, arises the problem of reconciliation between the needs of identification and those of minimization in the use of data³⁰.

A very long-standing problem, which the European Commission has dealt with more recently, intending *to provide tools to clarify / support the application of the*

²⁷ Case law, so far, dealt with similar cases about the so called sharenting: the publication on social networks, by a parent or a third party, of images concerning minors' children, in cases of separation or divorce, where - among other things - in most cases the parents had included among the conditions of the separation / divorce agreement a mutual agreement for the publication of images

²⁸ According to Coppa § 312.5 (*Parental consent*). «[...] (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: (i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan; (ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iii) Having a parent call a toll-free telephone number staffed by trained personnel; (iv) Having a parent connect to trained personnel via video-conference; (v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or (vi) Provided that, an operator that does not "disclose" (as defined by §312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email».

²⁹ A. Astone, 'L' accesso dei minori d'età ai servizi della c.d. società dell'informazione: l'art. 8 del Reg. (UE) 2016/679 e i suoi riflessi sul codice per la protezione dei dati personali' (2019) 35(2) *CI* 614.

³⁰ EDPB *Guidelines on consent* 05/2020, concerned, like previous versions of WP29, of the minimization principle, provide that: «[135. Age verification should not lead to excessive data processing. The mechanism chosen to verify the age of a data subject should involve an assessment of the risk of the proposed processing. In some low-risk situations, it may be appropriate to require a new subscriber to a service to disclose their year of birth or to fill out a form stating they are (not) a minor.65 If doubts arise, the controller should review their age verification mechanisms in a given case and consider whether alternative checks are required 132. When providing information society services to children on the basis of consent, controllers will be expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities».

rules on data protection with respect to minors, referring to a Commission project on tools for age identification - pilot project for the demonstration of an interoperable technical infrastructure for the protection of minors, including age verification and parental consent. This is expected to support the implementation of child protection mechanisms based on existing EU legislation on child protection online³¹.

4. The effectiveness assessment in light of the negotiation practice.

In the aforementioned intervention by the European Commission relating to *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, the Commission intended to initiate an *ex post* analysis process of the impact of the GDPR, which is not part of the formal assessment and adequacy procedure (within the REFIT program³²), but which constitutes a functional analysis tool for an investigation of effectiveness - in the sense of functionalisation of the objectives - of the legislation.

Here, some critical points have been identified, at the end of the initial period of application.

With regard to the processing of minors, the problems were intercepted in the fragmentation of the transposition regulations, as well as in the exercise of the rights of the data subjects: « *As a result, there is still a degree of fragmentation which is notably due to the extensive use of facultative specification clauses. For instance, the difference between Member States in the age of children consent in relation to information society services creates uncertainty to children and their parents as to the application of their data protection rights in the Single Market. This fragmentation also creates challenges to conducting cross-border business, innovation, in particular as regards new technological developments and cybersecurity solutions. For the effective functioning of the internal market and to avoid unnecessary burden on companies, it is also essential that national legislation does not go beyond the margins set by the GDPR or introduces additional requirements when there is no margin.*

The Commission will [...] explore whether, in the light of further experience and relevant case-law, proposing possible future targeted amendments to certain provisions of the GDPR might be appropriate, regarding [...] the possible harmonisation of the age of children consent in relation to information society services.

The Board and data protection authorities are invited to: adopt further guidelines which are practical, easily understandable, and which provide clear answers and avoid ambiguities on issues related to the application of the GDPR, for example on processing children's data and data subject rights, including the exercise of the right of access and the right to erasure, consulting stakeholders

³¹ Communication from the Commission to the European Parliament and the Council *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM/2020/264 final of 24 June 2020 <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0264>

³² On the processes undertaken in 2019, see https://ec.europa.eu/info/files/eus-efforts-simplify-legislation-2019-annual-burden-survey_en

in the process».

In the communication, the Commission warns about the existence of different regulations in the single market and the impact of uncertainty on the development of the market, technological solutions and unitary procedures also for the purposes of cybersecurity.

Such in-depth analysis, conducted in the evaluation processes of European legislation, gives clues on the development of procedures and verification methods, especially to implement adjustments, also in light of national solutions.

In this perspective, the aim of the rules on this subject is to guarantee conditions for a conscious and responsible choice on the part of the data subject, which are the most critical elements in the child / adolescent, and which can be better guaranteed through methods of identification and parental authorization (in the sense of *ex ante protection*).

However, starting from the analysis of case law and *further experiences* (negotiation practices, application practices, which could escape the analysis of the dispute, but also studies), the crucial issues of protection of the minor cannot be connected only to the expression of informed consent, given the heuristics and cognitive biases underlying individual choices regarding the protection of personal data (*privacy dilemma, privacy paradox*)³³. Whilst, the main issue can be found in a broader control of the purposes and methods of use of such data.

In this regard, it is central a global assessment of the application of data protection legislation, starting from that of the general principles.

If we look at the negotiation practice, for example at the information of the most popular social networks with regard to messaging services among minors, it can be verified that in the communications of users, identification data (telephone number, device identifier, operating system version, app version, information on the platform, country code and mobile network code and marks for monitoring acceptance of the update are not stored and the chosen commands) as well as the metadata (times of use, functions used), are subject to processing and profiling for marketing purposes, also by third parties³⁴.

The video and music sharing applications, on the other hand, apart from the declared broader profiling and behavioral analysis based both on personal and usage data, and on all shared, uploaded and communicated contents, declare that they address individuals of not less than 13 years age, that not elaborate / intrusive verification mechanisms are envisaged, and refer to parental control systems for parents, relying on reports between users in any case³⁵. Even the

³³ See our, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo*, in ODCC, 2018, p. 67 ss.

³⁴ See. [www.whatsapp.com](https://www.whatsapp.com/privacy): WhatsApp Privacy Policy (last modified January 4, 2021)

³⁵ V. [www.tiktok.com](https://www.tiktok.com/legal/report/privacy) : Privacy Policy. Last update: July 2020. With regard to the treatment of minors: « TikTok is intended for users thirteen years of age and older. If your son or daughter is under the age of thirteen, please do not allow him or her to use the app. If you learn that your son or daughter under the age of thirteen has opened an account on TikTok, you can report it to us via the form at <https://www.tiktok.com/legal/report/privacy>. We will take appropriate action immediately. For more information about the proper way to use our app, please refer to our Terms of Service and Community Guidelines [...] We encourage you to maintain supervision over all of your children's Internet use, including the apps they may download. Both ... and ... provide parental control systems that allow you to block or restrict at the device level specific apps, features, videos, music, and more [...] Family Pairing is a feature that allows you to pair a parent's account with that of a teenage child. Once activated you can control from your account the Application Control functions of the paired account, including: Time Management: allows you to manage the time the child can spend daily on TikTok. Direct Messages: limits the users who can send

declarations of collaboration with the sector Authorities do not appear to have a decisive impact on the data protection models adopted³⁶.

For none of the services indicated above, there is any reference, in the information, to a limitation of the profiling of minors (even as suggested by the regulatory authorities)³⁷, or to techniques of anonymization or pseudo-anonymization, expressions of the application of the principle of *privacy by design*, having particular relief in the processing of personal data of minors. It is well known that anonymization of data is a precarious result, in the case of large volumes of data collected from a plurality of sources, given that the intersection of data allows a high possibility of re-identification of the interested, so that even the data relating to the location deemed anonymous may in fact not be, so the «*mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances*»³⁸. However, a serious application of regulatory instruments (including the techno-principle of *privacy by design*) at a system-level can certainly constitute an indication of potential effective data protection³⁹. The adoption of these techniques does not result from the information on the protection of personal data, nor from other elements obtainable from official communications⁴⁰.

These observations lead, as anticipated, to the need for a global assessment of the measures and programs of adaptation to European legislation, with specific regard to minors, by these giants of communication services. Simply referring to parental control systems or "*digital well-being*" options (daily time limitation option in the use of applications) does not appear to be sufficient⁴¹.

messages to the minor's account or disables the feature altogether. Please note: direct messages are automatically disabled for accounts belonging to users between the ages of 13 and 15. Restricted Mode: prevents the appearance of content that may not be suitable for everyone. To enable Family Pairing, you must be logged into the respective TikTok accounts on both devices. In Settings, tap on the Application Control section, then on Family Pairing: to pair the accounts and enable».

³⁶ In relation to the aforementioned provision, the company has undertaken to: guarantee the cancellation, within 48 hours, of the accounts reported and which result, upon verification, in the name of users under 13 years of age; strengthen the blocking mechanisms of the devices used by under-18-year-old users to try to access the platform; study and develop solutions, also based on artificial intelligence, which, in compliance with the regulations on the protection of personal data, allow to minimize the risk of children under 13 accessing the platform; launch new communication initiatives, in order to educate to a conscious and safe use of the platform and to remember that the platform is not suitable for an audience of under-12s; study and elaborate a new information created in simple language and with interactive and engaging methods dedicated to underage users; share with the Authority, data and information relating to the effectiveness of the various measures adopted, in order to collaborate in the identification and adoption of increasingly effective measures capable of containing the phenomenon.

³⁷ See. *supra* para. 2.

³⁸ EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, Adopted on 21 April 2020.

³⁹ Faced with large amounts of data within demographic groups, even the removal of sensitive data can be reconstructed by artificial intelligence algorithms.

⁴⁰ For a criticism of the (inadequate) compliance of the TikTok app with the personal data protection regulations, J Ausloos, V Verdodt, 'Confusing by design: a Data Protection Law Analysis of TikTok's Privacy Policy' [2021], available online at www.beuc.eu

⁴¹ In totalitarian systems, even the protection of minors passes through apparently similar instruments (the limitation of the times of use) but of totally different binding force and scope. See for example the rules of limitation of the time of use in China: Beijing released a regulation that requires children under 18 not to play from 22:00 to 8:00 and for more than 90 minutes continuously on weekdays, which become three hours in the weekends. With regard to online games, law no. 88 of 2009 (art.24, par.17) established that the concessionaires adopt or make available tools and measures for self-limitation or for self-exclusion from the game, the exclusion from access to the game by minors, as well as the display of the related prohibition in

On the other hand, these systems can formally and substantially prove to be useful, if they converge with parental training and awareness policies conducted at an institutional level, also taking into account the related educational tasks and surveillance duties that can lead to the discovery of fraudulent behavior by the parents (*fake profiles*) and the effective implementation of the limitations on usage times.

From the point of view of *ex post* protection, remedies are rarely available.

For example, the contract invalidating remedies (invalidation of the authorization) do not always appear suitable for protecting the data subjects' interests, although in principle applicable: take, for example, the strict interpretation of deception by the minor (Article 1426 of the Italian Civil Code), which could reasonably be configured only where verification mechanisms are sophisticated; the success in the restitution of the costs (when the service has been downloaded and used); or liquidation of damages (in case of fraud).

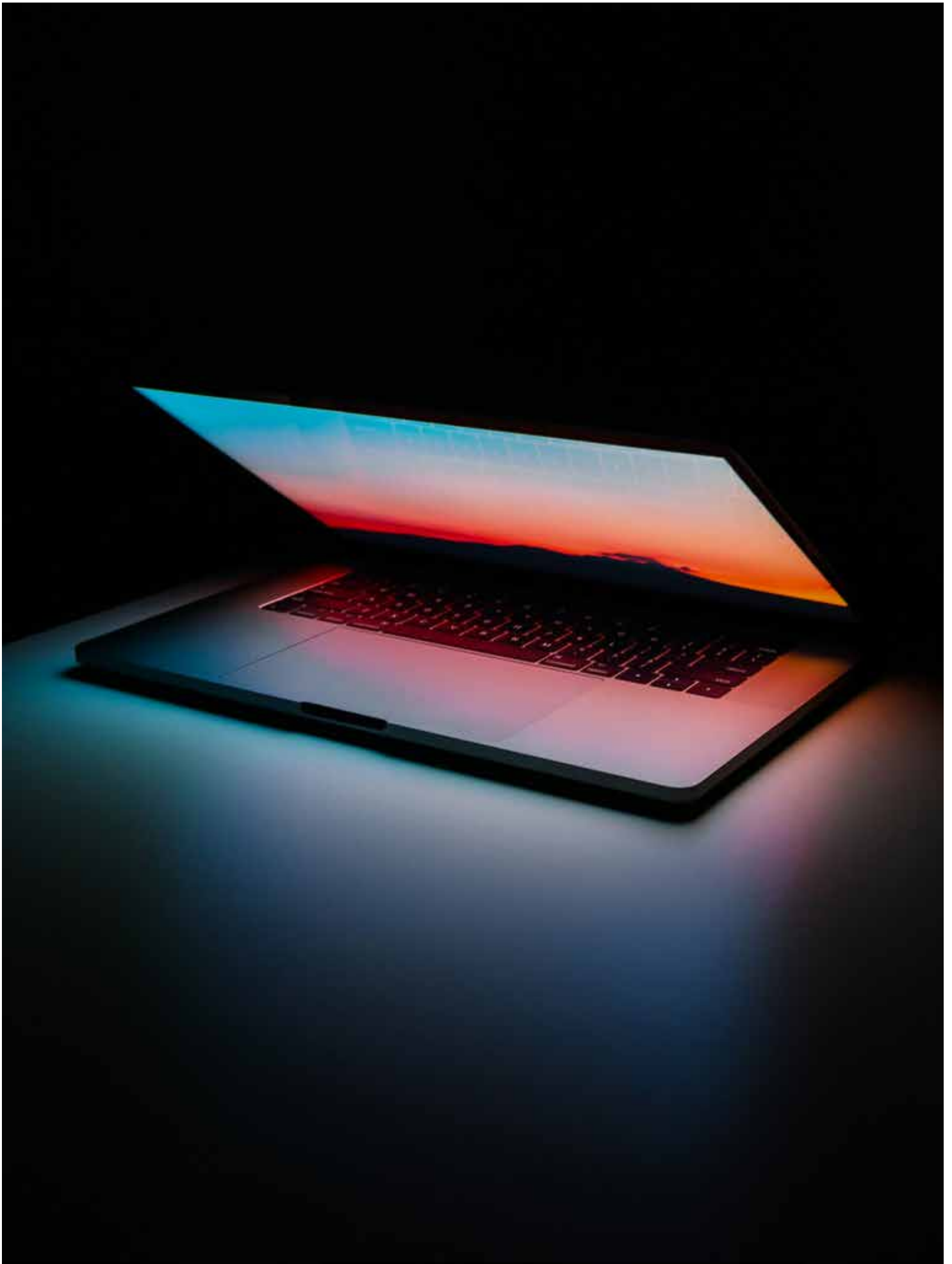
In case of damages, it can be difficult to link directly, in a causal relation, damages (moral or material) with the use of the social network, for affecting general sphere of human activity as the well-being or the training of minors.

Therefore, on a large scale, one should rely on an *ex-ante* (preventive) *protection*, in the sense of substantial *compliance* with all existing legislation (not limited to the rules on information and consent), combined with the administrative action to be part of the competent Authorities, whose role becomes increasingly central. These objectives must concern the communication industry through a concretely implemented *privacy by design* and that intercepts very specific *default options* in the case of goods (also aimed at minors).

In this gap, between the market and the protection of fundamental rights, lies the most important challenge of this age⁴².

a visible way in the virtual gaming environments managed by the licensee. Furthermore, through the so-called game account, a sort of mandatory self-limitation is made possible for the player, since at the time of opening the account he establishes his own weekly or monthly spending limits, with consequent inhibition of access to the system in case of reaching the predefined threshold. For players there is also the option of self-exclusion from the concessionaire's site, with consequent impediment to a new access. Moreover, through the game account registry, the activity of each player is monitored, as on opening the account the player must provide his tax code; the control system allows all transactions to be tracked and stored in a nominative way. <https://www.ilfattoquotidiano.it/2019/11/07/cina-contro-la-dipendenza-da-videogiochi-il-governo-impone-il-copri fuoco-per-i-minorenni/5552554/>

⁴² In this sense, there is the regulatory evolution that is affecting the regulation of communication platforms at European level (*Digital Service Package*) and which deserves a close connection and integrated vision in the light of the GDPR, together with the future regulation of artificial intelligence (Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (COM (2021) 206 final), which in turn takes up the regulation techniques of the GDPR (risk-based approach, sanctions).





Gli intermediari dei dati

Data Intermediaries

DIANORA POLETTI

Judge of the Italian Supreme Court of Cassation
Formerly Full Professor of Private Law at Università di Pisa

Abstract

La strategia europea sui dati ha quale fulcro la condivisione e la libera circolazione delle informazioni, anche personali. È chiara espressione del perseguimento di questo obiettivo il recente regolamento UE 2022/868/UE (Data Governance Act), che detta norme che riguardano il riutilizzo dei dati pubblici e che disciplinano l'attività degli intermediari dei dati. Il contributo offre una prima lettura di queste ultime norme del DGA, soffermandosi sul ruolo dei fornitori dei servizi di condivisione dei dati e sulla nuova figura del data holder, collocata all'interno di un "altro mercato" dei dati, che si intende regolare con obblighi di notifica preventiva e con altri adempimenti volti a scongiurare usi impropri dei dati trattati.

Sharing and free circulation of information, including personal one, is the core of the European Data Strategy. A clear expression of the pursuit of this goal is the recent Regulation (EU) 2022/868 (Data Governance Act), which contains rules affecting the reuse of public data and regulating the activities of data intermediaries. The paper offers a first reading of these latest DGA provisions, focusing on the role of data sharing service providers and on the new figure of the data holder, placed within an "other market" of data, meant to be regulated through prior notification requirements and other fulfillments aimed at avoiding misuse of processed data.

Keywords: GDPR; DGA; Data Protection; Data Governance; Data intermediaries; Data brokers; Data Act.

Summary: [Introduction: Dalla Data Protection alla Data Governance.](#) – [1. Gli obiettivi della Strategia europea sui dati.](#) – [2. L'attività di intermediazione dei dati nel Reg. \(UE\) 2022/868 \(Data Governance Act\).](#) – [3. La regolazione degli intermediari nell' "altro mercato" dei dati: Data Sharing Services Providers, Data Intermediaries e Data Cooperatives.](#) – [4. L'altruismo dei dati.](#) – [5. Gli infomediari dei dati tra positività e ambiguità.](#) – [Conclusions.](#)

Introduction: Dalla Data Protection alla Data Governance.

Il percorso iniziato con il Regolamento UE 2016/679 (GDPR) ha posto le basi per il futuro della *digital economy*, volta a spingere l'innovazione e a creare modelli di business non solo *data-driven* ma *data-based*.

Non stupisce che in un breve torno di anni il cambiamento di paradigma, riguardo ai dati, sia stato radicale, in ragione del loro incremento esponenziale¹, della loro crescente utilità anche per lo sviluppo dei sistemi di intelligenza artificiale, dell'elevato valore non solo economico delle aggregazioni di dati. Se la difficile conciliazione tra la protezione dei dati personali e la loro circolazione era l'obiettivo dichiarato del GDPR fin dal suo primo articolo (per vero già presente nella direttiva "madre"²), oggi l'accento è posto sul riutilizzo delle informazioni e sulla loro condivisione, tanto che l'espressione chiave è ormai "*data sharing*". Da qui, la necessaria considerazione della rete di relazioni che realizzano la circolazione delle informazioni e ne consentono lo sfruttamento e l'opportunità del loro governo, anzi, della loro *governance*³, che accomuna in un quadro unitario tipologie ben differenti di dati: quelli personali e quelli non personali, non sempre facilmente separabili e spesso accomunati in *set* di dati misti, che comprendono entrambe le tipologie⁴.

Il testo riproduce la relazione svolta al Convegno su "La circolazione dei dati personali: persona, contratto e mercato", organizzato dal Dipartimento di Ingegneria dell'impresa dell'Università degli studi di Tor Vergata il 25 marzo 2022, con qualche aggiornamento sul *Data Governance Act*, nel frattempo approvato nella sua versione definitiva. La pubblicazione mantiene il carattere colloquiale dell'intervento, limitando le note ad un corredo essenziale.

¹ Dati previsionali dell'UE stimano al 530% l'aumento del volume globale dei dati nell'anno 2025.

² Evidenzia V. RICCIUTO, *La patrimonializzazione dei dati personali*, in *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO E V. RICCIUTO, Torino, 2019, p. 28 ss., che la direttiva 96/45/CEE, unitamente ad un quadro normativo incentrato sulla tutela dell'integrità morale dell'individuo, non disconosceva la formazione e lo sviluppo di un mercato dei dati, considerati anche nella loro valenza patrimonialistica.

³ Sull'uso del termine "governance" sia consentito il rinvio a D. POLETTI, *A proposito di fonti nell'"ecosistema digitale"*, in *Principi, clausole generali, argomentazione e fonti del diritto*, a cura di F. RICCI, Milano, 2018, p. 345.

⁴ Ai dati non personali e alla loro libera circolazione – come noto – è dedicato il regolamento (UE) 2018/1807, il cui art. 2, punto 2, prevede che, qualora "un insieme di dati composto sia da dati personali che da dati non personali, il presente regolamento si applica alla parte dell'insieme contenente i dati non personali. Qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati, il presente regolamento lascia impregiudicata l'applicazione del regolamento (UE) 2016/679". Sulle varie tipologie di dati v. C. IRTI, *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in *Privacy and Data Protection in Software Services*, a cura di R. SENIGAGLIA, C. IRTI E A. BERNES, Springer, 2022, p. 49 ss.

L'Unione europea ha dunque preso atto della profonda trasformazione dell'economia e della preziosa miniera rappresentata dai dati, tanto da porre tra i suoi obiettivi la creazione di un mercato europeo unico, basato sul loro scambio massivo. Come ben sintetizzato nella Strategia europea in materia di dati del febbraio 2020, la Commissione si è impegnata ad avviare un'azione legislativa specifica avente a oggetto la creazione di “un autentico mercato unico di dati – aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore”⁵.

Uno dei fondamentali pilastri di questa strategia è il *Data Governance Act* (DGA), che mira a creare un quadro normativo per il processo di condivisione dei dati, personali e non. L'iter della proposta di regolamento, presentata il 25 novembre 2020⁶, ha subito una decisa accelerazione: nel dicembre 2021 Parlamento europeo e Consiglio hanno raggiunto un accordo provvisorio sul testo, che conteneva taluni aggiustamenti rispetto alla precedente stesura, preannunciando la votazione a breve della versione finale risultante dai negoziati interistituzionali. In effetti, già il 3 giugno 2022 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione europea il regolamento 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il reg. UE 2018/1724 (Regolamento sulla *governance* dei dati).

Anche se è previsto un differimento di quindici mesi per l'entrata in vigore del regolamento, secondo una tecnica già riscontrata in precedenti atti normativi, i tempi tutto sommato rapidi per la sua definitiva approvazione testimoniano l'intento dell'Unione Europea di essere protagonista nella *data economy*, con il baluardo della difesa dei diritti e la salvaguardia dei suoi valori.

L'ultimo tassello di tale mosaico, in ordine temporale, è rappresentato dalla proposta di regolamento del 23 febbraio 2022 (il c.d. *Data Act*)⁷, che detta regole armonizzate per il corretto accesso e uso dei dati (sia personali sia non personali) generati dall'uso dei prodotti connessi e dei servizi correlati. Come dichiarato dal Commissario per il Mercato interno, tale proposta si propone soprattutto di sbloccare una grande quantità di dati industriali e commerciali in Europa, rendendoli disponibili in primo luogo ai proprietari dei dispositivi connessi, alle aziende e, in circostanze eccezionali, agli enti governativi, così da allentare la presa che su queste tipologie di dati hanno alcune grandi realtà tecnologiche, in larga parte non europee.

1. Gli obiettivi della Strategia europea sui dati.

⁵ Commissione europea (2020), *A European strategy for data*, Comunicazione, https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf, p. 5.

⁶ Proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati del 25 novembre 2020, CPM (2020) 767 final.

⁷ Proposal for a Regulation on harmonised rules on fair access to and use of data, consultabile qui: <https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data>.

L'obiettivo dell'Unione è molto chiaro ed è espressamente dichiarato: generare valore dai dati e attraverso i dati, incrementando la loro circolazione e la loro condivisione attraverso l'aumento della fiducia negli intermediari dei dati.

L'incertezza giuridica legata alla frammentarietà del quadro normativo rappresenta un ostacolo all'efficiente sfruttamento delle potenzialità legate al riutilizzo dei dati e solleva profili critici per la sicurezza e la tutela dei diritti dei diversi soggetti coinvolti, a maggior ragione per la natura transfrontaliera della condivisione dei dati. Per promuovere l'innovazione e la creazione di modelli di business complementari basati sui dati è considerato indispensabile un ambiente legislativo altamente armonizzato, che definisca un modello europeo di condivisione dei dati con intermediari indipendenti da qualsiasi operatore che detenga un grado significativo di potere di mercato.

Questi interventi eurounionali non stanno creando in realtà un mercato dei dati, ma stanno regolando un mercato già operante, o, forse più precisamente, stanno aggiungendo un nuovo segmento a questo mercato, con inevitabili problemi di riconduzione dei soggetti economici già esistenti alle categorie di intermediari individuate dal DGA, di cui a breve si dirà. In questo mercato operano infatti non solo le *Big Tech*, il cui strapotere l'Unione intende arginare, ma attori economici già noti: i *data brokers*, che hanno costruito il loro modello economico proprio sulla circolazione dei dati, consentendo l'accesso alle società che ne sono prive tramite la previa acquisizione dei dati nell'infosfera, direttamente dall'interessato o facendosi trasferire da altre *data companies*, tramite l'impiego del diritto alla portabilità. Il prototipo è quello della società californiana Lumeria, importato venti anni dopo in Italia dalla società Hoda Srl con il celebre servizio Weople⁸, oggetto di attenzione dell'Autorità garante della concorrenza e del mercato (che a gennaio 2021 ha escluso, in merito a presunte pratiche concorrenziali denunciate da alcuni operatori economici, la necessità di compiere ulteriori accertamenti) e del Garante per la protezione dei dati personali italiano, che ha ritirato la richiesta di parere inoltrata al Comitato Europeo dei Garanti, nella consapevolezza che il caso coinvolgeva il più generale e delicato tema della commerciabilità dei dati personali.

In questo quadro, il DGA si propone di indirizzare l'evoluzione dell'attuale economia digitale tra le maglie di una *governance* generale europea, capace di offrire un approccio alternativo all'attuale modello commerciale delle grandi piattaforme tecnologiche integrate perché volto a generare meccanismi di funzionamento aperti e collaborativi dei servizi di condivisione dei dati e a prevedere, al contempo, "un accesso non discriminatorio all'economia dei dati per le imprese di tutte le dimensioni, in particolare le PMI e le start-up con mezzi finanziari, giuridici o amministrativi limitati"⁹.

2. L'attività di intermediazione dei dati nel Reg. (UE) 2022/868 (Data Governance Act).

⁸ Sul quale v. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa/Europa*, 2021, 215 ss.

⁹ Cfr. Il Considerando 27.

Il DGA, al quale solo si vogliono qui dedicare alcune considerazioni, pone anzitutto norme che riguardano il riutilizzo di determinati dati in possesso di pubbliche amministrazioni ed enti pubblici, che vanno a completare (anche se non sempre linearmente) la disciplina della direttiva 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione nel settore pubblico, da poco attuata nel diritto interno con il d. lgs. n. 200/21.

Di interesse in questa sede risultano le previsioni che mirano a disciplinare l'attività degli intermediari dei dati, ossia dei fornitori dei servizi di condivisione dei dati personali, il cui ruolo viene considerato essenziale dal legislatore eurounionale.

Preliminarmente si può evidenziare che il passaggio tra la versione del DGA del novembre 2020 e quella successivamente licenziata mostra un ripensamento dei colegislatori. L'EDPB aveva criticato il nuovo registro linguistico adottato dal legislatore europeo, che parlava di titolare dei dati invece di interessato (ric conducendo alla nozione di interessato il c.d. *data holder*) e la dottrina, in sede di primo commento, non aveva mancato di segnalare negativamente la nuova reificazione che la riemersione di una situazione di tipo dominicale portava con sé¹⁰.

La stesura ultima è più chiara al riguardo. Accanto al *data subject* (che è l'interessato come definito dal GDPR) si collocano i nuovi *data holders* (i "titolari dei dati"), ossia le persone giuridiche, compresi gli enti pubblici e le organizzazioni internazionali, o le persone fisiche diverse dagli interessati rispetto agli specifici dati in questione, che hanno il diritto di concedere l'accesso o di condividere dati personali e non personali. I *data users* o "utenti dei dati" sono definiti come le persone fisiche o giuridiche che hanno accesso legittimo a determinati dati personali o non personali e che hanno diritto, anche a norma del GDPR in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali (art. 2, n. 8 e n. 9).

La definizione del servizio di intermediazione dei dati è affidata all'art. 2, n. 11 ("un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali") che riassume le tipologie di intermediari con le quali si apre il capo III del Data Governance Act.

Tre sono queste tipologie.

Alla prima appartengono i "servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi; tali servizi possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati, nonché l'istituzione di altra infrastruttura specifica per l'interconnessione di titolari dei dati con gli utenti dei dati". Si tratta di una tipologia che ricalca il modello dei *data marketplaces* e ad

¹⁰ F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., specie p. 240: "si noti che non viene introdotta solo una novità prettamente terminologica: si usano concetti che spostano l'attenzione sulla commercializzazione dei dati personali, spingendo verso una reificazione dei dati al fine di favorire la creazione di mercati alternativi rispetto a quelli creati dai *Big Tech*".

essa si addice il riferimento al carattere mercantile della condivisione che compare nella definizione di servizi di intermediazione, in cui la condivisione è prodromica alla sempre più libera circolazione. Questi fornitori di servizi di *data sharing* dovrebbero ridurre i costi di transazione, combinando le fonti di dati e mettendo in contatto utenti e fornitori. Dalla definizione restano esclusi gli operatori che raccolgono dati da fonti esterne per offrire servizi, senza stabilire un rapporto diretto tra titolari e utenti dei dati.

Se la prima tipologia riguarda il rapporto titolari dei dati-utenti dei dati, la seconda ha sostanzialmente ad oggetto la relazione tra interessato e utente dei dati. La categoria è quella dei fornitori dei “servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679”. Essa comprende i fornitori che offrono i loro servizi agli interessati, che non dovrebbero elaborare o aggiungere valore ai dati, ma hanno lo scopo di rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano. Tali fornitori assistono i singoli individui nell'esercizio dei loro diritti a norma del GDPR: ad essi compete la possibilità di gestire la concessione e la revoca del consenso al trattamento dei dati, nonché l'esercizio dei diritti riconosciuti dal regolamento. In tale contesto, è importante che il modello commerciale di tali fornitori garantisca che non vi siano incentivi disallineati che incoraggino i singoli individui a utilizzare tali servizi per mettere a disposizione più dati che li riguardano di quanto non sia nel loro stesso interesse. Tra i prestatori dei servizi e gli interessati pare sussistere un rapporto giuridico di natura fiduciaria a cui si ricollega l'obbligo per i primi di agire nel migliore interesse dei secondi, garantendo che i dati trattati non vengano utilizzati per scopi diversi o illeciti. Ad una prima considerazione, non è dato capire se questo tipo di organizzazioni coincida con (o piuttosto inglobi) i sistemi di gestione delle informazioni (i c.d. PIMS, *Personal Information Management Systems*), che consentono agli interessati di gestire i propri dati personali in sistemi di archiviazione sicuri, in locale o online e di condividerli quando desiderano e con parti da loro ritenute affidabili, creando “spazi” per i dati personali, già oggetto di attenzione dell'Opinion 9/2016 dell'*European Data Protection Board*.

La terza tipologia è rappresentata dai servizi di cooperative di dati. Ai sensi del considerando 31 DGA, le cooperative di dati mirano anch'esse a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati. Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali, microimprese e piccole e medie imprese che in termini di conoscenze in materia di condivisione dei dati sono spesso equiparabili ai singoli individui¹¹. Anche queste organizzazioni (costituite da interessati, da imprese

¹¹Le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle

individuali o da piccole o medie imprese) hanno come obiettivo principale quello di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, specie per quanto riguarda il compimento di scelte informate prima di acconsentire al trattamento dei dati.

Il mercato dell'intermediazione e dell'infomediazione sembra tracciato con certo nitore. Al di là degli infomediari che offrono servizi di supporto agli interessati, anche con l'offerta di consulenza, la condivisione di dati può infatti avvenire tra due imprese, come pure fra impresa e consumatore, come si legge espressamente nel considerando 32 del DGA. La scomparsa del riferimento "con riguardo alla remunerazione in qualsiasi forma", riferito alla condivisione, che compariva nel testo precedente, non esime dalla constatazione che si stanno ponendo ulteriori premesse per la monetizzazione dei dati¹² e che, nonostante il riferito chiarimento sui *data holders*, sia in corso una spinta verso la "proprietarizzazione" dei dati, come dimostra – tra l'altro – il riferimento alla possibilità di recupero degli stessi in caso di insolvenza del fornitore (art. 12, lett. h).

3. La regolazione degli intermediari nell' "altro mercato" dei dati: Data Sharing Services Providers, Data Intermediaries e Data Cooperatives.

Il DGA mira a regolare i servizi di intermediazione dei dati introducendo meccanismi di controllo che fanno a meno dell'autorizzazione, pure propugnata come regime meno blando dai garanti europei¹³, per propendere verso un sistema di notifica obbligatorio all'autorità competente nazionale e una serie di obblighi e requisiti posti in capo ai fornitori di servizi di condivisione di dati, volti a scongiurare un uso improprio dei dati trattati. A titolo esemplificativo, il fornitore deve garantire un elevato livello di sicurezza e mettere in atto procedure di natura preventiva per scoraggiare pratiche abusive o fraudolente, agendo nell'interesse superiore degli interessati nell'esercizio dei loro diritti¹⁴.

La *ratio* ispiratrice della disciplina è quella di garantire il ruolo neutrale degli intermediari in questione rispetto ai dati scambiati tra gli utenti, realizzando una separazione anche strutturale del modello organizzativo dell'attività di impresa. Neutralità, esclusività dello scopo e segregazione sono dunque gli strumenti cui è affidato il controllo dell'attività di intermediazione, di competenza di una nuova autorità Garante (il Comitato europeo per l'innovazione in materia di dati e le propaggini delle singole unità nazionali), con inevitabili problemi di

posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi (dal considerando 31).

¹² G. CERRINA FERONI, *Luci e ombre della Data Strategy europea*, in www.agendadigitale.eu, 12 maggio 2022.

¹³ Cfr. il parere congiunto del Comitato europeo per la protezione dei dati e del Garante europeo per la protezione dei dati n. 3/2021 sulla Proposta di regolamento del Parlamento e del Consiglio relativo alla governance europea dei dati, p. 37.

¹⁴ Per una prima riflessione cfr. CAUSARANO, *Intermediari di dati e Blockchain: luci e ombre nel prisma della tutela dei dati personali*, in *Il potere della tecnica e la funzione del diritto. Un'analisi interdisciplinare di Blockchain*, a cura di E. NAVARRETTA, L. RICCI E A. VALLINI, I, Torino, 2021, p. 179 ss. e, volendo, D. POLETTI, *La Blockchain tra controllo e "commercializzazione" dei dati personali*, *ivi*, p. 161 ss.

coordinamento tra le molteplici *authorities* che ormai popolano lo scenario dei dati e del loro trattamento, inteso in senso lato.

Emerge da questi sviluppi normativi una nozione di circolazione del dato in senso tutt'altro che connotato da negatività. Negli intenti del legislatore unionale, la nuova *governance* europea dei dati incentrata sugli intermediari, configurati come soggetti indipendenti tanto dai titolari dei dati quanto dagli utenti dei dati, potrà facilitare l'emergere di ecosistemi basati sui dati affidabili e agevolmente fruibili.

4. L'altruismo dei dati.

Il DGA si spinge inoltre ad ipotizzare una circolazione dei dati in ottica altruistica.

Il capo IV della proposta è finalizzato proprio ad agevolare l'altruismo dei dati, fenomeno sino ad oggi piuttosto trascurato, eppure di grande interesse per gli studiosi, perché introduce, nella circolazione dei dati, una logica sostanzialmente donativa. Si tratta di dati messi a disposizione su base volontaria (tramite il consenso, dunque) da parte degli interessati o di dati non personali messi a disposizione da parte dei titolari dei dati *per scopi di interesse generale*, come la tutela della salute pubblica, la mobilità, la lotta al cambiamento climatico, ma anche la statistica ufficiale, la ricerca scientifica o il miglioramento dei servizi pubblici. Il DGA si occupa di dettare i requisiti che devono essere posseduti dalle organizzazioni dedicate all'altruismo dei dati, che dovranno operare mediante una struttura giuridicamente indipendente, anche in questo caso separatamente dalle altre attività che l'ente abbia intrapreso.

In luogo dell'apparato di notifiche, viene istituita la possibilità per le organizzazioni che praticano l'altruismo dei dati di registrarsi in qualità di "organizzazioni per l'altruismo dei dati riconosciute nell'UE", purché soddisfino una serie di requisiti, al fine di accrescere la fiducia nelle loro attività. Tali organizzazioni saranno soggette ad una serie di obblighi di trasparenza. Sarà inoltre sviluppato un modulo europeo comune di consenso all'altruismo dei dati per ridurre i costi della raccolta dei consensi e facilitare la portabilità dei dati.

Come chiarito dal Considerando 46, agli Stati membri è lasciata la previsione di ulteriori tutele, che dovrebbero comprendere la possibilità di trattare i dati pertinenti in un ambiente di trattamento sicuro gestito dalle organizzazioni riconosciute per l'altruismo dei dati, meccanismi di sorveglianza quali consigli o comitati etici, compresi i rappresentanti della società civile, per garantire che il titolare del trattamento mantenga standard elevati di etica scientifica e di protezione dei diritti fondamentali, strumenti tecnici efficaci e comunicati con chiarezza per revocare o modificare il consenso in qualsiasi momento.

La circolazione in chiave positiva dei dati può dunque diventare circolazione in ottica altruistica, solidaristica, sostanzialmente *not for profit* (requisito che devono possedere gli enti "altruistici").

5. Gli infomediari dei dati tra positività e ambiguità.

Il mercato dell'*infomediation*, destinato ad imporsi all'attenzione dell'interprete e delle *Authorities*, nella prospettiva costante del bilanciamento tra tutela della persona ed esigenze commerciali, dovrà essere più puntualmente definito in tutti i suoi aspetti.

L'atteggiamento del legislatore europeo è comunque quello di un regolatore che guarda ai servizi di intermediazione dei dati non già (o non più) come ad un pericolo per i diritti fondamentali dell'interessato, ma come a un'opportunità offerta allo stesso e a un beneficio per il mercato, tramite la regolazione con meccanismi di notifica e di vigilanza. Una sorta di terza via, incentrata sulla dichiarata "*voluntary sharing of data by individuals and businesses*", che si colloca tra la chiusura ormai improponibile e l'apertura generalizzata auspicata da Thomas Ramge e Viktor Majer Schönberger¹⁵.

Posto che lo scambio dei dati (che – quanto ai dati personali – non può essere di tipo tradizionalmente traslativo) non solo è sottostante ad un importante, anzi importantissimo segmento di produzione economica, ma costituisce proprio il presupposto fondante dell'ulteriore crescita del sistema economico europeo, non stupisce la sequenza sempre più pervasiva di regole che lo riguardano, che appaiono rivelatrici del ruolo del legislatore europeo nell'economia e che interrogano gli osservatori sulla proporzionalità degli strumenti prescelti.

In questo quadro la funzione degli intermediari non è però esente da ambiguità¹⁶: visti come soggetti in grado di assicurare i diritti degli interessati nel contesto tecnologico, essi potrebbero invece finire per esaltare la redditività dei dati personali (non a caso ormai il termine invalso è "commodificazione" o "monetizzazione" delle informazioni), incoraggiandone l'utilizzo per fini commerciali. Circostanza, questa, che potrebbe portare ad una progressiva erosione delle garanzie di tutela degli interessati, ingenerando quello che è stato definito il sottoproletariato dei dati (la propensione dei soggetti meno abbienti a cedere anche informazioni ad elevato tasso di sensibilità per ricavarne piccoli introiti), con il rischio dello svilimento dei diritti fondamentali della persona¹⁷.

Anche per evitare questi esiti il DGA si preoccupa di dettare le condizioni per la fornitura di servizi di condivisione (art. 12), al fine di evitare possibili abusi degli intermediari, tra i quali il divieto di utilizzare i dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e i servizi di condivisione dei dati; il divieto di utilizzo dei metadati raccolti nel corso della fornitura del servizio di condivisione (come data, ora, geolocalizzazione) per scopi diversi dallo sviluppo del servizio stesso; l'obbligo di agire nell'interesse superiore degli interessati nel facilitare l'esercizio dei loro diritti, anche fornendo consulenza – come già si è anticipato – sui potenziali utilizzi dei dati e sui termini e le condizioni standard collegati a tali utilizzi.

All'interprete è richiesto un "surplus" di attività. Mentre è ancora impegnato a definire la tipologia del contratto con il *data subject* "cede" i suoi dati personali (in

¹⁵ T. RAMGE E V. MAJER SCHÖNBERGER, *Fuori i dati! Rompere i monopoli per rilanciare il progresso*, Milano, 2021.

¹⁶ BRAVO, *op. cit.*, p. 254.

¹⁷ Ammoniva dai rischi della creazione del "sottoproletariato del digitale", una sorta di "Quinto Stato" formato da quanti siano disposti a cedere, con i propri dati, la libertà, in cambio dei servizi offerti in rete solo apparentemente 'a prezzo zero' già A. Soro, *L'universo dei dati e la libertà della persona*, Relazione 2018, p. 7. E cfr. P. Stanzione, *Introduzione*, in *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, p. 5 ss.

realtà, il consenso al trattamento dei suoi dati personali) in cambio di una prestazione di servizi e ad analizzare la recente attuazione, ad opera dei d. lgs. nn. 173/2021 e 170/2021, della direttiva n. 770/2019 sulla fornitura di contenuti digitali e di servizi digitali e della direttiva n. 771/2019 sui contratti di vendita di beni con contenuto digitale, nonché ad interrogarsi ancora sull'apparente dichiarata gratuità di contratti sostanzialmente onerosi, altri problemi giuridici (e soprattutto precise scelte di politica del diritto) si affacciano all'orizzonte.

Non vi è stato neppure il tempo di osservare compiutamente un lato del mercato e la negoziabilità che riguarda i rapporti tra gli interessati e le *digital platforms*, che appare necessario porsi il problema di esaminare l'altro lato del mercato, studiando la struttura e il contenuto del contratto tra l'intermediario e l'utilizzatore, avente ad oggetto dati non personali o dati personali altrui e riempiendo di contenuto, quanto all'impiego di questi ultimi, gli strumenti della loro "messa a disposizione" (espressione che compare in più luoghi del DGA).

Questa indagine dovrà certamente muovere dal GDPR ma avrà necessità di allargarsi per tenere in debito conto i rimedi contro le scorrettezze e gli abusi del mercato dei dati, alla cui repressione è deputata la proposta di *Data Act*, che si propone di tutelare le micro, piccole e medie imprese che puntano alla creazione di modelli di business fondati sui dati dalle clausole vessatorie "unfair" unilateralmente imposte dai *data holders*.

Conclusions.

Brevi notazioni conclusive possono appuntarsi su alcune linee di prospettiva e alcuni nodi problematici, da affidare alla riflessione futura e meno approssimativa su un testo che meriterà ben più attenta considerazione.

Guardando al trend più generale del legislatore europeo, non può che essere indicato l'ulteriore aumento della già densa complessità, dovuto alla coesistenza di discipline differenti: la protezione dei dati personali e la disciplina di quelli non personali, la regolamentazione della condivisione dei dati e del loro commercio, il governo delle piattaforme, grandi e piccole, ma anche la tutela della proprietà intellettuale, la salvaguardia della concorrenza, la protezione della piccola e media impresa pure nella fruizione dei servizi di intermediazione on line, la tutela del consumatore, anche nella veste di acquirente di prodotti e servizi digitali. Il flusso ormai continuo di interventi regolamentari dell'Unione pone altresì problemi di coordinamento e di armonizzazione "interna" delle diverse discipline, che l'inserimento in una strategia comune non supera del tutto, tanto da sollevare l'interrogativo se non fosse stato più opportuno ed efficiente adottare un organico e generale *corpus juris digitalis*¹⁸.

Tutti questi interventi realizzano una sorta di "*GDPR by default*", posto che la normativa sulla protezione dei dati personali viene sempre dichiarata intangibile e prevalente, ma è indubbio che già nel confronto con il DGA, il GDPR riveli le proprie debolezze, specie in ordine al diritto al controllo.

È indubbio che nel contesto della condivisione dei dati personali, diretto a perseguire il risultato di un sistema "*open as possible, closed as necessary*", tale

¹⁸ CERRINA FERONI, *op. loc. cit.*

da coniugare le esigenze di condivisione di una grande mole di dati con il rispetto delle stringenti disposizioni del GDPR, giochi un ruolo significativo il diritto alla portabilità dei dati personali introdotto nell'art. 20, che deve essere coniugato con il rafforzamento dell'interoperabilità verso cui spinge la normativa europea. Non è un caso che tra le condizioni a cui sono assoggettati i servizi di intermediazione dei dati, l'art. 12 DGA preveda che il fornitore "agevola lo scambio dei dati nel formato in cui li riceve da un interessato o da un titolare dei dati, li converte in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati" e che lo stesso debba adottare misure adeguate per garantire l'interoperabilità con altri servizi di intermediazione dei dati, segnando in tal modo il passaggio dall'interoperabilità dei formati all'interoperabilità dei servizi¹⁹.

In dottrina è stata segnalata la "valenza polifunzionale" di tale diritto, in grado, per un verso, di valorizzare "al massimo livello il potere dell'interessato di controllo sui dati", rappresentando in tal modo "l'espressione più piena del diritto alla protezione dei dati personali nella sua proiezione positiva"; capace, per altro verso, di porsi in maniera fortemente dinamica come fattore propulsivo della libera circolazione dei dati, quale diritto che ha la sua iniziale giustificazione nell'incentivazione del mercato e delle dinamiche concorrenziali²⁰ e che esprime un tipico potere di disposizione dell'interessato. Negli scenari in esame il diritto alla portabilità finisce per esaltare maggiormente questo suo secondo volto, tanto da apparire più funzionale al controllo dei *data holders*, che detengono i dati, piuttosto che a quello dei *data subjects*²¹.

Il difficile esercizio del diritto al controllo di questi ultimi in un mercato dei dati mostra la necessità del ricorso a forme di aggregazione, come le cooperative di dati o gli intermediari *ad adiuvandum*, secondo uno scenario che fa chiaramente trapelare il percorso verso una tutela sempre più di matrice collettiva, prospettata con una certa timidezza dall'art. 80 GDPR, in parte recuperato dal legislatore italiano nel novellato art. 142 cod. priv., che consente all'interessato, nel presentare reclamo al Garante, di conferire mandato ad un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati, con riguardo alla protezione dei dati personali²².

Per fare sì che l'interessato rimanga soggetto attivo del flusso dei propri dati il *data subject* deve sostanzialmente condividere questi dati con altri e delegare

¹⁹ Sul rapporto tra portabilità e interoperabilità: E. BATTELLI e G. D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in *Privacy digitale*, a cura di E. TOSI, Milano, 2019, p. 201 ss.

²⁰ S. TROIANO, *Il diritto alla portabilità dei dati personali. Riflessioni sul GDPR*, in *Persona e mercato dei dati*, a cura di N. ZORZI GALGANO, Milano, 2019, p. 199.

²¹ Pronosticava che il diritto alla portabilità dei dati sarebbe stato destinato a essere utilizzato "più che 'dagli' interessati, 'attraverso' gli interessati, dai titolari del trattamento il cui business dipende, in misura diversa, dalla capacità di accumulare grandi quantità di dati personali e di analizzarli al fine di costruire profili sempre più attendibili di utenti e consumatori e/o implementare i propri modelli di business", G. Scorza, *Il diritto alla portabilità tra privacy e regole del mercato*, in *Regolare la tecnologia: il reg. Ue 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di A. Mantelero e D. Poletti, Pisa, 2018, p. 308.

²² F. CASAROSA, *La tutela aggregata dei dati personali nel Regol. Ue 2016/679: una base per l'introduzione di rimedi collettivi?*, in *Regolare la tecnologia: il reg. Ue 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, cit., p. 235 e ss.

l'esercizio dei suoi diritti. Fattore, questo, che deve indurre a riconsiderare il meccanismo della delega dell'esercizio di diritti attinenti alla sfera personale non sconosciuto alla l. 675/1996, che all'art. 13 prevedeva la possibilità dell'interessato di conferire, per iscritto, delega o procura a persone fisiche o ad associazioni, poi scomparso nella successiva storia legislativa della *data protection* italiana.

Il tentativo è quello di rafforzare il "*data subject empowerment*" ma collocato all'interno della circolazione e sempre più intermediato, posto che l'interessato può chiedere che i dati siano resi disponibili direttamente a terzi (tra questi terzi dovrebbero essere escluse le "very large platforms" come definite dalla proposta di *Digital Service Act*), trasformando il trattamento dei dati in una faccenda inserita in una dinamica circolatoria e per di più non relegata all'interno di un unico rapporto contrattuale ma situata all'interno di una rete di rapporti contrattuali.

Il terreno è oltremodo delicato, perché al dinamismo del mercato non si confanno rigidità o anacronismi, mentre il mantenimento della centralità della persona e dei suoi diritti necessita di regole forti. Solo combinando queste esigenze si potrà offrire una risposta (consapevolmente) positiva all'interrogativo che si poneva lo *European Data Protection Board*, nella menzionata Opinion 9/2016: "*Sharing Data, Sharing Benefits?*".



DO
MORE

Circolarità economica e trasparenza del prodotto Economic circularity and product transparency

MARIA ANTONIA CIOCIA^{ID}

Full Professor of Private Law at Università degli Studi della Campania Luigi Vanvitelli

Abstract

La riflessione svolta nell'articolo induce a dover necessariamente conformare la tutela consumeristica agli obiettivi generali dell'economia circolare. A livello ordinamentale si rende necessaria una rivisitazione normativa alla luce della diversa ponderazione di valori che, sovverte il rapporto persona/profitto in nome dell'incremento di possibilità di vita delle generazioni future. Nello stesso senso, l'adeguamento alla logica di sostenibilità del mercato implica un cambiamento nei contenuti del diritto all'informazione garantito al consumatore, che deve orientare le sue scelte in modo sostenibile. In tale ottica, la tutela del consumatore, ben oltre il rapido e aggressivo svolgimento dei meccanismi di consumo, dovrà estendersi nella direzione di privilegiare scelte coerenti in un contesto di mercato equo, sostenibile e solidale. In questo contesto, la trasparenza nell'etichettatura, la configurazione di un nuovo ambito di illiceità connotato dalla violazione della sostenibilità ambientale, costituzionalmente protetta, nonché il rafforzamento delle garanzie di durata dei beni di consumo sono fattori che convergono nel senso dell'instaurazione dell'economia circolare.

The reflection carried out in the article leads to the need to necessarily conform consumer protection to the general objectives of the circular economy. At the legal level, a regulatory review is necessary in light of the different weighting of values which subverts the person / profit relationship in the name of increasing the possibility of life for future generations. In the same sense, the adaptation to the logic of market sustainability implies a change in the contents of the right to information guaranteed to the consumer, who must guide his choices in a sustainable way. In this perspective, consumer protection, well beyond the rapid and aggressive development of consumption mechanisms, must extend in the direction of favoring coherent choices in a fair, sustainable and supportive market context. In this context, transparency in labeling, the configuration of a new area of illegality characterized by the violation of environmental sustainability, constitutionally protected, as well as the strengthening of the durability guarantees of consumer goods are factors that converge in the sense of establishing circular economy.



Keywords: Economia circolare; Consumatore; Prodotto; Responsabilità; Sviluppo sostenibile.

Sommario. [Introduzione.](#) – [1. Green deal europeo e modello circolare dell'economia.](#) – [2. Strumenti pubblicistici per l'attuazione dello sviluppo sostenibile.](#) – [3. Etichettatura e trasparenza.](#) – [4. Pratiche commerciali scorrette ed economia circolare.](#) – [5. Trasparenza e informazione.](#) – [6. Diritto di recesso e recensioni certificate.](#) – [7. Riflessioni sulle caratteristiche dei beni.](#) – [8. Responsabilità del venditore, onere della prova e denuncia.](#) – [9. Garanzia e diritto di regresso.](#) – [Conclusioni.](#)

Introduzione.

In coordinamento con le rinnovate istanze di sostenibilità ambientale, la tutela del consumatore assume nuovi contenuti in una dimensione evolutiva che intende conferire valore aggiunto alle scelte della persona che, ben oltre il conseguimento del profitto, persegua interessi rilevanti in termini di sostenibilità. Rinnovata ponderazione di interessi che consente di ipotizzare il passaggio dal «contratto ecologico»¹ al «contratto sostenibile». L'evoluzione si origina nell'economia globalizzata attraverso una dinamica di sviluppo tipo lineare ad un modello caratterizzato dalla circolarità del ciclo produttivo e di consumo, così come finalizzato al recupero, riuso e riciclo del rifiuto. La configurazione del contratto *tout court*, va rivisitata alla luce del ruolo pro-attivo del consumatore, che porta a privilegiare, in una visione antropocentrica della persona, scelte eque, responsabili e solidali che privilegino la considerazione della presenza nel processo produttivo di elementi naturali sostenibili, in termini di durabilità. In questo modo si delinea l'innovativa categoria del «contratto sostenibile» con l'orientamento fondante il c.d. «consumo critico», da intendersi come modo di acquisto di beni e servizi, scelti non soltanto in funzione di prezzo e di indubbie qualità ma in un'ottica solidaristica, condivisa tra produttori e consumatori, informata alla circolarità della filiera produttiva. L'autonomia privata, partendo dal «contratto ecologico», quale visione ancorata alla tutela di elementi naturali basilari può pervenire ad un modello di produzione e consumo che preserva detti elementi al limite del loro esaurimento, contemplando il principio di solidarietà ambientale quale volano del sistema economico². Può essere senz'altro interessante, interrogarsi sul fondamento costituzionale del «contratto sostenibile» che, indubbiamente, rappresenta una sintesi degli artt. 9, 32 cost., al 41, 42, 43 e 44 cost., in combinazione con l'art. 2 cost. che informa alla solidarietà le scelte collettive alla base della sostenibilità ambientale, baluardi dell'edificazione del nuovo ordine, imprescindibile per le attuali e future generazioni ed interesse condiviso e condivisibile tra le parti. Centrale in questa

¹ Si veda, M. PENNASILICO, *Contratto ecologico e conformazione dell'autonomia negoziale*, in *Riv. dir. amb.*, 2017, 1-29.

² Cfr. M. MONTEDURO e S. TOMMASI, *Paradigmi giuridici di realizzazione del benessere umano in sistemi ecologici ed esistenza indisponibile e ad appartenenza necessaria*, in AA.VV., *Benessere e regole di rapporti civili. Lo sviluppo oltre la crisi*. Atti del 9° Convegno Nazionale S.I.S.D.I.C. in ricordo di G. Gabrielli, Napoli 8-9-10 maggio 2014, Napoli, 2015, 161 ss.

nuova strategia l'istituzione del Ministero della transizione ecologica, così come la modifica degli artt. 9 e 41 della Costituzione, nel senso della consapevolezza generalizzata della complessità ed urgenza della svolta sistemica³. E' chiara la necessità di una variazione nell'orientamento delle politiche e degli investimenti pubblici in funzione degli obiettivi di sviluppo sostenibile fissati già nel 2015 dall'Agenda 2030 dell'ONU⁴. Il Trattato sull'Unione Europea all'art. 3, paragrafo 3, istituisce un mercato interno e «si adopera» per lo sviluppo sostenibile dell'Europa che deve svolgersi secondo quattro direttive: i) crescita economica equilibrata; ii) stabilità dei prezzi; iii) economia sociale di mercato fortemente competitiva, che miri alla piena occupazione e al progresso sociale; iv) elevato livello di tutela e di miglioramento della qualità dell'ambiente. Obiettivi questi ultimi che divengono globali. Le linee d'azione suddette devono essere estese anche ai rapporti con il resto del mondo. L'Unione contribuisce «allo sviluppo sostenibile della Terra» in un principio di cooperazione internazionale e solidarietà tra popoli.

1. *Green deal* europeo e modello circolare dell'economia.

Nel marzo 2020, nel quadro del *Green Deal* europeo, la Commissione ha presentato un nuovo piano d'azione per l'economia circolare, nel quale ha annunciato iniziative legislative relative all'attuazione della strategia volta a rendere i prodotti idonei a un'economia climaticamente neutra, efficiente sotto il profilo delle risorse e circolare, come mirata a ridurre al massimo i rifiuti e a garantire che, gradualmente, le prestazioni conseguite dai soggetti più all'avanguardia in materia di sostenibilità divengano la norma. La direttiva sulla progettazione ecocompatibile⁵, considera nel proprio ambito oggettivo i prodotti

³ L'Agenda 2030 per lo sviluppo sostenibile, adottata dall'ONU il 25 settembre 2015, è stata sottoscritta da 193 Paesi, inclusa l'Italia. Essa stabilisce 17 obiettivi di sviluppo sostenibile, *Sustainable Development Goals*, SDGs e 169 *target* da raggiungere entro il 2030. Proprio al fine di rafforzare il coordinamento delle politiche pubbliche, in vista del perseguimento degli obiettivi in materia di sviluppo sostenibile indicati dalla risoluzione A/70/L.I (adottata dall'Assemblea generale dell'Organizzazione delle Nazioni Unite il 25 settembre 2015) a decorrere dal 1° gennaio 2021 il Comitato interministeriale per la programmazione economica assume la denominazione di Comitato interministeriale per la programmazione economica e lo sviluppo sostenibile (CIPESS). Sempre dalla medesima data, nella legge 27 febbraio 1967, n. 48, e in ogni altra disposizione vigente, qualunque richiamo al Comitato interministeriale per la programmazione economica deve intendersi riferito al Comitato interministeriale per la programmazione economica e lo sviluppo sostenibile (CIPESS).

⁴ La nuova denominazione viene introdotta dal c.d. Decreto Clima, d.l. 14 ottobre 2019, n. 111, il primo decreto-legge dedicato totalmente all'ambiente realizzato in Italia.

⁵ La Direttiva 2005/32/CE ha disciplinato l'immissione nel mercato e l'utilizzo di prodotti che consumano energia (*Eco-design Directive for Energy-using Products - EuP*), atto che prevede l'adozione di criteri di progettazione funzionali alla riduzione dell'impatto ambientale e al miglioramento dell'efficienza energetica. Con l'intento di uniformare la produzione europea in senso di ecocompatibilità e corretto funzionamento del libero mercato, l'Unione Europea ha abrogato questa direttiva ed emanato la Direttiva 2009/125/CE, entrata in vigore nel 2009. È evidente come la Direttiva voglia configurare un quadro giuridico europeo per l'individuazione dei prodotti connessi all'energia, che devono soddisfare requisiti minimi in materia di efficienza energetica, le cosiddette specifiche di progettazione ecocompatibile con l'obiettivo di ridurre l'impatto negativo sull'ambiente durante tutto il ciclo di vita del prodotto. La Direttiva distingue l'*ecodesign* per l'impatto ambientale dall'*ecodesign* per l'efficienza energetica. Il primo parte dalla consapevolezza che proprio nella fase progettuale si determina l'impatto ambientale che il prodotto provocherà durante il suo ciclo di vita, ne deriva la rilevanza di sviluppare prodotti orientati alla riduzione degli impatti ambientali nelle fasi del ciclo di vita del prodotto, requisito che viene verificato attraverso la valutazione del ciclo di vita, *Life Cycle Assessment*, LCA, ossia valutazione di ogni fase del ciclo di vita del prodotto dall'estrazione e

connessi all'energia, ma è in corso un ampliamento dell'ambito oggettivo di riferimento finalizzato ad includere sostanze chimiche nocive in prodotti quali apparecchiature elettroniche e TIC (tecnologie dell'informazione e della comunicazione), prodotti tessili, mobili, acciaio, cemento e prodotti chimici. L'iniziativa sarà sviluppata in stretto coordinamento con altre annunciate nell'ambito del piano d'azione per l'economia circolare, in particolare quelle

trasformazione delle materie prime, passando per la produzione e l'utilizzo, fino alla gestione del fine vita del prodotto (e cioè il riuso, il riciclo e lo smaltimento ultimo dei rifiuti che ne derivano). L'ecodesign per l'efficienza energetica che pone al centro della valutazione l'obiettivo della efficienza energetica come contributo sostanziale al raggiungimento degli obiettivi di riduzione delle emissioni di gas a effetto serra con specifica attenzione alle le specifiche di progettazione ecocompatibile relative al consumo di energia elettrica nei modi stand-by e spento delle apparecchiature elettriche ed elettroniche domestiche e da ufficio. I tipi di prodotti attualmente disciplinati da queste regole sono quelli che consumano energia (caldaie, computer, elettrodomestici, ecc.). La direttiva impone due tipi di indicazioni ossia, requisiti specifici e requisiti generali. Nel primo caso viene richiesta l'indicazione di valori esatti ed è fissato un limite, nel consumo massimo di energia o per le quantità minime di materiali riciclati da utilizzare nella produzione. I requisiti generali non fissano valori limite, ma possono richiedere che: il prodotto sia "efficiente dal punto di vista energetico" oppure "riciclabile"; si forniscano informazioni su come usare e conservare il prodotto in modo tale da ridurre al minimo l'impatto sull'ambiente; si effettui un'analisi del ciclo di vita del prodotto per individuare opzioni e soluzioni di progettazione alternative. L'introduzione di nuovi requisiti minimi può comportare un divieto di vendere tutti i prodotti non conformi nei paesi dell'UE. Esempio: le lampadine ad incandescenza, la cui vendita è stata gradualmente vietata dal 2009 in poi. Ulteriore tappa evolutiva è rappresentata dalla revisione della progettazione ecocompatibile da parte della Commissione europea con uno studio che mostri la fattibilità e l'efficacia. La Direttiva quadro è stata integrata dalla graduale emanazione di regolamenti attuativi finalizzati a definire specifiche norme per ogni categoria di prodotto cui i produttori devono attenersi e solo l'adozione dei parametri indicati dai Regolamenti dà diritto alla marcatura Ce, senza della quale i prodotti non possono essere immessi sul mercato europeo. La Direttiva non si applica ai mezzi di trasporto di passeggeri o merci. Di seguito i regolamenti europei attuativi della direttiva 2009/125/CE: regolamento Commissione Ue 30 marzo 2011, n. 327/2011/UE di ventilatori a motore la cui potenza elettrica di ingresso è compresa tra 125 W e 500 kW; regolamento Commissione Ue 6 marzo 2011, n. 206/2012/UE dei condizionatori d'aria e dei ventilatori; regolamento Commissione Ue 21 giugno 2012, n. 547/2012/UE pompe centrifughe per acqua per il pompaggio di acqua pulita; Regolamento Commissione Ue 12 dicembre 2012, n. 1194/2012/UE (come lampade direzionali, delle lampade con diodi a emissione luminosa e delle pertinenti apparecchiature; regolamento Commissione Ue 26 giugno 2013, n. 617/2013/UE dei computer e dei server informatici; regolamento Commissione Ue 8 luglio 2013, n. 666/2013/UE degli aspirapolvere; regolamento Commissione Ue 813/2013/UE apparecchi per il riscaldamento d'ambiente e degli apparecchi di riscaldamento misti; regolamento Commissione UE 4/2014/UE dei motori elettrici; regolamento Commissione Ue n. 66/2014/UE forni, piani cottura e cappe da cucina per uso domestico; regolamento Commissione Ue 548/2014/UE i trasformatori di potenza piccoli, medi e grandi; regolamento Commissione Ue 1253/2014/UE unità di ventilazione, utilizzate per effettuare il ricambio dell'aria esausta, con aria proveniente dall'esterno in un edificio o in una sua parte; regolamento Commissione Ue 2015/1095/UE degli armadi refrigerati professionali, degli abbattitori, delle unità di condensazione e dei chiller di processo; regolamento Commissione Ue 2015/1189/UE caldaie a combustibile solido (biomassa legnosa e carboni fossili); regolamento Commissione Ue 2015/1188/UE apparecchi per il riscaldamento d'ambiente locale (stufe per uso domestico e industriale utilizzate per riscaldare i singoli ambienti entro cui sono situate); regolamento Commissione Ue 2015/1185/UE degli apparecchi per il riscaldamento d'ambiente locale (stufe utilizzate per riscaldare i singoli ambienti entro cui sono situate) a combustibile solido (biomassa legnosa e carboni fossili); regolamento Commissione Ue 2016/2281/UE; regolamento dei prodotti di riscaldamento dell'aria, dei prodotti di raffrescamento, dei chiller di processo ad alta temperatura e dei ventilconvettori; regolamento Commissione Ue 2019/424/UE su server e prodotti di archiviazione dati online; regolamento Commissione Ue 2019/1781/UE messa in funzione dei motori elettrici e dei variatori di velocità; regolamento Commissione Ue 2019/1782/UE alimentatori esterni; regolamento Commissione Ue 2019/1783/UE trasformatori di potenza piccoli, medi e grandi; regolamento Commissione Ue 2019/1784/UE delle apparecchiature di saldatura; regolamento Commissione Ue 2019/2019/UE apparecchi di refrigerazione; regolamento Commissione Ue 2019/2024/UE frigoriferi ad armadio utilizzati dai negozi per la vendita diretta; regolamento Commissione Ue 2019/2023/UE relativa all'immissione sul mercato e alla messa in funzione di lavatrici e lavasciuga per uso domestico; regolamento Commissione Ue 2019/2022/UE per la progettazione ecocompatibile relative all'immissione sul mercato e alla messa in funzione delle lavastoviglie per uso domestico; regolamento Commissione Ue 2019/2021/UE, display elettronici, compresi i televisori, i monitor e i pannelli segnaletici digitali; regolamento Commissione Ue 2019/2020/UE (prodotti per illuminazione, anche a batteria).

riguardanti la responsabilizzazione dei consumatori, affinché svolgano un ruolo attivo nella transizione ecologica, consapevoli di dover dare attuazione alle dichiarazioni ambientali anche con l'utilizzo di metodi per misurare l'impronta ambientale dei prodotti e delle organizzazioni. Tali iniziative, insieme, intendono istituire un quadro normativo coerente, nell'ambito del quale beni, servizi, modelli imprenditoriali e modelli di consumo sostenibile diventeranno centrali.

2. Strumenti pubblicitici per l'attuazione dello sviluppo sostenibile.

In quest'ottica anche la dialettica produttore-consumatore assume nuovi connotati. In particolare, occorre riconoscere la portata strategica della responsabilità da parte dei produttori nel dar vita a trasformazioni tecnologiche che consentano produzioni sostenibili⁶ in termini di passaggio da un modello di produzione lineare ad uno circolare, che investa nella valorizzazione del rifiuto in termini di recupero, riutilizzo e trasformazione. Da altro punto di vista, il consumatore deve realizzare forme di consumo critico, preferendo prodotti «sostenibili» provenienti da tecnologie pulite. È evidente come la strategia per innovare il contesto normativo e strategico debba essere perseguita sia a livello privatistico, attraverso l'adozione di modelli imprenditoriali circolari, che attraverso strumenti pubblicitici, quali criteri di aggiudicazione degli appalti e presenza in essi di «clausole verdi» o CAM «criteri ambientali minimi», e tramite l'attuazione degli obiettivi dell'Agenda 2030 che sono strumenti idonei a innovare la tecnologia produttiva.

3. Etichettatura e trasparenza.

Nel breve e medio periodo, di fondamentale rilevanza sarà reindirizzare verso questa visione le leve strategiche attuative di politiche pubbliche, ma anche la modifica della tutela del consumatore attraverso interventi che rendano trasparente il processo di produzione con l'etichettatura. Il sistema EMAS dell'UE è uno strumento di gestione destinato ad aziende e altre organizzazioni per valutare e migliorare le loro prestazioni ambientali. Il sistema è disponibile per le aziende dal 1995⁷, ma era originariamente limitato alle aziende del settore

⁶ Nel marzo 2020, nel quadro del *Green deal* europeo, la Commissione ha presentato un Piano d'azione per promuovere l'economia circolare, nel quale ha annunciato una strategia in materia di prodotti sostenibili, volta a rendere i prodotti idonei a un'economia climaticamente neutra, efficiente sotto il profilo delle risorse e circolare, nel ridurre i rifiuti e nel garantire che, gradualmente, le prestazioni conseguite dai soggetti più all'avanguardia in materia di sostenibilità divengano la norma. L'iniziativa legislativa prevede una revisione della direttiva sulla progettazione ecocompatibile, il cui campo di applicazione sarà ampliato al di là dei prodotti connessi all'energia, nonché ulteriori misure legislative. Affronterà, inoltre, la questione della presenza di sostanze chimiche nocive in prodotti quali apparecchiature elettroniche e TIC, prodotti tessili, mobili, acciaio, cemento e prodotti chimici. L'iniziativa sarà sviluppata in stretto coordinamento con la responsabilizzazione dei consumatori, affinché svolgano un ruolo attivo nella transizione ecologica, e con la necessità di corroborare le dichiarazioni ambientali, utilizzando metodi per misurare l'impatto ambientale dei prodotti e delle organizzazioni. Tali iniziative, insieme, si propongono di istituire un quadro politico coerente, nell'ambito del quale beni, servizi e modelli imprenditoriali sostenibili diventeranno la norma assieme a modelli di consumo più sostenibili.

⁷ L'etichettatura fornisce informazioni essenziali che consentono ai consumatori di compiere scelte consapevoli. Il marchio europeo di qualità ecologica è un sistema facoltativo, creato nel 1992 per

industriale. Dal 2001, il sistema EMAS è aperto a tutti i settori economici, inclusi i servizi pubblici e privati. Nel 2009, il regolamento EMAS (CE) n. 1221/2009 è stato rivisto e modificato con l'obiettivo di incoraggiare ulteriormente le organizzazioni ad aderirvi. La revisione del regolamento EMAS ha migliorato l'applicabilità e la credibilità dell'intervento. Nel 2017 gli allegati I, II e III del regolamento EMAS sono stati modificati per includere la revisione della norma ISO 14001: 2015. Il regolamento (UE) 2017/1505 che modifica tali allegati è entrato in vigore il 18 settembre 2017. Il marchio di qualità viene così ad essere un elemento fondante il sistema di sostenibilità ambientale. In altro ambito, quello biologico non è trascurabile la portata della l. n. 23 del 9 marzo 2022 (Pubblicata nella G.U. n. 69 del 23 marzo 2022), recante "Disposizioni per la tutela, lo sviluppo e la competitività della produzione agricola, agroalimentare e dell'acquacultura con metodo biologico", entrata in vigore lo scorso 7 aprile 2022, che disciplina il sistema delle autorità nazionali e locali e degli organismi competenti, i distretti biologici, l'organizzazione della produzione e del mercato, nonché le azioni per la salvaguardia, la promozione e lo sviluppo della produzione agricola e agroalimentare con metodo biologico. La Legge n. 23/2022 introduce l'uso di un marchio nazionale per contraddistinguere i prodotti ottenuti con il metodo biologico, realizzati con materie prime coltivate o allevate in Italia. In questi termini il l'istituzione di un marchio biologico italiano, di proprietà esclusiva del Ministero delle politiche agricole alimentari e forestali (Mipaaf),

incoraggiare le imprese a commercializzare prodotti e servizi rispondenti a determinati criteri ambientali. I criteri sono fissati e riveduti dal comitato dell'Unione europea per il marchio di qualità ecologica (CUEME), che è inoltre responsabile per i requisiti di valutazione e di verifica ad essi connessi. I prodotti e i servizi certificati con il marchio ecologico sono caratterizzati da un logo recante un fiore, che permette ai consumatori, inclusi gli acquirenti pubblici e privati, di identificarli facilmente. Il marchio è stato finora assegnato a prodotti quali detersivi, elettrodomestici, prodotti cartacei, abbigliamento, prodotti per la casa e il giardino, lubrificanti e servizi come quelli della ricettività turistica. I criteri per l'assegnazione del marchio di qualità ecologica non sono basati su un unico fattore, bensì su studi che analizzano l'impatto di un prodotto o di un servizio sull'ambiente durante il suo ciclo di vita. La revisione nel 2008 del Regolamento sul marchio di qualità ecologica (CE) n. 66/2010 intendeva promuovere l'uso di tale sistema facoltativo riducendo l'onere economico e burocratico legato all'applicazione delle norme. Il 30 giugno 2017 la Commissione ha presentato le conclusioni della sua valutazione (controllo dell'adeguatezza) del regolamento sul marchio di qualità ecologica. La Commissione ha rilevato che il regolamento produce un valore aggiunto per l'UE, tuttavia, è parzialmente efficace (poiché consente di migliorare le prestazioni ambientali per i prodotti su cui è apposta l'etichetta, ma i criteri potrebbero non essere adeguati e la loro diffusione rimane ridotta per alcune tipologie di prodotti) e parzialmente efficiente (poiché i costi legati alla conformità possono rappresentare un ostacolo alla partecipazione in alcuni casi). Circa il settore energetico, la direttiva 92/75/CEE ha introdotto un sistema di etichettatura energetica degli elettrodomestici, in cui le informazioni contenute negli opuscoli illustrativi forniscono ai potenziali consumatori dati sui consumi energetici di tutti i modelli disponibili. Dalla sua introduzione nel 1995, il sistema di etichettatura energetica UE si è trasformato in una guida ampiamente riconosciuta da produttori e consumatori. Nel giugno 2010, la direttiva sull'etichettatura energetica (2010/30/CE) ha ampliato la sua applicazione ad una più ampia gamma di prodotti che consumano energia o connessi all'energia. Il regolamento (UE) 2017/1369 del 4 luglio 2017 istituisce un nuovo quadro per l'etichettatura energetica e abroga la direttiva 2010/30/CE, introducendo nuovi requisiti in materia di etichettatura energetica per singoli gruppi di prodotti. In concreto, cinque gruppi di prodotti (frigoriferi, lavastoviglie, lavatrici, televisori e lampade) sono stati «riscaldati»: un prodotto con una classe di efficienza energetica A + + +, ad esempio, diventerà una classe B, senza alcuna modifica del suo consumo di energia. Ciò consentirà ai consumatori di distinguere più chiaramente i prodotti più efficienti sotto il profilo energetico. A differenza della summenzionata direttiva 2009/125/CE, di revisione della direttiva 2005/32/CE che incentra la propria attenzione sul perfezionamento tecnico dei prodotti nella progettazione ecocompatibile, la direttiva 2010/30/CE estende l'ambito di applicazione ai prodotti connessi all'energia diversi dai prodotti che consumano energia: si tratta di prodotti che non impiegano energia durante il loro utilizzo, ma che hanno un impatto indiretto sul consumo energetico, come i dispositivi che consumano acqua, le finestre e i materiali d'isolamento.

verrà a caratterizzare i prodotti biologici ottenuti da materia prima italiana che verranno contraddistinti dalla dicitura “Biologico italiano”. Il logo del marchio biologico italiano, che potrà essere richiesto su base volontaria, sarà individuato mediante concorso di idee da bandire entro 180 giorni dalla data di entrata in vigore della Legge n. 23/2022. Sono tutt’oggi in corso di emanazione le condizioni e modalità pratiche di attribuzione del marchio da parte del Mipaaf, ma sicuramente il nostro Paese con l’approvazione della legge compie un deciso avanzamento nel senso della trasparenza e della qualità dei prodotti⁸.

4. Pratiche commerciali scorrette ed economia circolare.

Il complesso delle dinamiche evolutive comporta il superamento del mercato inteso come contesto in cui gli scambi si svolgono liberamente per la realizzazione del profitto, a favore di un contesto di accordi tra privati in cui l’autonomia negoziale deve essere finalizzata all’efficienza e alla sostenibilità duratura ed agevolata dalla trasparenza delle caratteristiche e qualità dei prodotti o servizi. Ciò implica l’emarginazione dal libero svolgimento dei traffici di meccanismi obsoleti che, lungi da realizzare il benessere della collettività, degradano l’ambiente in favore del profitto individuale.

Preliminare è sicuramente un cambiamento nei processi tecnologici di produzione, con eliminazione dei rifiuti dal ciclo produttivo e/o riutilizzo degli scarti di lavorazione. Ulteriore sforzo tecnologico dovrà svolgersi nel senso di prolungare i cicli di vita dei prodotti, con trasparente indicazione della durata che possa direzionare la scelta verso prodotti più ecosostenibili. In questi termini, è possibile segnare una tappa evolutiva di rilievo nella specificazione teorica insita nell’individuazione di una ulteriore specie dello schema negoziale che, nell’ambito della prevalenza degli interessi ambientali, vada oltre la doverosità dell’uso responsabile delle risorse naturali (propria del contratto ecologico) per svolgersi nel senso del prolungamento della durata del ciclo di vita del prodotto e dell’eliminazione di rifiuti dal ciclo produttivo *id est* il contratto sostenibile.

5. Trasparenza e informazione.

Al di là di considerazioni di tipo tecnologico che incidono sulle caratteristiche tecniche del prodotto e guidano le scelte di consumo, va effettuata un’ulteriore riflessione su quali siano le norme a tutela del consumatore da rimodulare alla luce del nuovo paradigma della sostenibilità.

Ritengo che l’ambito oggettivo delle c.d. pratiche commerciali sleali nei rapporti tra professionisti e consumatori, vada riesaminato sia relativamente alle condotte precontrattuali (comunicazioni commerciali, pubblicità, attività di

⁸ Il nostro Paese segue il percorso evolutivo anticipato dalla Germania. La legge nazionale tedesca sull’etichettatura dei prodotti biologici (ÖkoKennzG) del 10 dicembre 2001, ha istituito il logo “Bio-Siegel”, che può essere richiesto e utilizzato su base volontaria, a condizione che venga rispettata la normativa europea in materia di produzioni biologiche (all’epoca dell’istituzione del logo, il Reg. CEE n. 2092/1991) e che venga previamente informato il Ministero dell’Agricoltura tedesco.

marketing) sia relativamente alle condotte tenute contestualmente o posteriormente alla conclusione del contratto. Accanto, infatti, al divieto generale di porre in essere pratiche commerciali scorrette - vietando pratiche commerciali ingannevoli (artt. 21-23 c. cons.) aggressive (artt. 24-26 c. cons.) e attribuendo alla Autorità garante per la concorrenza ed il mercato poteri di accertamento e di irrogazione di sanzioni amministrative pecuniarie nei confronti di professionisti responsabili, nell'ambito di procedimenti disciplinati dall'art. 27 c. cons. - andranno senz'altro inserite le pratiche di c.d. *greenwashing* che si sostanziano in un ecologismo e responsabilità sociale di mera apparenza, cui non corrisponde alcun contenuto sostanziale, ma solo una strategia di apparente rispetto dei canoni di sostenibilità ambientale. In tal senso diventa necessario un rafforzamento del quadro istituzionale vigente in termini di sorveglianza e accreditamento al fine di giungere alla creazione di una vera e propria economia circolare. La configurazione del *greenwashing* come illecito consumeristico, anche oltre l'atto di concorrenza sleale, implica l'individuazione degli elementi sulla base dei quali sia possibile stabilire che la pratica posta in essere costituisca un mezzo non conforme ai principi della correttezza professionale e idoneo di per sé a danneggiare la concorrenza, come anche il consumatore, sino a potersi spingere nell'ambito della illiceità civilistica in termini di violazione di norme imperative, proprio in considerazione della recente rilevanza costituzionale acquisita dalla sostenibilità ambientale. L'azienda che pone in essere una pratica di *greenwashing*, tenta di incrementare il proprio fatturato, collocandosi in un segmento di mercato *green*, senza in realtà attuare una politica di produzione sostenibile e sopportarne i relativi costi, ma solo sfruttando gratuitamente il *favor* ormai esistente per i prodotti sostenibili, su cui *competitors* hanno investito a livello produttivo e pubblicitario. Il codice del consumo distingue allo stato le pratiche commerciali ingannevoli ed aggressive. Le prime ai sensi degli artt. 21 e 23 del codice del consumo sono quelle idonee ad indurre in errore il consumatore medio, falsandone il processo decisionale. L'induzione in errore può riguardare il prezzo, la disponibilità sul mercato del prodotto, le sue caratteristiche, i rischi connessi al suo impiego. A ben vedere il *greenwashing* potrebbe rientrare in questa categoria quanto alla mancanza delle caratteristiche promesse.

L'autorità considera illecite anche le pratiche che inducono il consumatore a trascurare le normali regole di prudenza e vigilanza relativamente all'uso dei prodotti pericolosi per la salute e la sicurezza di bambini o adolescenti. Se l'impresa pone in essere pratiche contenenti molestie, coercizione o altre forme di indebito condizionamento, il comportamento è considerato aggressivo (artt. 24-26 del codice del consumo), dove l'aggressività della pratica dipende dalla natura, dai tempi, dalle modalità, dall'eventuale ricorso alle minacce fisiche e verbali. Sebbene, possa ipotizzarsi un ragionevole livello di riconducibilità delle fattispecie ingannevoli dal punto di vista della sostenibilità alle categorie esposte, tuttavia, l'applicabilità appare debole sul piano della misurabilità degli effetti. Il giudizio di "ingannevolezza" andrà a basarsi su ogni elemento oggettivo in grado di pregiudicare verosimilmente le scelte economiche del consumatore o di ledere gli interessi di un'azienda concorrente, a nulla rilevando il profilo soggettivo del comportamento dell'azienda scorretta.

Con il successivo d.lgs. 6 settembre 2005, n. 206 (codice del consumo), la precedente normativa è stata assorbita e viene introdotto all'art.2, il diritto dei consumatori alla tutela della salute, alla sicurezza e qualità dei prodotti e dei servizi, all' adeguata informazione e corretta pubblicità ed alla correttezza, trasparenza e equità dei rapporti contrattuali, formulazione senz'altro idonea a ricomprendere fattispecie aventi influenza negativa sull'attuazione di istanze di sostenibilità, ma in forma generica ed attenuata. Sul punto qualche difficoltà può sussistere a livello probatorio, sull'effettiva portata della sostenibilità e scarsa correttezza dell'informazione veicolata. Nel 2014, l'Istituto di Autodisciplina Pubblicitaria ha pubblicato il Codice di Autodisciplina della Comunicazione Commerciale, introducendo per la prima volta, l'abuso di dichiarazioni che richiamano la sostenibilità ambientale *“La comunicazione commerciale che dichiara o evoca benefici di carattere ambientale o ecologico deve basarsi su dati veritieri, pertinenti e scientificamente verificabili. Tale comunicazione deve consentire di comprendere chiaramente a quale aspetto del prodotto o dell'attività pubblicizzata i benefici vantati si riferiscono”* (art.12). Il processo di configurazione della sanzionabilità del *greenwashing* si accentua nel 2015 con la promulgazione della l. 221/2015 sulla Green Economy *“Disposizioni in materia ambientale per promuovere misure di green economy e per il contenimento dell'uso eccessivo di risorse naturali”*, (c.d. “collegato ambientale” alla Legge di stabilità 2016). Con notevoli disposizioni destinate ad avere maggiore impatto ed efficacia sulle previsioni a tutela dell'ambiente e forte impulso a favore del riutilizzo delle risorse e dei materiali. A livello europeo, anche in considerazione della più recente emanazione del Trattato istitutivo della CEE, l' art. 153 rappresenta l'anticipazione dell' articolo 169 TFUE: *«al fine di promuovere gli interessi dei consumatori ed assicurare un livello elevato di protezione dei consumatori, l'Unione contribuisce a tutelare la salute, la sicurezza e gli interessi economici dei consumatori nonché a promuovere il loro diritto all'informazione, all'educazione e all'organizzazione per la salvaguardia dei propri interessi»*. Si menzionano, poi, l'art. 12 TFUE, secondo il quale l'Unione, nel definire ed attuare altre politiche o attività deve sempre tenere in considerazione le esigenze connesse alla tutela dei consumatori; e l'art. 38 della Carta dei diritti fondamentali dell'Unione europea, la quale ribadisce la protezione dei consumatori accordata dall'UE, affermando che nelle politiche europee deve essere garantito sempre il massimo livello di protezione degli individui. Rilevante da questo punto di vista, la proposta della Commissione europea per l'istituzione di un mercato unico dei prodotti verdi, emanata il febbraio 2013 mediante la comunicazione 196/2013 *Single Market for Green Products*, con lo scopo di esortare gli Stati Membri ad una sensibilità maggiore per l'uso efficiente di risorse, migliorando e armonizzando i processi di misurazione della sostenibilità ambientale dei prodotti verdi per incentivarne la diffusione e fornire ai consumatori informazioni veritiere e comprovate, svolta decisamente completata dal regolamento sulla tassonomia, adottato dal Parlamento europeo il 18 giugno 2020 con l'intento di definire univocamente, nel contesto dei mercati finanziari, il concetto di *“attività economica sostenibile dal punto di vista ambientale”*, onde rendere chiaro agli investitori il tasso di sostenibilità di un'azienda alla quale destinare flussi di capitali d'investimento. Il Regolamento definisce come ecosostenibile un'attività economica che: 1) contribuisce in maniera sostanziale a uno o più obiettivi

ambientali; 2) non danneggia in modo significativo nessun obiettivo ambientale europeo; 3) è svolta senza violare i diritti umani. Altre iniziative dell'Unione Europea, finalizzate alla tutela dei consumatori da fattispecie contrarie alla sostenibilità ambientale quali fenomeni di *greenwashing* e nel complesso informazioni non veritiere sulla sostenibilità e trasparenza dei prodotti che scelgono di acquistare, sono state incluse nella nuova agenda dei consumatori dell'Ue (2020-2025) e nello specifico : il *Green Consumption Pledge* (impegno per consumi sostenibili), formulato nel gennaio 2021, al fine di rafforzare il ruolo dei consumatori nella transizione verde cui si accompagna la proposta legislativa sulla dimostrazione della veridicità delle affermazioni ecologiche. Da segnalarsi anche l'introduzione dell'obbligo di dotare i prodotti alimentari di etichette nutrizionali armonizzate tra gli Stati membri e dell'obbligo di etichetta energetica UE per gli elettrodomestici, al fine di permettere ai consumatori di conoscere l'efficienza energetica di taluni prodotti e di acquistarli nella consapevolezza di reali risparmi. Nel quadro normativo così delineato, si aggiunga un rilievo sistematico nei casi in cui i brand ricorrono al *greenwashing* mentendo sull'impatto ambientale delle proprie strategie di produzione o nelle etichette dei loro prodotti, possono trovare applicazione gli artt. 2043 c.c. e ss. , nella misura in cui la sostenibilità può dirsi assurda a rango di diritto soggettivo assoluto e in quanto tale rende applicabile la tutela aquiliana, segnatamente riguardo al danno reputazionale che potrebbe conseguire il consumatore e all'eventuale diffusione di informazioni scorrette relativamente al prodotto o al processo di produzione, considerata l'introduzione della sostenibilità nella carta costituzionale attraverso le modifiche degli artt. 9 e 41.

6. Diritto di recesso e recensioni certificate.

La rivisitazione proposta va estesa anche alla trasparenza e al diritto all'informazione che rappresentano i perni della tutela consumeristica. Appare indispensabile, infatti, la promozione di un sistema obbligatorio di etichettatura che garantisca un livello eccellente dal punto di vista ambientale attraverso organismi di certificazione indipendenti e accreditati che realizzino sistemi nazionali o europei di marchi di sostenibilità, dove il requisito della sostenibilità dovrà basarsi sulla considerazione del processo tecnologico produttivo circolare. In altro senso, si renderebbe opportuna l'eliminazione di tutte le prassi che appesantiscono il ciclo di consumo, esemplificativamente l'art. 52 cod. cons., finalizzato alla protezione del consumatore nell'acquisto di beni a distanza, potrebbe di fatto confliggere con gli obiettivi di sostenibilità in termini di circolarità e limitazione o addirittura eliminazione dei rifiuti dal ciclo di produzione/consumo. A ben vedere, il consumatore è protetto, ai sensi di detta norma, attraverso il riconoscimento del diritto di recesso nella compravendita realizzata senza un'accorta ponderazione sulle qualità promesse dal prodotto. La *ratio* della tutela, che risiede nel riconoscimento del diritto del consumatore alla restituzione del bene al mittente, sortisce un effetto parzialmente confliggente con i principi della sostenibilità, in quanto implica un appesantimento della catena di distribuzione in

termini di duplicazione di movimentazione delle merci sul territorio nazionale e un'ulteriore produzione di rifiuti da imballaggio⁹.

La riflessione induce a dover necessariamente conformare la tutela consumeristica agli obiettivi generali e ciò in una ponderazione di valori che, in nome dell'incremento di possibilità di vita delle generazioni future, veda posposto l'interesse del consumatore rispetto all'interesse all'affermazione di un modello di circolarità nella dialettica produzione-consumo. Nello stesso senso, l'adeguamento alla logica di sostenibilità del mercato implica un cambiamento nei contenuti del diritto all'informazione garantito al consumatore, che deve orientare le sue scelte in modo sostenibile. In tale ottica la tutela del consumatore, ben oltre il rapido e aggressivo svolgimento dei meccanismi di consumo, dovrà svolgersi nella direzione di privilegiare scelte coerenti e un mercato equo, sostenibile e solidale. Ciò non comporterà la prevalenza del produttore rispetto al consumatore, ma la priorità della tutela ambientale di fronte alla quale si conformeranno tanto il professionista/produttore o fornitore di servizi, quanto il consumatore nel senso del perseguimento degli obiettivi connessi alla sostenibilità del mercato¹⁰. In quest'ottica potrebbe aver senso un intervento sulla tutela consumeristica nella fase della formazione della determinazione volitiva prodromica alla conclusione del contratto, attraverso l'introduzione di una certificazione delle recensioni relative al prodotto, al fine di ridurre la possibilità che il bene oggetto di compravendita non abbia le caratteristiche promesse. A fronte di tale sorta di certificazione del «*rating*» del prodotto potrebbe venire meno la necessità di garantire il diritto di recesso al consumatore, non più consona ad un modello di acquisto sostenibile quanto a produzione di scarti ed imballaggi ed inutile movimentazione di merci sul territorio nazionale e/o internazionale.

7. Riflessioni sulle caratteristiche dei beni.

Se tutto ciò è vero, è parimenti vero, per altro verso, che la sostenibilità implica anche una riflessione sulle caratteristiche dei beni che nel consumo devono essere assolutamente trasparenti. In proposito interviene la Direttiva UE 2019/771 sulle garanzie per i beni di consumo¹¹, che modifica la disciplina della

⁹ Si veda in proposito, B. KEIRSBILCK, E. TERRY, A. MICHE e I. ALOGNA, *Sustainable Consumption and Consumer Protection Legislation*, Luxembourg, 2020, 20.

¹⁰ M. FABRE - MAGNAN, *What is a Modern Law of Contracts?*, in *Eur. Rev. Contr. Law*, 2017, 376.

¹¹ Direttiva adottata il 20 maggio 2019 prevede un nuovo quadro normativo in tema di conformità dei beni di consumo e abroga la precedente direttiva 1999/44/CE relativa a vendita di beni di consumo e garanzie associate recepite agli artt. 129-134 del decreto legislativo n. 206 del 6.9.2005 (codice del consumo). La direttiva intende coordinare la tutela del consumatore con la diffusione del commercio elettronico e con la centralità assunta dalla tecnologia. L'ambito soggettivo della direttiva è quello B2C e quello oggettivo è rappresentato dai beni mobili materiali anche con implicazioni digitali in termini di contenuto o fornitura di servizi digitali sia alla vendita online che a quella offline. Sono esclusi dall'ambito oggettivo i contratti di fornitura di contenuti o servizi digitali. In particolare, la definizione di bene ricomprende non solo qualsiasi bene mobile materiale, ma anche qualsiasi bene mobile materiale che necessita di contenuti digitali o di servizi digitali per funzionare (beni con elementi digitali). Sono inserite anche le definizioni di contenuto digitale (cioè i dati prodotti o forniti in formato digitale) e di servizio digitale, nonché quelle di compatibilità (capacità del bene di funzionare con hardware o software con cui sono normalmente utilizzati i beni del medesimo tipo, senza che sia necessario convertire i beni, l'*hardware* o il *software*), di funzionalità (la capacità del bene di svolgere tutte le sue funzioni in considerazione del suo scopo), e interoperabilità (la

conformità del bene oggetto di transazione, sostituendo il complesso quadro di presunzioni, di cui all'art. 2 della direttiva 1999/44/CE, con due distinti profili di conformità: l'uno inquadrabile dal punto di vista soggettivo (art. 6, dir. 771/2019/UE) e l'altro rilevante in senso oggettivo (art. 7). Tra questi, guardando alla sostenibilità, assume particolare significato la lettera d) dell'art. 7 che fa riferimento alla durabilità quale requisito oggettivo di conformità, in modo che il venditore sia obbligato a fornire al consumatore (art. 5) un bene che possieda la durabilità normale di un bene del medesimo tipo, che il consumatore può ragionevolmente aspettarsi (art. 7.1.d.).

A fronte dell'obbligo principale del venditore di consegnare al consumatore beni conformi al contratto di vendita, la direttiva stabilisce che il venditore debba garantire che al consumatore siano forniti gli aggiornamenti, compresi quelli di sicurezza, necessari per mantenere tali beni conformi nel tempo. In caso di difetto di conformità, rimangono fermi i rimedi posti a tutela del consumatore quali il ripristino della conformità del bene (ossia, la riparazione o la sostituzione), senza spese per il consumatore e la riduzione del prezzo o la risoluzione del contratto. Rimedi questi ultimi esperibili dal consumatore quando il venditore non ha completato la riparazione o la sostituzione o non l'abbia realizzata entro un periodo ragionevole, guardando al tempo in cui il venditore è stato informato dal consumatore in merito al difetto di conformità, oppure quando il venditore ha rifiutato di ripristinare la conformità dei beni. Qualora permanga un difetto di conformità, nonostante il venditore abbia tentato di ripristinare la conformità dei beni o il difetto di conformità sia così grave, il consumatore potrà esperire il rimedio dell'immediata riduzione del prezzo o della risoluzione del contratto di vendita. Tuttavia, il consumatore non ha diritto di risolvere il contratto se il difetto di conformità è di lieve entità (l'onere sull'entità del difetto di conformità è a carico del venditore). Nel caso, infine, in cui il difetto di conformità si riferisca solo a uno, o ad alcuni, dei beni forniti nell'ambito dello stesso contratto di vendita e vi sia un motivo per la risoluzione del contratto di vendita solo in relazione ad alcuni tali beni, il consumatore può risolvere il contratto anche in relazione agli altri beni sebbene conformi, qualora non si possa ragionevolmente presumere che il consumatore accetti di tenere solo i beni conformi.

8. Responsabilità del venditore, onere della prova e denuncia.

Come è evidente il venditore, così come già previsto dalla precedente direttiva 1999/44/Ce e dal codice del consumo continua ad essere responsabile nei confronti del consumatore per qualsiasi difetto di conformità esistente al momento della consegna o che si manifesti entro due anni dalla consegna. Rimane ugualmente fermo il principio dell'inversione dell'onere della prova, ma ne è stato esteso il termine di presunzione: infatti, in base alla nuova direttiva 2019/771, qualsiasi difetto di conformità che si manifesti entro un anno dal momento della consegna si presume già esistente al momento della consegna

capacità del bene di funzionare con *hardware* o *software* diversi da quelli con cui sono normalmente utilizzati i beni dello stesso tipo).

(con possibilità per gli Stati membri di allungare il periodo fino a due anni¹²). Resta vigente la disposizione che consente agli Stati membri di prevedere che gravi sul consumatore, per l'esercizio dei suoi diritti, l'onere di denunciare al venditore il difetto di conformità entro un periodo di (almeno) due mesi dalla data in cui ha constatato il difetto. Mentre per quanto riguarda la vendita di beni di seconda mano, le parti possono concordare una responsabilità o un termine di prescrizione più breve, a condizione, però, che tale periodo non sia inferiore a un anno.

9. Garanzia e diritto di regresso.

Circa la garanzia convenzionale, definita «garanzia commerciale», deve essere fornita al consumatore su un supporto durevole, al più tardi al momento della consegna della merce. La garanzia commerciale deve includere una dichiarazione chiara che stabilisca che il consumatore dispone per legge di rimedi a titolo gratuito, in caso di difetto di conformità dei beni, e che tali rimedi non sono pregiudicati dalla garanzia commerciale; la chiara indicazione del nome e dell'indirizzo del garante; la procedura che il consumatore deve seguire per ottenere l'applicazione della garanzia commerciale; la designazione dei beni ai quali si applica la garanzia commerciale e le condizioni della garanzia commerciale. Recepite queste previsioni minime, gli Stati membri possono stabilire norme su altri aspetti relativi alle garanzie commerciali che non sono regolate dalla direttiva 2019/771. Nel caso in cui, poi, le condizioni stabilite nella garanzia commerciale siano meno vantaggiose per il consumatore, rispetto alle condizioni stabilite nella relativa pubblicità, la garanzia commerciale vincola il venditore secondo quanto previsto nella pubblicità.

Il nostro Stato, oltre a rispettare il termine di recepimento della direttiva, ha previsto una tutela più rigorosa rispetto a quanto sancito nella direttiva, andando oltre la massima armonizzazione tra le discipline dei vari paesi UE¹³. In particolare, con il d.lg. 4 novembre 2021, n. 170 viene esteso l'ambito oggettivo sino a ricomprendervi beni con elementi digitali e animali vivi. Sono previste, poi, specifiche disposizioni in materia di aggiornamento dei beni, nello specifico di quelli digitali, e di errata installazione, con modifica degli artt. da 128 a 135 del c. cons., ove sono stati inseriti gli articoli dal 135 *bis* al 135 *septies*. Il titolo III, il capo I, precedentemente dedicato alla vendita di beni di consumo, ora riguarda solo la vendita di beni *tout court*. Nella definizione di venditore, viene ricompreso

¹² Ai sensi della direttiva 1999/44 e delle attuali norme del Codice del Consumo (art. 132), tale periodo di presunzione è limitato a sei mesi dalla consegna.

¹³ S. PAGLIANTINI, *Contratti di vendita di beni: armonizzazione massima, parziale e temperata della Dir. UE 2019/771*, in *Giur. it.*, 2020, 217; F. ADDIS, *Spunti esegetici sugli aspetti dei contratti di vendita di beni regolati nella nuova direttiva (UE) 2019/771*, in *Nuovo dir. civ.*, 2020, 5; E. FERRANTE, *La direttiva 19/771/UE in materia di vendita al consumo: primi appunti*, in *Annuario del contratto*, 2018, Torino, 2019, 23. Un giudizio negativo sulla mancata attenzione ai profili della sostenibilità proprio della direttiva, che entrerà in vigore a decorrere dal 1 gennaio 2022, è espresso, tra gli altri, da E. VAN GOOL e A. MICHEL, *The New Consumer Sales Directive 2019/771 and Sustainable Consumption: a Critical Analysis*, in <http://dx.doi.org/10.2139/ssrn.3732976>, e da V. MAKE e TERRY, *Circular Economy and Consumer Protection*, cit., 236.

anche «il fornitore di piattaforme se agisce per finalità che rientrano nel quadro della sua attività e quale controparte contrattuale del consumatore per la fornitura di contenuto digitale o di servizi digitali». Sono presenti anche le definizioni relative ai contenuti digitali, al servizio digitale, alla compatibilità, interoperabilità e al supporto durevole. In relazione ai contratti di fornitura di contenuti digitali o servizi digitali, le disposizioni in parola si applicano ai contenuti digitali o ai servizi digitali incorporati o interconnessi con beni, i quali sono forniti con il bene in forza del contratto di vendita, indipendentemente dal fatto che i predetti contenuti digitali o servizi digitali siano forniti dal venditore o da terzi. Lì dove è bene precisare che per bene si intende qualsiasi bene mobile materiale anche da assemblare, l'acqua, il gas e l'energia elettrica quando sono confezionati per la vendita in un volume delimitato o in quantità determinata e anche i beni usati. Il contratto di vendita viene equiparato alla permuta, somministrazione, appalto, contratto d'opera e ad ogni altro contratto finalizzato alla fornitura di beni da fabbricare o produrre. Con riferimento al diritto di recesso, la normativa è quasi invariata, fatto salvo un inciso relativo, come già notato in precedenza, ai beni e servizi digitali. Come il venditore finale, se responsabile verso il consumatore per un difetto di conformità dipendente dalla condotta di una persona nei passaggi precedenti della medesima catena contrattuale distributiva, compresa l'omissione di fornire gli aggiornamenti per i beni con elementi digitali, ha diritto di regresso nei confronti della persona o delle persone responsabili nella catena di transazioni commerciali. Relativamente ai contratti di fornitura di beni con elementi digitali, il venditore, ai sensi dell'art. 133 comma 2, c. cons., viene considerato responsabile per il difetto di conformità entro due anni (o più di due anni) a seconda della durata della fornitura continuativa del prodotto o servizio digitale oggetto della vendita e, qualora il contenuto digitale o il servizio digitale non sia conforme, spetterà al venditore l'onere della prova per qualsiasi difetto di conformità che si manifesti entro quel termine.

Quanto, infine, alla tutela rimediabile a disposizione del consumatore, il nuovo art. 135 *bis* non apporta alcuna modifica. Infatti, ai fini del ripristino alla conformità del bene, il consumatore può sempre scegliere tra riparazione e sostituzione, purché il rimedio prescelto non sia impossibile o eccessivamente oneroso per il venditore, con riferimento al valore del bene in assenza del difetto, all'entità del difetto e alla possibilità di esperire il rimedio alternativo, senza inconvenienti per il consumatore. Il consumatore ha sempre diritto alla riduzione proporzionale del prezzo o alla risoluzione del contratto se il venditore non ha provveduto alla riparazione o sostituzione del bene, se si manifesta un difetto di conformità nonostante il tentativo di ripristino del bene, se il difetto di conformità è così grave da giustificare la riduzione del prezzo o la risoluzione, se il venditore ha dichiarato che non procederà al ripristino della conformità entro un termine ragionevole. *A contrario*, il consumatore non ha il diritto di risolvere il contratto se il difetto di conformità è lieve e spetta al venditore dimostrarlo. Inoltre, il consumatore potrà rifiutarsi di eseguire il pagamento di qualsiasi parte di prezzo fino a quando il venditore non abbia adempiuto agli obblighi previsti a suo carico. Restano, naturalmente, ferme le disposizioni del c.c. che disciplinano l'eccezione di inadempimento e il concorso del fatto del consumatore.

Sembra adottare, invece, l'ottica della circolarità dei cicli di vita dei prodotti il novellato art. 135 *ter*, il quale dispone che la riparazione o sostituzione devono

avvenire senza spese, entro un congruo lasso di tempo, senza notevoli inconvenienti per il consumatore che avrà diritto ad una riduzione del prezzo proporzionale alla diminuzione di valore del bene. La risoluzione del contratto verrà esercitata mediante dichiarazione diretta al venditore. Se il difetto di conformità riguarda solo alcuni dei beni consegnati, il contratto può essere risolto limitatamente ad essi. In caso di risoluzione, il consumatore dovrà restituire il bene al venditore a spese di quest'ultimo e il venditore ha l'obbligo di rimborsare al consumatore il prezzo pagato per il bene al momento di ricevimento e per le eventuali prove fornite dal consumatore in ordine al fatto di aver restituito o spedito il bene.

Alla garanzia legale di conformità si aggiungono, senza sostituirle o limitarle, le garanzie convenzionali, di diversa ampiezza e/o durata. Chiunque offra garanzie convenzionali deve sempre specificare che si tratta di garanzie diverse e aggiuntive rispetto alla garanzia legale di conformità che tutela i consumatori. Le garanzie convenzionali concernenti la durabilità di determinati beni nell'arco di un determinato periodo di tempo, obbliga il produttore alla riparazione o alla sostituzione dei beni durante l'intero periodo di durata della garanzia. La dichiarazione di garanzia convenzionale viene fornita al consumatore su supporto durevole ed è redatta con linguaggio semplice e comprensibile. Ai sensi dell'art. 135 *sexies* è nullo qualsiasi patto volto a limitare o eludere le garanzie previste a favore del consumatore. Per quanto non sia espressamente previsto, la novella rinvia alle norme del Codice civile in tema di formazione, validità ed efficacia dei contratti, comprese le conseguenze della risoluzione del contratto e il diritto al risarcimento del danno. Le nuove norme sono in vigore dal 1° gennaio 2022 e si applicano esclusivamente ai contratti conclusi successivamente a tale data.

Conclusioni.

Dalla disamina effettuata si può giungere alla conclusione che l'acquisita consapevolezza della necessità di ridurre il rifiuto e il *favor* verso il riutilizzo o il riciclo o riuso, unitamente alla trasparenza del prodotto ottenuta attraverso un'etichettatura sempre più esplicita ben può incidere sulle scelte di consumo e far propendere verso l'acquisto di beni durevoli, riciclabili o fatti con materiali riciclati, utilizzabili a lungo attraverso manutenzioni e riparazioni efficaci e minimizzazione dei rifiuti generati al termine del ciclo di vita. Alternativa valida in tal senso è l'opzione verso prodotti biodegradabili non inquinanti. In ciò consiste la nuova tipologia di consumo: il consumo critico.

L'acquisizione della consapevolezza della doverosità verso sè stessi e verso il prossimo della riduzione dello spreco rappresenterà la svolta per l'instaurazione dei principi dell'economia circolare e la transizione verso la vera sostenibilità economica.





Piattaforme digitali e contratto. Digital platforms and contracts.

ROBERTO CARLEO

Full Professor of Private Law at Università degli Studi di Napoli
Parthenope
Lawyer

Abstract

La disciplina del contratto è – come tutta la società – rivoluzionata dall'avvento delle piattaforme digitali. Nascono nuovi soggetti, beni, opportunità e problemi, che pongono l'esigenza di nuove discipline e finanche di nuove tecniche normative idonee a regolamentare lo spazio a-territoriale di internet. Rispetto alla concezione tradizionale del mercato, la disciplina degli scambi che avvengono nella E-Agorà sfugge alla sovranità dei legislatori dei singoli stati territoriali e richiede la virtuosa collaborazione dei protagonisti e, in particolare, proprio delle piattaforme digitali, in un'ottica di co-regolazione tra pubblico e privato, agevolata dal ruolo delle Authorities di settore, anche in applicazione del principio di sussidiarietà.

Contracts regulation is - like the whole society - revolutionised by the advent of digital platforms. New subjects, goods, opportunities, and problems arise, creating the need for new disciplines and even new regulatory techniques capable of regulating the a-territorial space of the Internet. Compared to the traditional conception of the market, the regulation of the exchanges that take place in the E-Agorà escapes the sovereignty of the legislators of the single territorial states and requires the virtuous collaboration of the protagonists and, in particular, of the digital platforms, in a perspective of co-regulation between public and private, facilitated by the role of the sector



Keywords: Digital Platforms; Contracts.

Summary: [1. Introduzione: La rivoluzione del contratto nell'era della digitalizzazione.](#) – [2. Il problema dell'applicazione della legge e della sovranità degli Stati nello spazio a-territoriale e globale della rete: una soluzione adottata dal GDPR con il c.d. principio di *accountability*.](#) – [3. Alcuni nuovi problemi del contratto nel sistema di internet e della *blockchain*.](#) – [4. Responsabilità delle piattaforme nei confronti degli utenti e regole di concorrenza: il caso Bolger vs Amazon.](#) – [5. Conclusione: Il ruolo delle piattaforme \(*Over The Top*\) tra co-regolazione e sussidiarietà.](#)

1. Introduzione: La rivoluzione del contratto nell'era della digitalizzazione.

L'erompere delle piattaforme digitali ha rivoluzionato la disciplina e la stessa struttura del contratto¹.

Non può non riverberarsi anche sul diritto l'impatto della digitalizzazione e della "datificazione" della società².

Nella "E-Agorà" si affermano nuove tecniche di realizzazione dello scambio di beni e servizi che non sembra possibile ricondurre pianamente alla disciplina tradizionale dettata dal codice civile.

Il diritto non può rimanere estraneo al fenomeno, poiché il mercato (anche digitale) è "*locus artificialis*" necessariamente costituito dal diritto stesso, secondo le celebri osservazioni di Irti³.

La legislazione speciale, specie di derivazione europea, ha introdotto nuove regole che non sono risultate suscettibili di essere recepite e coordinate nel codice civile, mediante la tecnica della *novella*, ma restano affermate in diverse fonti di cognizione, costituite da una moltitudine di leggi speciali, talvolta consolidate in "*codici di settore*", oltre che da regolamenti e da molte altre nuove fonti, soprattutto di autoregolazione o di co-regolazione, in ossequio al principio di sussidiarietà orizzontale sancito dall'art. 118 Cost.⁴.

Il problema non è ovviamente limitato ai confini nazionali, ma è un problema globale che riguarda tutto il mondo ed esige regole uniformi in tutti i territori esistenti dove arriva la rete. La legislazione italiana sul punto diventa ben poco rilevante, se non quando è destinata a recepire ed attuare direttive europee, ma anche i confini dell'Europa rappresentano solo una piccola parte della ben più vasta area di riferimento, da intendersi come totale, universale e sconfinata.

La rivoluzione del contratto, oggi in pieno atto, venne colta in anticipo da Natalino Irti nel celebre saggio "*Scambi senza accordo*"⁵, che può essere

¹ Lo scritto riprende il testo della Relazione tenuta alla presentazione del Progetto di Ricerca Prin 2020 "E-AGORA" - *Online Platform Contracts: economic efficiency and rights' protection of service users. Technological innovation and service sharing in a social world*, tenutasi il 1 luglio 2022 presso l'Università degli Studi di Napoli "Parthenope", Villa Doria d'Angri.

² Su cui, proprio in apertura di questi lavori, abbiamo ascoltato le parole di Maurizio Ferraris, e rinviando al suo libro: M. FERRARIS, *Documanità* (Laterza 2021).

³ Così N. IRTI, *L'ordine giuridico del mercato*, Bari, 1998.

⁴ Si rinvia alle ricerche raccolte nei volumi a cura di MARIO NUZZO in AA.VV., *Il principio di sussidiarietà nel diritto privato*, Torino, 2014,

⁵ N. IRTI, *Scambi senza accordo*, in *Riv. Trim. Dir. Proc. Civ.*, 1998, p. 347 ss.

considerato un antesignano manifesto del commercio elettronico.

Irti - già dalla fine dello scorso secolo - ha precorso la dissoluzione del contratto in una combinazione di atti unilaterali convergenti.

Non più un accordo, ovvero un incontro di volontà realizzato mediante una negoziazione espressa attraverso un dialogo umano (*homo loquens*), bensì una meccanica scelta di soluzioni predeterminate, imm modificabili ed omologate, selezionate attraverso gesti meccanici e comportamenti concludenti silenziosi di entrambe le parti del contratto (*homo videns*), quali possono essere sia la fisica esposizione della merce offerta in un grande magazzino (reale o virtuale) a condizioni prestabilite, sia la collocazione della stessa merce nel carrello del consumatore, sia il *click* di un tasto o di un *touch screen* su un terminale elettronico (*computer, tablet, smartphone* etc.).

Il passaggio dal mercato reale a quello virtuale (oggi non più consistente solo in veicolo per lo scambio di beni o servizi reali, ovvero fruibili nella realtà concreta, bensì anche come spazio virtuale per lo scambio di beni e servizi che non vengono ad esistere nel mondo reale ma restano confinati nel “*metaverso*”) pone una infinita serie di nuove opportunità e di nuove sfide, che non possono enunciarsi in poche battute.

Le novità normative, specie derivanti dalla legislazione europea, sono tantissime, recentissime ed in continua evoluzione.

Una fonte europea fondamentale per la regolazione dei contratti con le piattaforme digitali è il Regolamento 2019/1150/UE, volto a garantire che i rapporti contrattuali tra i fornitori di servizi di intermediazione *online* e le imprese che si avvalgono delle piattaforme per offrire al pubblico beni e servizi (c.d. “*utenti commerciali*”) siano condotti secondo correttezza e buona fede.

Ma ancora più recente, nella direzione della responsabilizzazione delle piattaforme digitali e della rimozione delle “*asimmetrie informative*”⁶, è il *Digital Service Act* (DSA), ovvero il disegno di legge che impone alle *Big Tech* una maggiore responsabilità sui contenuti illegali o nocivi che circolano sulle loro piattaforme, sul quale appena un paio di mesi fa la Commissione Europea ha raggiunto un accordo politico.

Ed in queste stesse recentissime date sono state varate o sono in corso di approvazione altre fonti importanti (*Data Governance Act* e *Data Act*), nella direzione di regolare i profili diventati fondamentali dei “dati” e della loro tutela⁷, restando sempre in attesa del (possibile) nuovo accordo tra la Commissione Europea ed il Governo degli U.S.A. sul trasferimento extra UE dei dati personali degli utenti, a seguito della nota bocciatura del c.d. *Privacy Shield* ad opera della Corte di Giustizia UE⁸.

In questa sede non è possibile, né utile, passare in rassegna le singole novità

⁶ Le conseguenze in termini di validità del contratto e di responsabilità delle piattaforme sono studiate dalla unità di ricerca dell'Università Cattolica di Milano, con il prof. Antonio Albanese.

⁷ Oggetto di studio della unità di ricerca dell'Università di Verona, con il prof. Riccardo Omodei Salè. Questo PRIN si propone, ovviamente, di analizzare e di studiare tutta la normativa di riferimento, anche con il beneficio dell'accordo di collaborazione con AGCOM (con cui abbiamo il privilegio di poter collaborare, come abbiamo ascoltato dal Presidente e dagli autorevoli dirigenti che sono qui intervenuti) che consentirà di attingere al prezioso serbatoio dei dati concreti raccolti dall'Autorità anche per la cura di un apposito osservatorio sulle piattaforme digitali.

⁸ Si rimanda per un'ampia e completa ricostruzione del dibattito al volume *La protezione transnazionale dei dati personali. Dai “Safe harbour principles” al “Privacy Shield”*, a cura di G. RESTA e V. ZENO-ZENCOVICH, Roma, 2016.

o tentare di ricostruire un quadro normativo aggiornato.

Ciò che si intende qui evidenziare è, piuttosto, la rivoluzione che avviene non solo nella disciplina e nelle sue fonti, ma anche nelle stesse tecniche di regolazione della rete.

2. Il problema dell'applicazione della legge e della sovranità degli Stati nello spazio a-territoriale e globale della rete: una soluzione adottata dal GDPR con il c.d. principio di *accountability*.

Internet è uno spazio a-territoriale, di talché pone innanzitutto il problema della applicazione del diritto, quale che sia il contenuto dello stesso.

In altri termini, prima ancora di porre le regole del contratto, occorre stabilire *chi* debba dettarle e, soprattutto, *come* lo Stato possa garantire la coercibilità di queste regole.

Lo Stato esercita il proprio potere (solo) sul proprio territorio, ma la norma da applicare in uno spazio (a-territoriale) pone un problema di sovranità⁹.

Non a caso in Europa nell'ambito di alcuni mercati regolati (ad esempio per le assicurazioni) si impone che le imprese utilizzino sistemi di *cloud computing* che abbiano i propri server localizzati in paesi determinati e comunque entro i confini del territorio della Unione Europea¹⁰.

Tuttavia (a parte alcune eccezioni, come quella appena menzionata, in cui è stato possibile imporre dei limiti) in generale i tentativi di ricondurre lo spazio "libero" della rete nel territorio fisico in cui si trovano i server si sono rivelati inadeguati, poiché è fin troppo facile, con gli strumenti tecnologici, eludere la territorialità ed accedere in maniera anonima e non agevolmente tracciabile con il riferimento ad un determinato territorio.

Eloquente appare il caso delle norme sulla *privacy* (o, meglio, sul trattamento dei dati personali) ove il legislatore europeo del GDPR ha escogitato un sistema nuovo ed originale per consentire l'applicazione delle norme anche oltre il territorio europeo.

Questa soluzione consiste nell'abbandonare la regola di dettaglio posta dal legislatore, scegliendo invece di responsabilizzare un determinato regolatore (il "*data controller*"), ovvero un soggetto che viene appositamente selezionato come colui il quale ha il potere di regolare, ma nel contempo deve altresì rispondere della adeguatezza delle regole che avrà dettato rispetto agli obiettivi che il legislatore si limita ad enunciare astrattamente in termini di principi generali.

Questo passaggio "*dalla regola al regolatore*"¹¹ è segnato dalla introduzione del c.d. principio di *accountability*, che rappresenta per il nostro paese una novità e può essere tradotto con responsabilità e insieme prova della stessa responsabilità: esso è sovente tradotto come "principio di rendicontazione" o "di responsabilità" e consiste nell'obbligo di conformarsi e di dimostrare.

Il significato della parola "*accountability*" presenta una difficoltà di traduzione

⁹ Come bene ha osservato sempre N. IRTI, *Norma e Luoghi. Problemi di geo-diritto*, Roma-Bari, 2001.

¹⁰ Sul punto cfr. F. TRUBIANI, *I servizi di cloud computing tra tutela del consumatore e sostenibilità digitale*, Padova-Milano, 2022.

¹¹ Ci si consenta il rinvio a R. CARLEO, *Il principio di accountability nel GDPR: dalla regola alla auto-regolazione*, in *Nuovo dir. civ.*, 2021, 1, p. 359 ss. (consultabile al link: <https://www.dikegiuridica.it/admin/file/NDC1-21-Carleo.pdf>).

in lingua italiana giacché contiene in sé contestualmente vari significati, quali quelli di libertà, responsabilità, prova e rendicontazione. L'affermazione legislativa di questo principio segna una nuova tecnica normativa capace di estendere l'efficacia della disciplina della protezione dei dati personali ovunque nello spazio della rete, anche oltre i limiti del territorio europeo.

Il legislatore abbandona la regola di dettaglio e affida ad un “*regolatore responsabilizzato*” – il *data controller* – la scelta delle soluzioni più adeguate per il raggiungimento dell'obiettivo, della cui idoneità il *data controller* poi verrà chiamato a rispondere ove insorgano problemi.

Ed è così che - grazie a questo “*geniale*” espediente che consente lo “*scollamento tra legge e territorialità*”¹² - la protezione dei dati personali dovrebbe funzionare indipendentemente dal territorio degli Stati, ovvero anche in uno spazio a-territoriale, qual è appunto quello di internet.

3. Alcuni nuovi problemi del contratto nel sistema di internet e della blockchain.

I nuovi problemi del contratto – così come le nuove opportunità che si dischiudono – nel sistema di internet e della *blockchain* sono innumerevoli e non è certo possibile in questa sede darne conto, se non con qualche sporadico accenno, a mo' di rapido volo d'uccello, solo su qualcuno di essi.

Basti pensare, ad esempio, ai nuovi soggetti protagonisti del mercato che nascono proprio grazie alle piattaforme digitali e difficilmente potrebbero altrimenti esistere, tra i quali innanzitutto il *prosumer*¹³, ovvero un consumatore che riesce ad assumere nel contempo anche l'opposta qualità soggettiva di professionista, offrendo - grazie alla efficienza della rete (che supplisce alla necessità di dotarsi di una organizzazione aziendale adeguata per l'esercizio dell'impresa) - lo scambio di beni o servizi¹⁴.

Oppure si pensi, dal punto di vista degli oggetti, alla irruzione nel mercato di nuovi beni “virtuali”, privi di consistenza materiale¹⁵, quali i *bitcoin* o altre criptovalute, nonché i *Non Fungible Token*, che attualmente imperversano soprattutto nel mercato dell'arte, permettendo di certificare la “rarità digitale” di un bene, sfruttando (come già avviene anche per le criptovalute) la tecnologia *blockchain*, ovvero un equivalente digitale di un registro delle transazioni.

Ed ancora sempre la *blockchain* pone nuove affascinanti opportunità in tema di forma, prova e pubblicità degli atti giuridici, tanto da fare ipotizzare una semplificazione di procedure e regole vigenti per la circolazione di taluni diritti.

Più in generale, è la stessa nozione di “documento” che viene ad essere ampliata a dismisura a seguito della moltitudine dei dati che vengono generati digitalmente e che possono essere conservati e riprodotti su diversi supporti¹⁶, al punto che sembra suscettibile di essere superata persino la stessa nozione tradizionale di forma scritta o quella di prova scritta.

¹² Sono parole di L. FLORIDI, *Il verde e il blu. Idee ingenue per migliorare la politica*, Milano, 2020, p. 28 s.

¹³ Fortunata locuzione che si deve a A. TOFFLER, *The third wave*, New York, 1980.

¹⁴ Sul punto si veda R. BOCCHINI, *La polivalenza delle posizioni contrattuali nella sharing economy*, in *Nuovo dir. civ.*, 2021, 1, p. 246 ss.

¹⁵ Cfr. BYUNG CHUL HAN, *Le non cose*, titolo originale: “*Unding*”, 2021

¹⁶ Cfr. ancora M. FERRARIS, *Documanità*, cit.

Tuttavia il tema della conservazione dei dati digitali apre anche a dubbi sulla capacità e sulla resistenza futura della memoria digitale, inducendo spesso a ritenere che i dati digitali - a differenza del vecchio e tradizionale supporto cartaceo - possano essere esposti ad inopinati *black out* per varie cause, quali cataclismi naturali o attacchi di pirati informatici (come - sia pure assai raramente - già è accaduto).

La stessa obsolescenza (anche programmata)¹⁷ del *software* (oltre che dell'*hardware*) necessario per leggere i dati digitali potrebbe contribuire ad accrescere il rischio di “*generazioni dimenticate*” o di “*buchi neri nella storia*”¹⁸.

Inoltre la conservazione della sempre crescente mole di dati (che richiederebbe uno spazio che pare non essere illimitato, di talché si impone comunque la necessità di scegliere dati da cestinare per sempre) pone anche l'opposto problema del *diritto all'oblio* (trattato dalla Corte Europea nel celebre caso *Google Spain*, che concede agli utenti interessati il diritto di “*deindicizzare*” taluni dati ritenuti sconvenienti, rendendoli con ciò di non immediata visibilità e reperibilità, pur senza cancellarli).

Il tema della conservazione dei dati pone anche quello della trasmissione ereditaria: i dati personali sono beni? Seguono le regole della successione ereditaria? Le risposte sono diverse. Probabilmente va operata una distinzione tra i dati, a seconda delle informazioni che essi contengono. Sul punto, in particolare con riguardo alla successione - o meglio all'accesso - all'*account* del defunto si registrano risposte diverse nei diversi ordinamenti: mentre negli Stati Uniti le richieste di accesso vengono tendenzialmente negate (salvo che con riferimento a dati specifici, quali le mail direttamente intercorse con il richiedente) seguendo fedelmente solo la volontà espressa dal *de cuius*, il cui *account* viene chiuso al momento della morte, viceversa in Europa si tende ad ammettere una successione universale anche nell'*account* (così in Germania) oppure - in Italia - si ammette un diritto di accesso (invero indiscriminato) da parte dei “*congiunti*” che facciano richiesta al provider adducendo “*ragioni familiari meritevoli di protezione*” (ai sensi dell'art. 9, comma 3 del Codice della Privacy (D.Lgs. 196/2003, come modificato dall'art. 2 *terdecies* D.lgs. n. 101/2018).

Sulla base di tale norma, nell'ultimo anno alcuni Tribunali italiani (¹⁹ hanno accolto dei ricorsi di urgenza promossi contro il gestore (Apple) volti ad ottenere le *password* dell'*account* personale del *de cuius*, prima che esso fosse disabilitato, come previsto dal contratto.

In particolare i suddetti Tribunali hanno condiviso la argomentazione secondo cui la clausola contrattuale che prevede la intrasferibilità del profilo personale (*account*) non sarebbe oggetto di un valido consenso espresso dall'utente.

Ma la soluzione suscita non poche perplessità se si pensa - tra l'altro - che l'accesso indiscriminato dei congiunti al profilo di un utente deceduto (che non avrebbe espresso alcun consenso tantomeno alla divulgazione dei propri dati e men che meno di tutti essi) ben potrebbe coinvolgere anche profili di tutela della

¹⁷ Qui il riferimento va all'opera di S. LATOUCHE, *Usa e getta. Le follie dell'obsolescenza programmata*, Torino, prima ed. 2012 (trad. F. Grillenzoni).

¹⁸ Ci si consenta il rinvio a R. CARLEO, *il futuro della memoria digitale*, in *La Magistratura*, Fascicolo N.1/2022 (consultabile al link: <https://lamagistratura.it/informatica-e-nuove-tecnologie/il-futuro-della-memoria-digitale-2/>).

¹⁹ Ci si riferisce ai Tribunali di Milano (ord. 9 febbraio 2021), Bologna (ord. 25 novembre 2021) e Roma (ord. 10 febbraio 2022 n. 2688).

riservatezza dei dati personali di terzi, che invece dovrebbero senz'altro essere protetti.

Si pone quindi un problema di validità di espressione del consenso del titolare dei dati, che ben potrebbe essere superato - prima che dal legislatore (che potrebbe finire per esigere una "quarta firma" sui contratti, relativa appunto alla intrasferibilità dei dati) - dalle stesse piattaforme, le quali potranno autonomamente prevedere e organizzare dei meccanismi che consentano agli utenti (appositamente resi edotti) di esprimere chiaramente le proprie scelte, come in taluni casi già sta avvenendo (si pensi ad esempio ai profili commemorativi di *facebook*).

Anche sotto tale profilo, emerge il problema centrale per la disciplina dei contratti conclusi con o attraverso piattaforme digitali in relazione ai requisiti di validità del consenso espresso dagli utenti: esso impone una revisione delle regole in materia di vizi della volontà, unitamente a quelle della correttezza e della trasparenza delle informazioni che devono essere garantite, nonché quelle della prevenzione e repressione delle pratiche commerciali scorrette.

Ed anche nuove procedure alternative alla giurisdizione ordinaria (anch'essa rivoluzionata dalla digitalizzazione grazie all'introduzione del processo telematico) per la risoluzione delle controversie *online* (ODR) si vanno sviluppando attraverso le piattaforme digitali, che consentono di implementare sistemi sempre più rapidi, efficienti ed economici, con la garanzia della gestione e della sorveglianza dello Stato attraverso le Autorità amministrative indipendenti (e in particolare dell'AGCOM).

Da ultimo, ma non certo in ordine di importanza, non può omettersi un cenno, tra i molti altri profili che dovrebbero essere richiamati, al tema degli *smart contracts* e della intelligenza artificiale, la quale penetra anche nei meccanismi di costituzione ed esecuzione del contratto.

È forse ancora presto per definire i temi della personalità giuridica o della capacità giuridica delle macchine (sulla cui possibile vita o sulla cui reale autonomia dall'uomo la maggioranza degli interpreti nutre ancora un radicale scetticismo) ma si tratta di problemi che devono essere certamente affrontati in concreto e che sono stati già inseriti nell'Agenda del legislatore europeo.

4. Responsabilità delle piattaforme nei confronti degli utenti e regole di concorrenza: il caso Bolger vs Amazon.

L'analisi dei profili del contratto coinvolge necessariamente quella delle conseguenze della violazione delle regole, le cui sanzioni oscillano tra rimedi demolitori (ovvero la invalidità dei contratti) o risarcitori (ovvero la responsabilità delle piattaforme nei confronti degli utenti).

Le piattaforme hanno fino ad oggi (verosimilmente anche con le ultime normative in corso di approvazione) goduto di una esenzione dal coinvolgimento nella responsabilità su ciò che esse si limitano ad intermediare come meri "ospiti" di altri che negoziano tra loro, senza assumere alcuna "paternità" dei contenuti che vengono veicolati (si pensi alla estraneità dell'*host provider* rispetto a contenuti illeciti che transitano sulla piattaforma), ponendosi peraltro dei delicatissimi problemi intorno al ruolo di controllo (che rischierebbe di degenerare

in censura) che le piattaforme medesime svolgono per impedire (o ridurre) la circolazione dei contenuti che esse valutano come illeciti o meritevoli di essere in qualche misura confinati, se non del tutto rimossi.

Ha suscitato grande scalpore, appena due anni fa, il caso *Angela Bolger vs Amazon.Com*²⁰, nel quale la Corte d'appello della California ha condannato Amazon a rispondere in solido del risarcimento del danno subito da una signora che – tramite la piattaforma - aveva acquistato un prodotto (una batteria per un laptop) da un terzo venditore e produttore, che tuttavia era “consigliato” dalla piattaforma.

Ebbene, questa decisione non è affatto un danno per Amazon, ma anzi ne amplifica il potere planetario nel commercio elettronico: i consumatori preferiranno comprare attraverso questa piattaforma nella consapevolezza che l'affidamento riposto sulla stessa opera come garanzia della sicurezza dei prodotti, della quale risponderà – oltre al venditore e produttore diretto responsabile – anche l'intermediario commerciale che ha consigliato il prodotto medesimo.

La decisione è motivata dalla Corte proprio in ragione della autorevolezza e della credibilità planetaria di Amazon, che, se consiglia un prodotto, suscita il legittimo affidamento degli utenti e pertanto deve farsene garante in caso di danni.

Ed allora appare lecito domandarsi: il consumatore potrà godere di simile protezione anche se acquista in altri mercati o attraverso altri intermediari? Probabilmente no. E dunque questa ulteriore garanzia del consumatore opera come regola di concorrenza tra imprese, che finisce per favorire sempre maggiormente quelle più forti, che sono capaci di offrire maggiori garanzie e si rendono pertanto più appetibili (non solo per i consumatori ma anche per i produttori) rispetto a quelle altre che non hanno la forza di sopportare gli oneri delle forme di tutela dei consumatori.

5. Conclusione: Il ruolo delle piattaforme (*Over The Top*) tra co-regolazione e sussidiarietà.

Internet è un osservatorio privilegiato del *rapporto tra diritto e tecnica* (si pensi ai dialoghi di Natalino Irti con Emanuele Severino e Luigi Mengoni)²¹).

Può il diritto regolare i nuovi fenomeni del progresso della tecnica, oppure ne resta inesorabilmente travolto?

Le difficoltà che incontra il diritto sono evidenti e in parte ne abbiamo già trattato con riguardo ai problemi della a-territorialità della rete.

Già abbiamo ricordato che il mercato è *locus artificialis* e non *locus naturalis*, di talché esso esiste in quanto è creato dal diritto, sia quando il legislatore interviene, sia quando adotti la scelta politica di non intervenire (seguendo la celebre frase di Talleyrand - secondo cui intervento e non intervento sono la stessa cosa - richiamata da Irti, sempre nel già citato *L'ordine giuridico del mercato*)²².

²⁰ *Angela Bolger vs Amazon.Com, LLC*, (2020 WL 4692387) Cal. Court of Appeal, 8/13/20.

²¹ Cfr. N. IRTI e E. SEVERINO, *Dialogo su diritto e tecnica*, Bari, 2001.

²² Cfr. nota 3.

È certo, dunque, che il diritto debba regolare la tutela dei soggetti e le attività del mercato digitale, sia nei rapporti contrattuali con gli utenti sia per i profili di concorrenza tra imprese²³.

Ma il diritto trova nuovi strumenti e nuovi fonti che consentono la creazione di regole adeguate di cui si impone comunque il rispetto.

Non rileva più solo il diritto *eterodeterminato* dal legislatore (che non riesce ad inseguire e catturare le fughe in avanti della tecno-economia) ma si espande soprattutto il diritto che nasce dalla *autodeterminazione* degli stessi soggetti destinatari delle norme.

Emerge la necessaria applicazione concreta del principio di sussidiarietà (positivizzato nel nostro ordinamento nell'art. 118 Cost. con la riforma costituzionale del 2001) per cui il legislatore arretra e lascia spazio alla formazione responsabile di regole create da parte dei privati o delle istituzioni sociali più prossime agli interessi da tutelare, che vengono delegate dal legislatore a dettare norme anche di interesse generale.

Le autorità pubbliche cooperano dunque con gli stessi privati ai quali è affidato il compito ed il ruolo di dettare le regole più adeguate e di garantirne l'osservanza, in un'ottica di co-regolazione che sembra emergere sempre più nitidamente.

Autodisciplina, codici di condotta e *soft law*²⁴ finiscono ineludibilmente per segnare le fonti delle nuove regole e la garanzia dell'efficiente funzionamento del mercato digitale.

Le piattaforme digitali si rivelano al di sopra degli Stati e della legge (*Over The Top*, così definite in quanto agiscono "*al di sopra delle reti*", essendo prive di una propria infrastruttura e avvalendosi di internet) e appaiono ormai troppo potenti per essere sottoposte alla coercizione dei legislatori dei singoli Stati sovrani (ciascuno nei limiti del proprio territorio)²⁵.

Esse tuttavia - grazie alla loro autodisciplina e cooperazione - si fanno carico di stabilire e di fare osservare le regole a garanzia del corretto funzionamento mercato e - pertanto - anche e soprattutto a vantaggio della propria esistenza (oltre che del proprio profitto).

²³ I temi sono studiati dall'unità di ricerca dell'Università di Roma Europea, con la Prof. Valeria Falce.

²⁴ Argomento studiato dall'unità di ricerca dell'Università di Perugia, con la Prof. Alessandra Bellelli.

²⁵ Cfr. F. BASSAN, *Digital Platforms and Global Law*, Cheltenham, 2021.



Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"

The regime of liability from things in custody between traditional issues and 'algorithm liability'

GIOVANNA D'ALFONSO 

Associate Professor of Private Law

Università degli Studi della Campania Luigi Vanvitelli

Abstract

Di recente, la dottrina si interroga sulla riconduzione delle nuove ipotesi di responsabilità civile per l'intelligenza artificiale nell'alveo di taluni modelli di responsabilità civile extracontrattuale, previsti dal nostro sistema ordinamentale e, nello specifico, se sia applicabile, in determinate fattispecie, l'articolo 2051 c.c., alla luce dei principi sviluppatasi in ambito giurisprudenziale. Il contributo evidenzia come la disciplina codicistica della responsabilità da cose in custodia sia tuttora oggetto di interpretazioni giurisprudenziali innovative in riferimento alla natura della responsabilità, di guisa da delineare schemi poliedrici.

Recently, doctrine has questioned whether the new cases of civil liability for artificial intelligence can be brought within the scope of certain non-contractual liability models provided for by our legal system and specifically whether, in certain cases, Article 2051 of the Civil Code is applicable, in light of the principles developed in case law. The contribution highlights how the codified regulation of liability for things in custody is still subject to innovative jurisprudential interpretations with reference to the nature of liability, so as to outline polyhedral schemes.



Keywords: liability from things in custody; case-law interpretations of the discipline; artificial intelligence; new cases of civil liability.

Summary: [1. Introduzione: La fattispecie di cui all'art. 2051 c.c. e sue applicazioni.](#) – [2. La qualificazione giuridica della responsabilità da cose in custodia tra responsabilità "aggravata" e responsabilità "oggettiva".](#) – [3. Modelli giurisprudenziali innovativi. Rilievi critici.](#) – [4. I "nuovi" danni da sistemi di intelligenza artificiale: riconducibilità agli schemi di responsabilità civile vigenti nel nostro ordinamento versus riforma legislativa.](#) – [5. L'invocabilità del regime della responsabilità da cose in custodia.](#) – [Conclusioni.](#)

1. Introduzione: La fattispecie di cui all'art. 2051 c.c. e sue applicazioni¹.

L'art. 2051 c.c. regola la responsabilità civile del custode della cosa per i danni da questa provocati, statuendo che «ciascuno è responsabile del danno cagionato dalle cose che ha in custodia, salvo che non provi il caso fortuito».

La norma costituisce una delle fattispecie tipizzate dal legislatore, secondo modelli diversi rispetto all'impostazione dettata dalla clausola generale dell'art. 2043 c.c., in forza del quale il sorgere della responsabilità civile extracontrattuale è strettamente correlato al vizio del comportamento del danneggiante, in termini di colpevolezza. Ai sensi dell'art. 2051 c.c., il danneggiato che richieda la tutela giurisdizionale ha infatti accesso ad un «regime probatorio semplificato», in quanto legittimato a richiedere il risarcimento del danno patito, in ragione del mero rapporto sussistente tra la *res* ed il soggetto che lo custodisca, senza dover provare che la condotta di quest'ultimo sia soggettivamente imputabile².

L'art. 2051 c.c. enumera tre presupposti, ai fini del sorgere della responsabilità³. *In primis*, il legislatore pone, alla base della responsabilità della persona per il danno cagionato dalla cosa, la "custodia", ossia la relazione qualificata intercorrente con la *res*⁴. Tale rapporto si concretizza nell'esercizio di un "potere di governo" che il custode esercita sulla cosa e che gli consente di controllarla, di intervenire sulla stessa, al fine di eliminare o quantomeno attenuare eventuali situazioni di pericolo e di escludere l'ingerenza di terzi⁵. Ai

¹ Questo lavoro è il risultato del Progetto di Ricerca finanziato "Diritto e Intelligenza Artificiale: nuovi orizzonti giuridici della personalità e responsabilità robotica" (PID2019-108669RB-I00 /AEI/10.13039/501100011033), di cui la Dott.ssa Margarita Castilla Barea è la principale ricercatrice.

² Cfr. B. DE SANTIS, Brevi note su recenti riletture giurisprudenziali dell'art. 2051 c.c., in www.judicium.it, p. 2.

³ Cfr. F. ALTAMURA, La responsabilità della P.A. per i danni cagionati dai beni demaniali: il caso fortuito e l'esempio della macchia d'olio, in commento alla pronuncia Cass.civ., sez. VI, ord., 3-20 febbraio 2019, n. 4963, in *Danno e resp.* 2019, p. 371.

⁴ Cfr. R. SCOGNAMIGLIO, voce «Responsabilità civile», in *Nov.Dig.it.*, XV, Torino, 1976, p. 644; E. BONVICINI, La responsabilità civile per fatto altrui, Milano, 1976, p. 282; C. SALVI, voce «Responsabilità extracontrattuale» (*dir.vig.*), in *Enc.dir.*, XXXIX, Milano, 1988, p. 1227.

⁵ Cfr. M. COZZI, La responsabilità civile per danno da cose (*diritto italiano e francese*), Padova, 1935, p. 333; P.G. MONATERI, La responsabilità civile, in R. SACCO (a cura di), *Tratt.dir.civ.*, Torino, 1998, p. 1041. A livello giurisprudenziale, si v. Cass.civ., sez. III, sent., 12 luglio 2006, n. 15779, in www.cortedicassazione.it; Cass.civ., sez. III, sent., 23 maggio 2019, n. 13966, che si conforma alle precedenti pronunce della Suprema Corte, specificamente alla Cass.civ., sez. III, ord., 1 febbraio, 2018, n. 2478 e alla Cass.civ., sez. III, sent., 29 luglio 2016, n. 15761 *ivi*. Più di recente, si v. Cass.civ., sez. VI, ord., 27 maggio 2022, n. 17252, in

fini della responsabilità, ciò che conta, in sostanza, è la disponibilità di fatto, non disgiunta dalla disponibilità giuridica della cosa, indipendentemente sia dall'utilità mediata o immediata e di qualsiasi natura che il custode tragga dalla propria attività, sia dal titolo della custodia della *res*⁶. Il custode non sarà, quindi, inquadrabile *tout court* nell'ambito delle categorie classiche del diritto di proprietà, del possesso o della detenzione, poiché si deve individuare chi abbia il potere di custodia che divenga fonte di responsabilità. Viene, così, in rilievo non solo la posizione del proprietario, del possessore, del detentore⁷, ma anche quella del conduttore, dell'usufruttuario e del titolare del diritto di godimento sul bene altrui in senso ampio. Tant'è che, quando il custode della cosa sia una persona diversa dal proprietario, a quest'ultimo non potrà applicarsi la normativa prevista per il custode⁸.

In secondo luogo, occorre la "cosa" oggetto di custodia, causa diretta dell'evento dannoso. Ai fini dell'applicazione della disciplina, a differenza di quanto previsto dall'art. 2050 c.c., non deve sussistere la pericolosità intrinseca della *res*, quanto invece l'idoneità, per sua natura, a cagionare un danno oppure è d'uopo che la cosa sia divenuta tale, a causa dell'insorgere, nella medesima, di agenti dannosi determinati da peculiari condizioni in cui sia venuta a trovarsi e che l'abbiano fatta divenire fonte di danno per i terzi⁹.

www.puntodiritto.it, che riconosce la responsabilità del proprietario di un appartamento per i danni da infiltrazioni d'acqua subiti nell'appartamento sottostante.

⁶ Tra le numerose pronunce dalla Corte di legittimità, si v. Cass.civ., sez. III, sent., 24 marzo 2016, n. 5877, in *Danno resp.*, 2016, p. 839, con nota di V. VOZZA, *Danno da pioggia intensa: responsabilità e caso fortuito*; Cass.civ., sez. III, ord., 24 settembre 2015, n. 18877, in *Mass. Foro it.*, 2015, n. 608; Cass.civ., sez. I, sent., 5 novembre 2013 - 28 febbraio 2014, n. 4804, Cass.civ., sez. III, sent., 7 luglio 2016 n. 13945, Cass.civ., sez. III, sent., 19 marzo 2009 n. 6665, Cass.civ., sez. III, sent., 11 maggio 1991, n. 5267, tutte in www.cortedicassazione.it. Si v. anche Corte d'Appello di Genova, Sez. I, 05 aprile 2019 (www.ufficijudiziarigenova.it). Più di recente, Cass.civ., sez. VI-2, ord., 15 marzo 2022, n. 8408, in CED Cassazione 2022, ha affermato che la disponibilità della cosa da parte dell'utilizzatore non comporta necessariamente il trasferimento in capo a costui della custodia. Si v. anche Cass.civ., sez. III, ord., 22 aprile 2022, n. 12909, ivi, secondo cui il committente è sempre gravato dalla responsabilità da cose in custodia nei confronti dei terzi danneggiati dall'esecuzione di opere effettuate, in forza di un contratto di appalto; tale responsabilità non può venir meno per la consegna dell'immobile all'appaltatore, ai fini dell'esecuzione delle opere stesse, ma trova, piuttosto, un limite esclusivamente nel ricorso del caso fortuito; tutto ciò non esclude, come ovvio, ulteriori responsabilità del committente e/o dell'appaltatore, ex art. 2043 c.c. Sul tema della responsabilità del committente detentore dell'immobile che continui ad esercitare, di fatto, il potere di custodia e l'insorgere della responsabilità di cui all'art. 2051 c.c. in capo a costui, si v. Cass.civ., sez. III, sent., 23 dicembre 2021, n. 41435, in CED Cassazione 2021.

⁷ La giurisprudenza non riconosce la qualifica di "custode" né al mero detentore per ragioni di cortesia o di servizio, dal momento che trattasi di un soggetto influenzato dai poteri organizzativi o direzionali altrui; né al mero utilizzatore della cosa, a meno che il concedente non si sia spogliato del governo della stessa, per ragioni specifiche. Si v. Cass.civ., sez. III, sent., 29 luglio 2017, n. 22839, www.cortedicassazione.it. Recenti decisioni giurisprudenziali assumono rilevanza, con riferimento alla qualifica di "custode". In particolare, la sentenza del Trib. Roma, 16 febbraio 2022, n. 2486 ravvisa la responsabilità ex art. 2051 c.c. di un condominio che, già da anni, si occupava della manutenzione di un albero esterno al perimetro condominiale che aveva finito per rovinare su un'auto in sosta, qualificandolo come custode "volontario".

⁸ In tal senso cfr. L. CORSARO, voce «Responsabilità da cose», in *Dig.disc.priv.*, sez.civ., XVII, Torino, 1998, pp. 103, 106. Cfr. anche A. DE CUPIS, *Il danno*, II, Milano, 1979, p. 196; E. BONVICINI, op.cit., p. 282. Per l'ipotesi che il dovere di custodia gravi su più persone, cfr. L. MEZZASOMA *La responsabilità per danno da cose*, in *Rass. dir. civ.*, 1996, p. 393.

⁹ Cfr. C. DAINI, *La responsabilità da cose in custodia*, in *Danno e resp.*, 2019, p. 193; amplius, M. FRANZONI, *La responsabilità oggettiva. Il danno da cose e da animali*, in *I grandi orientamenti della giurisprudenza civile e commerciale*, diretta da F. GALGANO, Padova, 1988, pp. 117, 169-170; P.G. MONATERI, op.cit., p. 1038. La letteratura ha esaminato i rapporti tra l'art. 2051 c.c. e gli artt. 2050, 2053, 2054 c.c. Si concorda con la dottrina (L. CORSARO, op.cit., p. 104) che ha tracciato un ambito di applicazione autonomo dell'art. 2051 c.c. rispetto a tali norme: in primis, in confronto all'art. 2050 c.c., «responsabilità per l'esercizio di attività pericolose», laddove le cose utilizzate costituiscono strumenti di attività pericolosa e non, differentemente,

Si puntualizzi che la disciplina vigente fissa un regime ben diverso da quello previsto dalla normativa della responsabilità civile da cose in custodia, dettata dal codice civile del 1865 all'art. 1153 che si incardinava sul danno provocato da taluni «colle cose» avute in custodia¹⁰. L'art. 2051 c.c., facendo riferimento al danno provocato «dalla cosa», non ha la funzione di disciplinare le ipotesi in cui il mezzo dell'agire dell'uomo sia una *res*, quanto diversamente quelle in cui la stessa produca un danno, in ragione del proprio modo di porsi nella realtà, per un proprio «agire»¹¹. La cosa deve avere, di fatto, un «ruolo attivo nella produzione dell'evento»¹². Conseguentemente, quando la stessa costituisca lo strumento dell'agire della persona e tale attività cagioni un danno nell'altrui sfera giuridica, non si applicherà l'art. 2051 c.c., ma diversamente l'art. 2043 c.c.¹³.

Infine, deve esistere il nesso di causalità tra la cosa e l'evento dannoso.

Avendo riguardo alla ripartizione dell'onere probatorio, l'art. 2051 c.c. impone al danneggiato di fornire la prova dell'esistenza del rapporto di custodia tra il danneggiante e la cosa e del nesso causale tra la cosa in custodia e l'evento lesivo; il custode dovrà, invece, costituire la prova, quale esimente da responsabilità, dell'esistenza del «caso fortuito», idoneo ad elidere tale rapporto causale¹⁴.

Tuttavia, sebbene il legislatore abbia fissato codeste coordinate applicative, molte sono le questioni interpretative che si sono poste in riferimento al caso concreto. Al riguardo, si rilevi che la casistica della responsabilità civile da cosa in custodia è sconfinata¹⁵. A titolo esplicativo, si pensi alle impalcature di palazzi che permettano intrusioni di ladri nelle abitazioni; agli infortuni conseguenti alla dannosa sicurezza delle piste da sci, degli impianti sportivi in generale oppure di parchi acquatici, dotati di scivoli o di piscine e di parchi giochi in generale; ai danni cagionati da cose comuni al condominio¹⁶.

entità autonome e distinte da colui che svolge l'attività di custodia; in secondo luogo, rispetto all'art. 2053 c.c. che, nel disciplinare la responsabilità da rovina dell'edificio, attiene alla sua manutenzione ovvero allo stesso, quale risultato di un'attività di costruzione; infine, rispetto all'art. 2054 c.c., concernente la responsabilità da circolazione di veicoli, che si riferisce al danno che derivi dalla circolazione del veicolo, quale «cosa».

¹⁰ Ex multis, cfr. L. CORSARO, op.cit., p. 103; U. RUFFOLO, Intelligenza artificiale, machine learning e responsabilità da algoritmo, in *Giur.it.*, 2019, p. 1699 s.; G. CHINÉ, A. ZOPPINI, Manuale di diritto civile, Nel diritto ed., 2019, p. 2148, i quali precisano come tale forma di responsabilità non rappresenti una novità, in quanto già prevista dall'articolo 1153 c.c. del 1865 e che l'art. 2051 c.c. finisca con l'ampliare l'ambito di applicazione della disciplina, prevedendo, oltre al danno cagionato «colle cose», quello provocato «dalle cose».

¹¹ Emblematica la sentenza della Cass.civ., sez.un., 28 luglio 1954, n. 2759, in *Resp.civ.prev.*, 1955, p. 321; tra i numerosi autori, cfr. G. GENTILE, La responsabilità per le cose in custodia nel nuovo codice civile, ivi, 1941, p. 171; A. DE CUPIS, Dei fatti illeciti, in *Comm. Scialoja e Branca*, Bologna-Roma, 1971, p. 83.

¹² Cfr. L. CORSARO, op.cit., p. 105.

¹³ Ex multis, cfr. V. GERI, Responsabilità civile da cose in custodia, animali e rovina di edificio, 2 ed., Milano, 1974, p. 98 ss.; F.D. BUSNELLI, voce «Illecito civile», in *Enc.giur.*, XV, Roma, 1989, p. 25; P. TRIMARCHI, La responsabilità civile: atti illeciti, rischio, danno, Milano, 2017, p. 399.

¹⁴ Cfr. Cass.civ., sez. III, ord., 1 febbraio 2018, n. 2477, in *Giust.civ.*, 2018.

¹⁵ Per una puntuale carrellata della casistica, cfr. F. AGNINO, Danno cagionato da cose in custodia. Principi generali e fattispecie particolari della responsabilità del custode, Torino, 2020, p. 189 ss.

¹⁶ Di peculiare interesse è la recente ordinanza Cass.civ., III sez., 4 aprile-19 maggio 2022, n. 16224 che conclude una vicenda processuale molto lunga, attinente alle lesioni subite dalla cliente di un supermercato che era stata colpita violentemente dalle porte a scorrimento automatico. La Cassazione esclude il riconoscimento della natura contrattuale della responsabilità del supermercato, derivante dalla violazione di obblighi scaturenti dal contratto di vendita stipulato tra la società gestrice dello stesso e la cliente, sostenendo che la possibile concretizzazione del rischio dell'evento dannoso verificatosi sia ascrivibile non alla mancata osservanza di obblighi di protezione o della dovuta diligenza adempitiva della prestazione

Ancora, assume un ruolo di rilievo la responsabilità civile della Pubblica Amministrazione per i danni arrecati a cose o persone dai beni di sua proprietà, in innumerevoli ipotesi quali, ad esempio, allagamenti causati da forti precipitazioni atmosferiche¹⁷, caduta di rami, dissesto di manto stradale, macchie d'olio¹⁸. Per ragioni di economia espositiva, non ci si soffermerà sulle variegate questioni sollevate da tale fattispecie, oggetto di attenta analisi dottrinale e di numerose pronunce giurisprudenziali, in continuo evolversi¹⁹.

Tratteggiati i capisaldi della disciplina oggetto di attenzione, il contributo intende sottolineare come la stessa offra tuttora stimolanti spunti di riflessione per due ordini di ragioni.

La fattispecie di cui all'art. 2051 c.c. ha costituito e costituisce, pur sempre, oggetto di interpretazioni innovative, in riferimento alla natura della responsabilità, tant'è vero che gli schemi adottati dalla giurisprudenza sono poliedrici²⁰.

Inoltre, lo sviluppo rapido ed esponenziale delle tecnologie digitali emergenti solleva nuove questioni di responsabilità civile, con riferimento alle decisioni ed ai comportamenti assunti dai sistemi di intelligenza artificiale che cagionino danni ai soggetti con i quali interagiscano. In proposito, ci si interroga sulla riconduzione delle nuove ipotesi di responsabilità civile per l'intelligenza artificiale nell'alveo di taluni modelli di responsabilità civile extracontrattuale, previsti dal nostro sistema ordinamentale e, nello specifico, se sia applicabile, in determinate ipotesi, l'articolo 2051 c.c., alla luce dei principi sviluppatisi in ambito giurisprudenziale. Vieppiù, in vista dell'approvazione di provvedimenti europei, finalizzati ad offrire soluzioni alle nuove sfide poste dall'innovazione tecnologica, sorge il quesito se non sia appropriato operare uno sforzo di coordinamento ed aggiornamento della normativa vigente.

2. La qualificazione giuridica della responsabilità da cose in custodia tra responsabilità "aggravata" e responsabilità "oggettiva".

contrattuale da parte del venditore nei confronti dell'acquirente, quanto diversamente dalla realizzazione della potenzialità dannosa delle cose che si trovino nel supermercato. L'interesse del cliente a conservare la propria integrità fisica riceve tutela nella vita di relazione, prescindendo dall'acquisto di merci e, pertanto, il danno cagionato dalle cose che si trovino all'interno del locale integra, nel concorso degli altri elementi costitutivi della fattispecie di cui all'art. 2051 c.c., l'imputazione della responsabilità extracontrattuale da cose in custodia in capo alla società gestrice del supermercato, in qualità di custode delle cose medesime. La sentenza è pubblicata in www.cortedicassazione.it

¹⁷ Particolarmente interessante è l'ordinanza della Cass.civ., sez.VI, 28 luglio 2017, n. 18856, in Danno resp., 2018, pp. 41 ss., con nota di M. NATALE, Bombe d'acqua, allagamenti e responsabilità da cose in custodia della P.A.

¹⁸ Cfr. Cass.civ., sez. VI, ord., 3-20 febbraio 2019, n. 4963, cit.

¹⁹ Per una sintetica, ma efficace disamina dell'evoluzione giurisprudenziale in tale ambito, si v. B. DE SANTIS, op.cit., passim. In tema di responsabilità della P.A. per i danni arrecati dalla fauna selvatica, si v. Cass.civ., sez. III, sent., 20 aprile 2020, n. 7969 con commento di R. MARINO, Danno da fauna selvatica e regime di responsabilità oggettiva in capo alla Regione, in Dir. Agricoltura, 2020, p. 230 ss.

²⁰ In tale senso cfr. G. ALPA, La responsabilità civile. Parte generale, in ID. (a cura di), Diritto della responsabilità civile, Torino 2010, p. 739. Attenta dottrina sottolinea la persistente attualità della tematica, denotando le criticità della fattispecie dell'art. 2051 c.c., per, poi, interrogarsi sul futuro della responsabilità delle cose in custodia. Cfr. F.P. PATTI, Il declino della responsabilità oggettiva (a margine dell'art. 2051 c.c.), in Riv.dir.civ., 2019, p. 977.

Sin dall'entrata in vigore del codice civile vigente, sussiste un acceso dibattito sulla natura della responsabilità civile da cose in custodia. La letteratura ha elaborato due principali ricostruzioni, accolte dalla Corte di legittimità con orientamenti oscillanti.

La dottrina prevalente ha ricondotto la responsabilità da cose in custodia nell'ambito della responsabilità oggettiva²¹ che si basa sull'accertamento della sussistenza del solo nesso di causalità tra la "cosa" causativa del pregiudizio e l'evento dannoso, senza che assuma rilevanza la violazione colpevole dell'obbligo di custodire la cosa da parte del custode. Secondo tale prospettazione, ai fini della configurabilità della responsabilità, risulta sì essenziale la relazione intercorrente tra costui e la cosa custodita, ma sarà sufficiente il mero rapporto eziologico tra la cosa e l'evento lesivo²².

Alla base di tale ragionamento, vi è l'individuazione della *ratio* dell'art. 2051 c.c. nell'obiettivo di responsabilizzare colui che si trovi nella condizione di gestire i rischi tipicamente intrinseci all'esistenza della *res*²³.

La giurisprudenza maggioritaria ha, già da tempo, riconosciuto la natura oggettiva della fattispecie di cui all'art. 2051 c.c. La pronuncia che ha dato avvio alla moderna concezione dell'art. 2051 c.c. è la sentenza Cass.civ., sez.un., 11 novembre 1991, n. 12019²⁴. Successivamente l'indirizzo giurisprudenziale si è andato definitivamente affermando, a partire dalla sentenza della Cass.civ., sez. III, 20 maggio 1998, n. 5031²⁵.

²¹ Sul tema cfr. M. FRANZONI, *La responsabilità oggettiva*, Padova, 1995, passim.

²² Cfr. P. TRIMARCHI, Il "caso fortuito" quale limite della responsabilità per il danno da cose (Contributo ad una teoria del rischio d'impresa), in *Riv.trim.dir.proc.civ.*, 1959, p. 808 ss; M. COMPORTI, *Esposizione al pericolo e responsabilità oggettiva*, Milano, 1965, p. 91; P.G. MONATERI, *op.cit.*, p. 1039; C. CASTRONOVO, *La nuova responsabilità civile*, 3 ed., Milano, 2006, pp. 3029 ss.; A. JANNARELLI, «sub art. 2051 c.c.», in *Comm.Gabrielli*, Torino, 2011, pp. 234 ss.; V. GERI, *Responsabilità civile per danni da cose ed animali*, Milano, 1967, p. 298.

²³ Influyente dottrina ha sviluppato questa tesi, alla luce di un'interpretazione sistematica delle fattispecie di responsabilità speciali di cui agli artt. 2050-2054 c.c., strettamente correlata al rischio di impresa ed alle ripercussioni sul mercato assicurativo, fattori significativi che incidono sulla ripartizione dei danni e dei relativi costi dei consociati. L'Autore ha puntualizzato che la funzione della responsabilità oggettiva non è di punire, bensì di imputare a chiunque il «rischio oggettivamente creato» dalla propria attività, nella misura in cui esso sia esprimibile in costo ed amministrabile dal punto di vista economico, con le conoscenze e con i mezzi di previdenza che un buon amministratore abbia a propria disposizione. Cfr. P. TRIMARCHI, *Rischio e responsabilità oggettiva*, Milano, 1961, pp. 193 ss. La teoria del rischio è stata criticata da C. SALVI, *La responsabilità civile*, Milano, 1998, p. 149 e da C. CASTRONOVO, *La nuova responsabilità civile*, Milano, 1997, pp. 57 ss., il quale ha sostenuto la scarsa credibilità del rischio per talune delle fattispecie civilistiche di responsabilità speciali, in particolare con riguardo alla responsabilità civile da cose in custodia, richiamando le magistrali argomentazioni di G. CALABRESI, *The Costs of Accidents. A Legal and Economic Analysis*, Yale, 1970, trad. it. *Costo degli incidenti e responsabilità civile. Analisi economico-giuridica*, Milano, 1975, p. 183. Costui ha affermato che deve rispondere del danno colui che si trovi nella posizione più idonea a condurre un'analisi costi-benefici, ad accertare, cioè, la convenienza di evitare il danno rispetto al costo necessario per evitarlo.

²⁴ Pubblicata in *Nuova giur.civ.comm.*, 1992, p. 81, con nota di G. ALPA, *Responsabilità per rischio da cose in custodia*.

²⁵ In *Danno e resp.* 1999, p. 209, con nota di S. VOGLI, L'art. 2051 c.c. tra declamazioni e regole operazionali. Sulla stessa linea, ex multis, si v. le due sentenze gemelle Cass.civ., sez. III, 9 agosto 2004, nn. 15383 e 15384, in *www.cortedicassazione.it*; Cass.civ., sez. III, sent., 10 agosto 2004, n. 15429, in *Danno e resp.*, 2005, p. 725, con nota di P. LAGHEZZA, *Uso improprio del bene e responsabilità del custode*; Cass.civ., sez. III, sent., 9 novembre 2005, n. 21684, in *Foro it.*, 2006, I, c. 1807; Cass.civ., sez. III, sent., 6 luglio 2006, n. 15383, in *Corr. giur.*, 2006, 1358, con nota di V. CARBONE, *Responsabilità oggettiva del custode del bene demaniale*; Cass.civ., sez. III, sent., 14 luglio 2015, n. 14635, in *Foro it.*, 2015, I, c. 3153; Cass.civ., sez. III, sent., 29 luglio 2016, n. 15761, in *Arch.giur.circ.*, 2016, p. 958; Cass.civ., sez. III, ord., 1° febbraio 2018, n. 2481, in *Giust.civ.*, 2018; Cass.civ., sez. III, ord., 1° febbraio 2018, n. 2477, cit.; Cass.civ., sez. III, sent.,

La Suprema Corte ha individuato la *ratio* della norma nell'esigenza di apprestare uno strumento di allocazione del danno, improntato ad una "finalità di giustizia distributiva" che sia idonea a traslarlo dal soggetto leso, che incolpevolmente lo subisce, al custode che è tenuto a risponderne, in ragione del potere di fatto che esercita sulla cosa²⁶. Al riguardo, assume preminente interesse l'affermazione, contenuta nella sentenza della Cass.civ., Sez. III, 26 luglio 2019, n. 20312²⁷, che «il riconoscimento della natura oggettiva del criterio di imputazione della responsabilità custodiale si fonda sul dovere di precauzione imposto al titolare della signoria sulla cosa custodita, in funzione di prevenzione dei danni che da essa possono derivare».

In punto di distribuzione dell'onere probatorio, il danneggiato dovrà costituire la prova del nesso di causalità tra la cosa in custodia e l'evento dannoso, più propriamente che l'evento dannoso si è prodotto come conseguenza normale della condizione specifica, potenzialmente lesiva della cosa²⁸. Si rilevi che l'ordinanza Cass.civ., sez. III, ord., 1 febbraio 2018, n. 2482 ha precisato che, ai fini di addivenire ad una causalità giuridicamente rilevante, non basta una relazione causale avvalorata sul modello della c.d. teoria della "*conditio sine qua non*", ma deve darsi rilievo a quelle condizioni rilevanti –*ex ante*– che siano idonee a cagionare l'evento dannoso, secondo il modello della c.d. regolarità causale, ossia dell'*id quod plerumque accidit*²⁹.

In forza di tali principi, per "caso fortuito" deve intendersi tutto ciò che costituisca un'eccezione alla normale sequenza causale e che, ricondotto ad una valutazione *ex ante* ovvero in astratto, non sia oggettivamente prevedibile, con il risultato che all'imprevedibilità consegua l'inevitabilità dell'evento³⁰. Il custode, ai fini dell'esenzione dalla responsabilità, dovrà, dunque, dimostrare l'esistenza di un fattore esterno, "estraneo alla sfera soggettiva" (sussistente nel fenomeno

16 febbraio 2021, n. 4035, CED Cassazione 2021, sulla quale cfr. il commento di B. DE SANTIS, Cassazione n. 4035/2021: non basta la condotta colposa del danneggiato ex art. 1227, in www.judicium.it. Più di recente, si v. Cass.civ., sez. VI-2, ord., 15 marzo 2022, n. 8408, cit.; Cass.civ., sez. III, ord., 22 aprile 2022, n. 12909, cit.

²⁶ Cfr. B. DE SANTIS, Brevi note su recenti riletture giurisprudenziali dell'art. 2051 c.c., op.cit., p. 2 s. Tre le molteplici decisioni giurisprudenziali, si v., ex multis, Cass.civ., sez. III, sent., 13 gennaio 2015, n. 295, in Foro it., 2015, I, c. 460, con nota di P. LAGHEZZA; Cass.civ., sez. III, sent., 18 settembre 2014, n. 19657, ivi, c. 555. Per un'indagine della fattispecie nella prospettiva di analisi economica del diritto, cfr. E. BAFFI, D. NARDI, La responsabilità da custodia della P.A.: prospettive di analisi economica del diritto, in *Danno e resp.*, 2016, pp. 337 ss.

²⁷ In www.cortedicassazione.it

²⁸ Cfr. C. DAINI, op.cit., p. 194.

²⁹ Pubblicata in *Corr.giur.* 2019, p. 184, con nota di A. SCALERA, Caso fortuito: la Cassazione rimette le cose a posto. La pronuncia, nel tracciare un quadro completo della responsabilità per danni da cose in custodia, si pone nel solco dell'importantissima sentenza della Cass.civ., sez.un., 11 gennaio 2008, n. 576 (in *Corr.mer.*, 2008, p. 694, con nota di G. TRAVAGLINO, Causalità civile e penale: modelli a confronto) che ha sostenuto che, affinché si realizzi la causalità materiale nell'ambito della responsabilità extracontrattuale, deve farsi applicazione dei principi elaborati nel diritto penale dagli artt. 40 e 41 c.p., in forza dei quali un evento deve reputarsi provocato da un altro se, ferme restando le altre condizioni, il primo non si sarebbe realizzato in assenza del secondo (c.d. teoria della *conditio sine qua non*) e potrà esser ascritto, in maniera esclusiva, all'autore della condotta sopravvenuta, unicamente quando la stessa appaia tale da rendere ininfluenti le altre cause preesistenti. Ancora, all'interno di tali serie causali, occorre conferire rilevanza esclusivamente a quelle che risultino idonee a cagionare quell'evento, in relazione ad un dato probabilistico o statistico che sia anticipatamente valutabile, in forza del c.d. principio della regolarità causale. Sul punto cfr. C. DAINI, op.cit., p. 194.

³⁰ Cfr. C. DAINI, loc.op.ult.cit.

naturalistico, nella condotta del danneggiato o di un terzo³¹) che abbia i requisiti dell'imprevedibilità ed eccezionalità, tali da "interrompere" il nesso di causalità tra la cosa in custodia e l'evento lesivo³².

In via conclusiva, tale insegnamento giurisprudenziale ricostruisce il caso fortuito in chiave oggettiva, in quanto legato al nesso di causalità³³.

Come ovvio, in caso di mancata prova del caso fortuito, il custode sarà responsabile³⁴.

È quindi d'uopo rilevare che, se, ad oggi, l'orientamento esposto è avvalorato dalla letteratura e dalla giurisprudenza maggioritaria; per altro verso, l'insegnamento giurisprudenziale più risalente³⁵ ha ricostruito la fattispecie di cui all'art. 2051 c.c. in termini di responsabilità "aggravata" che, facendo eccezione agli artt. 2043 e 2697 c.c., si contraddistingue per l'inversione dell'onere della prova liberatoria, posto a carico del custode, presunto responsabile.

Questa impostazione ha rapportato la responsabilità da cose in custodia ad una presunzione legale di colpa, individuandone il fondamento nel fatto dell'uomo: specificamente nel comportamento del custode venuto meno al suo dovere di controllo e di vigilanza, da osservare al fine di evitare che la cosa produca danni. In tale ottica, la *presunzione iuris tantum* è superabile dal custode, sul quale incombe l'onere di provare di non essere "in colpa".

La dottrina tradizionale (seppure minoritaria)³⁶, nel solco di tale indirizzo giurisprudenziale, ha asserito che la presunzione legale di colpa del custode sia

³¹ Si v., ex multis, Cass.civ., sez. VI, ord., 27 maggio 2022, n. 17252, cit.; Cass.civ., sez. VI, ord., 3-20 febbraio 2019, n. 4963, cit.; Cass.civ., sez. VI, ord. 9 novembre 2017, n. 26533, in www.cortedicassazione.it; Cass.civ., sez. III, sent., 23 ottobre 1998, n. 10556, in Giust.Civ.Mass. 1998, p. 2166.

³² Si v., tra le più rilevanti pronunce, Cass.civ., sez. III, ord., 1° febbraio 2018, n. 2480, in Foro it., 2018, I, c. 1254, con nota di P. LAGHEZZA, Un manuale giudiziale sulla responsabilità da cose in custodia. Si v. anche Cass.civ., sez. III, sent., 19 febbraio 2008, n. 4279, in Mass.Giur.it., 2008; Cass.civ., sez. III, sent., 13 luglio 2011, n. 15389, in Mass.Foro it., 2011, n. 592; Cass.civ., sez. III, sent., 18 febbraio 2014, n. 3793, in Giur. it., 2014, p. 2135, con nota di P. VALORE, La r.c. da cose in custodia: natura e limiti. La dottrina (V. GERI, op.ult.cit., p. 184) distingue tra "fortuito autonomo", "fortuito eccezionale" e "fortuito concorrente", descrivendo il primo come un fattore esterno che abbia, di per sé, determinato l'eventus damni autonomamente, prescindendo dalla cosa e dal comportamento del custode, di modo tale che il danno appare solamente provocato dal caso fortuito; nel secondo caso, distintamente, la cosa sarebbe stata resa fattore eziologico dell'evento dannoso da un elemento o un fatto estraneo del tutto eccezionale ed imprevedibile, rispetto al quale, la res sarebbe, in ogni caso, la mera occasione del danno. Il "fortuito concorrente", di contro, non sarebbe idoneo ad assorbire l'intera causalità del danno, ma sarebbe un mero antecedente eziologico, il quale, però, non potrà essere invocato dal custode, ai fini dell'esclusione dalla responsabilità.

³³ Si v. Cass.civ., sez. III, ord., 1 febbraio 2018, n. 2482, in www.cortedicassazione.it, che, all'indomani di una decisione importante della stessa sezione della Suprema Corte, in tema di responsabilità civile da cose in custodia (Cass.civ., sez. III, ord., 31 ottobre 2017, n. 25837, in Corr. giur., 2018, p. 765 con nota di A. SCALERA, Caso fortuito: da Giustiniano a Napoleone si è persa l'imprevedibilità?), ha operato "alcune puntualizzazioni".

³⁴ Con la conseguenza che rimarrebbe a suo carico la "causa ignota". Così, M. FRANZONI, Dei fatti illeciti, in Comm. Scialoja e Branca, Bologna-Roma 1993, p. 587.

³⁵ Tra le prime decisioni in tal senso, Cass.civ., sez. III, sent., 1° aprile 1987, n. 3129, in Mass.Giur.it., 1987; Cass.civ., sez. III, sent., 11 maggio 1991, n. 5267, in Foro it., Rep. 1991, voce «Magazzini generali», n. 2; Cass.civ., sez. III, sent., 9 febbraio 1994, n. 1332, Mass.Giur.it., 1994. Successivamente, tra le numerose pronunce, Cass.civ., sez. III, sent., 27 dicembre 1995, n. 13114, Foro it., Rep. 1996, voce «Responsabilità civile», n. 185; Cass.civ., sez. III, sent., 22 maggio 1998, n. 5133, ivi, 1998, voce ult.cit., n. 118; Cass.civ., sez. III, ord., 17 maggio 2001, n. 6767, ivi, 2001, voce ult.cit., n. 355; Cass.civ., sez. III, sent., 27 agosto 1999, n. 8997, in Nuova giur.civ.comm., 2000, I, p. 352, con nota di F. GRITTI; Cass.civ., sez. III, sent., 9 marzo 2010, n. 5658, in Resp.civ.prev., 2010, p. 468, con nota di G. FACCI.

³⁶ Cfr. C.M. BIANCA, Diritto civile, 5, La responsabilità, 2 ed., Milano, 2012, p. 722; sulla stessa linea L. CORSARO, op.cit., p. 105 ss.; A. DE CUPIS, op.cit., pp. 187 ss.; P. FORCHIELLI, Intorno alla responsabilità senza colpa, in Riv.trim.dir.proc.civ., 1967, p. 1393.

motivata dalla circostanza che la peculiare relazione non occasionale con la cosa gli imponga obblighi di vigilanza, controllo e diligenza. Di conseguenza, l'attitudine della cosa a cagionare danni lo obbligherebbe ad adottare tutte le misure idonee a prevenire ed impedire la produzione di danni a terzi.

In quest'ottica, tale obbligo si riflette inevitabilmente sull'onere probatorio incombente sul danneggiante. Il custode, in conformità al principio di c.d. vicinanza alla prova³⁷, sarà gravato dall'onere di fornire la prova che il danno si sia realizzato in modo non prevedibile, né superabile con l'adozione di tutte le precauzioni rapportabili alla diligenza richiesta dalla natura, dalla funzione della cosa e dalle circostanze del caso concreto³⁸.

La tesi della "responsabilità aggravata" accoglie, in tal guisa, una nozione soggettiva del caso fortuito, in quanto connesso alla colpa³⁹.

Non deve tuttavia ritenersi⁴⁰ che, in tale prospettiva, la prova del caso fortuito si esaurisca nella dimostrazione, da parte del custode, dell'assenza di colpa. Ai fini dell'esclusione dell'imputazione della responsabilità, costui dovrà provare due elementi: sia il proprio comportamento diligente; sia il caso fortuito che sia idoneo a cagionare o a concorrere a causare il danno⁴¹.

³⁷ Secondo il quale l'onere della prova deve ragionevolmente gravare sulla parte processuale che sia più prossima, vicina alla fonte della prova, considerando, in concreto, la possibilità dei singoli soggetti in giudizio di provare le circostanze che ricadano nelle rispettive sfere d'azione. Amplius, cfr. S. PATTI, Prove, in Comm. Scialoja-Branca-Galgano-De Nova, sub art. 2697 c.c., Bologna, 2015, pp. 163 ss.

³⁸ Cfr. F.P. PATTI, op.cit., p. 985 che richiama i passaggi dell'ordinanza Cass.civ., sez. III, 31 ottobre 2017, n. 25837, cit.; si v. già Cass.civ., sez. III, sent., 20 febbraio 2006, n. 3651, in www.cortedicassazione.it; rieditata da Cass.civ., sez. III, sent., 9 giugno 2016, n. 11802, in Foro it., 2017, I, c. 1418, con nota adesiva di M.C. BIANCA; Cass.civ., sez. VI, ord., 28 luglio 2017 n. 18856, cit.

³⁹ Cfr. C.M. BIANCA, op.cit., pp. 726 ss.; A.L. CORSARO, op.cit., pp. 107 s.; tra autorevoli autori, ex multis, A. CANDIAN, voce «Caso fortuito e forza maggiore (Diritto civile)», in Nov.Dig., II, Torino, 1957, p. 991; G. COTTINO, voce «Caso fortuito e forza maggiore (dir.civ.)», in Enc.dir., VI, Milano, 1960, pp. 378 ss.

⁴⁰ Per le considerazioni che seguono, cfr. L. CORSARO, op.cit., p. 107; F.P. PATTI, op.cit., pp. 985 ss.

⁴¹ Negli ultimi anni, in ambito giurisprudenziale, indipendentemente dalla configurazione del caso fortuito in chiave oggettiva o soggettiva, la condotta colposa del danneggiato ha assunto sempre maggiore rilievo, ai fini dell'esenzione dalla responsabilità del custode. La giurisprudenza di legittimità, operando una revisione dei principi sull'obbligo di custodia, ha individuato in capo ai soggetti che entrino in interazione con la cosa un dovere di ragionevole cautela, come espressione massima del principio di solidarietà, stabilito dall'art. 2 Cost. che permea il nostro ordinamento. In forza di una lettura costituzionalmente orientata dell'art. 2051 c.c., i giudici sono pervenuti alla conclusione che debba tenersi doverosamente conto della condotta del danneggiato, alla luce del principio di autoreponsabilità, operando una valutazione del suo comportamento e del grado di incidenza causale che esso assuma sull'evento lesivo, ai sensi dell'art. 1227 c.c., per poi pervenire, anche d'ufficio, all'applicazione del primo comma. Secondo tale indirizzo ermeneutico, è compito del giudice valutare la condotta del danneggiato, tenendo conto del fatto che, quanto più la situazione di potenziale danno possa essere prevista e superata, attraverso l'adozione delle ragionevoli cautele normalmente attese e prevedibili in correlazione alle circostanze, tanto più incidente deve valutarsi l'efficienza causale del suo comportamento imprudente, nel dinamismo causale del danno. In definitiva, la condotta del danneggiante sarà qualificabile come caso fortuito, quando sia colposa e presenti caratteri di imprevedibilità da parte del custode ed eccezionalità, tali da interrompere il nesso causale tra la cosa in custodia ed il danno. Cfr. C. DAINI, op.cit., p. 195; B. DE SANTIS, op.ult.cit. p. 6. La giurisprudenza che si esprime in tali termini è copiosa. Tra le più recenti pronunce, Cass.civ., sez. VI-3, ord., 4 marzo 2022, n. 7173, in CED Cassazione 2022, che nega il risarcimento del danno a chi inciampi su uno scalino visibilmente dissestato, individuando una condotta imprudente dell'infortunato; Cass.civ., sez. III, ord., 12 aprile 2022, n. 11794, ivi, secondo cui, se il pedone inciampa sul tombino sporgente e pienamente visibile, la responsabilità non è del Comune, in quanto sussiste un concorso di colpa del danneggiato. Ex multis, Cass.civ., sez. VI, ord., 17 novembre 2021, n. 34886, in CED Cassazione 2021; Cass.civ., sez. III, ord., 14 dicembre 2021, n. 39965, ivi; Cass.civ., sez. VI, ord., 10 marzo 2021, n. 6554, ivi; Cass.civ., sez. III, sent., 16 febbraio 2021, n. 4035, cit.; Cass.civ., sez. III, ord. 2 ottobre – 20 novembre 2020, n. 26527, in CED Cassazione 2020; Cass.civ., sez. VI-3, ord., 13 gennaio 2020, n. 347, ivi; Cass.civ., sez. III, sent., 19 febbraio 2020, n. 4178, ivi; Cass.civ., sez. III, ord., 5 maggio 2020, n. 8478, in www.deiustitia.it; Cass. civ., sez. VI, sent., 3 aprile

Per di più, si osservi che la circostanza che la lettera dell'art 2051 c.c. richieda la prova del caso fortuito ha indotto parte della dottrina⁴² ad asserire la necessità della prova dell'esistenza di un caso fortuito positivo. Diversamente altri autori⁴³ sostengono che il fortuito possa essere dimostrato in via negativa, senza che tale prova collimi, per tale ragione, con la dimostrazione della custodia diligente. In realtà, il custode, dopo aver fornito la prova della propria diligenza nella custodia, dovrebbe esibire elementi di prova tali da "identificare" uno o più fatti estranei allo stesso che abbiano provocato il danno, anche se non riesca ad "individuare" il fatto precipuo, causa dell'evento dannoso. In tale modo, il custode darebbe prova che il danno sia dovuto ad una causa estranea alla propria sfera giuridica, seppure in via indiretta e per mezzo di presunzioni, possibili in tale ambito.

3. Modelli giurisprudenziali innovativi. Rilievi critici.

Una volta illustrate le linee direttrici dei due orientamenti, preme rimarcare che la ricostruzione della responsabilità "aggravata" è stata gradualmente superata da quella della responsabilità "oggettiva", inizialmente minoritaria e divenuta, nel corso del tempo, dominante.

Eppure la giurisprudenza è tuttora altalenante. Si è, difatti, assistito, negli ultimi anni⁴⁴, ad una crescente configurazione della responsabilità da cose in custodia quale ipotesi di responsabilità aggravata.

Tale rinnovato orientamento giurisprudenziale è stato ricusato con risolutezza dalla Corte di legittimità in dieci pronunce⁴⁵, tra le quali Cass.civ., sez. III, ord., 1 febbraio 2018, n. 2480, cit. che richiama le note sentenze Cass.civ., sez. un., 11 gennaio 2008, nn. 576, 577, 578, 581, 582 e 584⁴⁶. Il provvedimento rappresenta

2019, n. 9315 richiama le ordinanze Cass.civ., sez. III, 1 febbraio 2018, nn. 2480, 2481, 2482, cit. e la n. 2483, in CED Cassazione 2019; Cass.civ., sez. III, sent., 29 gennaio 2019, n. 2345, ivi; Cass.civ., sez. III, ord., 31 ottobre 2017, n. 25837, cit.; Cass.civ., sez. III, sent., 22 giugno 2016, n. 12895, in Mass.Foro it., 2016, n. 433; Cass.civ., sez. III, ord., 12 maggio 2015, n. 9547, ivi, 2015, n. 302; Cass.civ., sez. III, ord., 5 febbraio 2013, n. 2660, in www.cortedicassazione.it; Cass. civ., sez. III, sent., 22 marzo 2011, n. 6529, ivi.

⁴² Cfr. A. CANDIAN, op.cit., p. 990; G.COTTINO, op.cit., p. 381; P. FORCHIELLI, voce «Caso fortuito e forza maggiore I) Diritto civile», in Enc.giur.Treccani, Roma, 1991, p. 2.

⁴³ Per le osservazioni che seguono si fa riferimento a L. CORSARO, op.cit., p. 108.

⁴⁴ Cfr. Cass.civ., sez. III, ord. 31 ottobre 2017, n. 25838, in www.cortedicassazione.it; in senso conforme si v., ex multis, Cass.civ., sez. III, sent., 27 giugno 2016, n. 13222, in Rep.Foro it., voce «Responsabilità civile», n. 229; Cass.civ., sez. III, sent., 9 giugno 2016, n. 11802, in Foro. it., 2016, I, c. 3159. Tra le più recenti pronunce, cfr. Cass.civ., sez. III, ord., 10 giugno 2020, n. 11096, in CED Cassazione 2020. Si vedano, in particolare, le pronunce della Corte di legittimità, relative ai danni da allagamento provocati da eventi atmosferici eccezionali (Cass.civ., sez. III, ord., 11 febbraio 2022, n. 4588 in CED Cassazione 2022; Cass.civ., sez.VI, ord., 28 luglio 2017, n. 18856, in www.cortedicassazione.it, Cass.civ., sez. III, sent., 24 marzo 2016, n. 5877, cit.; Cass.civ. sez. III, ord., 24 settembre 2015, n. 18877, cit.; Cass. civ., sez. III, sent., 17 dicembre 2014, n. 26545, in Mass. Foro it., 2014, n. 943), che applicano prevalentemente il criterio della diligenza nella custodia, finendo col dare origine ad una specie di settore interno alla responsabilità civile da cose in custodia. Cfr. M. NATALE, op.cit., p. 47.

⁴⁵ Alle quali hanno fatto seguito molteplici decisioni, relative alla configurabilità della condotta del danneggiato quale caso fortuito, che partono dall'assunto della natura oggettiva della responsabilità da cose in custodia. Ex multis si v. Cass.civ., sez. III, sent., 16 febbraio 2021, n. 4035, cit.; Cass.civ., sez. III, ord., 14 dicembre 2021, n. 39965, in www.dirittodelrisparmio.it; Cass.civ., sez. III, ord., 5 maggio 2020, n. 8478, in www.deiustitia.it. Tra le più recenti pronunce che configurano la responsabilità da cosa in custodia quale "responsabilità oggettiva", si v. Cass.civ., sez. VI, ord., 27 maggio 2022, n. 17252, cit.; Cass.civ., III sez., 4 aprile - 19 maggio 2022, n. 16224, cit.; Cass.civ., sez. III, ord., 22 aprile 2022, n. 12909 cit.; Cass.civ., sez. VI-2, ord., 15 marzo 2022, n. 8408, cit.

⁴⁶ Pubblicate in Foro. it., 2008, I, c. 451 ss.

un tentativo di risoluzione del contrasto interpretativo, realizzatosi nell'ambito della terza sessione della Cassazione, con il quale si è deciso di non rinviare la questione di difformità di giudicati alle Sezioni Unite⁴⁷.

Per contro, si ritiene che, a fronte dei ripetuti *revirements* della Suprema Corte, sarebbe appropriato che, a distanza di più di venti anni dall'ultima presa di posizione sul tema con la sentenza della Cass. civ., sez.un., 11 novembre 1991, n. 12019, cit., le Sezioni Unite intervengano, nell'esercizio della propria funzione nomofilattica, per porre fine a tale conflitto, riconducendo ad uniformità l'interpretazione dell'art. 2051 c.c.⁴⁸.

Come già sottolineato la questione è dirimente. L'accoglimento dell'una o dell'altra ricostruzione incide significativamente sui profili applicativi della disciplina. Si pensi alla differenza principale, concernente la qualificazione del caso fortuito come elemento oggettivo, legato al nesso di causalità (tesi della responsabilità oggettiva) ovvero come elemento soggettivo, connesso alla colpa (tesi della responsabilità aggravata)⁴⁹.

Invero, si ritiene che quest'ultima interpretazione del contenuto della prova liberatoria non sia adattabile né alla struttura, né alla *ratio* della fattispecie di cui all'art. 2051 c.c. Le riflessioni critiche che si esporranno qui di seguito⁵⁰ costituiscono, ad avviso di chi scrive, valide argomentazioni per respingere la tesi della responsabilità "aggravata". Si osservi, innanzitutto, che la struttura normativa dell'art. 2051 c.c. definisce la responsabilità del custode fino al limite del caso fortuito, senza menzionare il criterio della diligenza. Per tale ragione, non è condivisibile l'asserzione che il custode sia esonerato dalla responsabilità, quando dimostri l'assenza di colpa: *in primis*, giacché la stessa contraddice la struttura della norma; inoltre, perché ne svuota il significato, interpretando la fattispecie alla stessa stregua di una figura di responsabilità per colpa, con l'unica singolarità del maggiore rigore, dovuto all'aggravamento dell'onere probatorio posto in capo al custode, il quale, di fatto, si libererebbe, fornendo la prova di aver fatto tutto il possibile, per impedire l'evento lesivo.

Secondo tale impostazione, la nozione di caso fortuito si estenderebbe eccessivamente, fino a coincidere con la prova liberatoria di cui all'art. 2050 c.c.⁵¹ e degli artt. 2047, 2048, 2054 c.c. Come sottolineato dalla dottrina⁵², l'art. 2051 c.c., nel prevedere, a carico del custode, l'onere di fornire la prova del caso fortuito, si differenzia dalle altre norme che usano formule quali «avere adottato tutte le misure idonee a evitare il danno» o «non aver potuto impedire il fatto» oppure «aver fatto tutto il possibile per evitare il danno», invertendo, così, l'onere

⁴⁷ Cfr. F.P. PATTI, op.cit., p. 982, nota 21.

⁴⁸ Cfr. M. NATALE, op.cit., p. 48.

⁴⁹ Diversamente F.P. PATTI, op.cit., pp. 983, 993, nell'enucleare taluni punti di contatto delle due ricostruzioni, precisa, in riferimento all'istituto del caso fortuito, che le differenze, discendenti dalla sua diversa qualificazione, rilevano prevalentemente dal punto di vista concettuale e si riducono, in modo ragguardevole, in fase applicativa. L'Autore sostiene che i giudici, nel valutare con fermezza la sussistenza del caso fortuito, pur partendo da presupposti distinti, a seconda della tesi avvalorata, pervengono a risultati simili, poiché finiscono, nell'esplicazione delle modalità di applicazione dei principi di diritto asseriti in materia di prova liberatoria, col fare riferimento ai medesimi parametri di "imprevedibilità" ed "inevitabilità".

⁵⁰ Per le quali cfr. M. NATALE, op.cit., p. 47.

⁵¹ Cfr. F. GALGANO, in I fatti illeciti, in Corso di diritto civile, Bologna, 2008, p. 127.

⁵² Cfr. E. VALSECCHI, Responsabilità aquiliana oggettiva e caso fortuito, in Riv.dir.comm., 1947, I, 167; P. TRIMARCHI, Rischio e responsabilità oggettiva, op.cit., p. 183; M. COMPORI, op.cit., p. 91; D. DE MARTINI, I fatti produttivi di danno risarcibile, Padova, 1983, p. 224; M. BESSONE, Cose in «custodia» e responsabilità civile per il danno a terzi, in Giur.mer., 1983, p. 665; M. FRANZONI, Dei fatti illeciti, op.cit., p. 589.

della prova della colpa in materia di fatti illeciti. L'interpretazione letterale e logico-sistematica dell'art. 2051 c.c. conduce, viceversa, alla constatazione che il legislatore abbia previsto, in quest'ipotesi, una prova liberatoria più severa delle altre indicate, abbandonando il principio della responsabilità per colpa.

Se si considera, in secondo luogo, la funzione della fattispecie di cui all'art. 2051 c.c., il legislatore ha stabilito un criterio di imputazione che tenga conto della *ratio* della norma, identificabile indubitabilmente nella responsabilizzazione di coloro che si trovino nelle condizioni di gestire i rischi tipicamente connessi all'esistenza della cosa⁵³. Di conseguenza, il principio della responsabilità per colpa non appare essere un criterio efficiente, giacché l'idea del rischio del custode rinvia logicamente al modello di responsabilità oggettiva che trasferisca il peso economico dell'evento pregiudizievole dal danneggiato che lo subisca incolpevolmente al danneggiante che abbia la disponibilità giuridica e materiale del bene. In tale prospettiva, come visto, il limite della responsabilità del custode si trova, in maniera esclusiva, nel caso fortuito, non coincidente con l'assenza di colpa ed interpretabile come elemento oggettivo, legato al nesso di causalità.

Or dunque, sebbene le ricadute applicative sul versante processuale, che sin qui si è provato ad mostrare, siano rilevanti, non può sottacersi che il dibattito si è arenato oramai sui due opposti modelli di responsabilità da cose in custodia. Nonostante gli arresti significativi della Corte di Cassazione, esso non è, ad oggi, sopito. Il che ha generato inevitabilmente l'esigenza, per le Corti, di adottare soluzioni interpretative del tutto innovative.

Di fondamentale rilievo è l'ordinanza della Cass.civ., sez. VI, 3-23 gennaio 2019, n. 1725, cit. che offre significativi spunti ricostruttivi della fattispecie di cui all'art. 2051 c.c.⁵⁴.

La Corte di legittimità, nell'articolare la propria decisione, ha preso le mosse dalla valutazione che la custodia si attua non solo nell'effettuare sulla cosa degli interventi riparatori successivi, miranti a neutralizzare, in un tempo ragionevole, gli elementi pericolosi non prevedibili che si siano comunque verificati; ma, altresì, in un'attività preventiva che, sulla base di un giudizio di prevedibilità *ex ante*, appresti quanto sia necessario per prevenire danni eziologicamente concernenti la cosa custodita. Da ciò si fa discendere che si possa rinvenire il caso fortuito, idoneo a determinare l'esclusione della responsabilità, nella condotta del terzo, purchè la stessa determini una modificazione dello stato della cosa che sia imprevedibile ed imprevedibile, nonchè non eliminabile o segnalabile tempestivamente. La responsabilità va, quindi, esclusa nell'ipotesi in cui il custode "non abbia avuto tempo sufficiente per intervenire ed eliminare l'impreveduto/imprevedibile"⁵⁵.

⁵³ Per tali notazioni cfr. M. NATALE, op.cit., p. 47 s.

⁵⁴ Nel caso di specie, la Suprema Corte ha cassato la sentenza della Corte d'Appello di Bari che aveva escluso la responsabilità di un Comune per i danni subiti dal conducente di un motociclo, il quale era caduto, a causa della presenza sulla strada della cera sparsa dai partecipanti a una processione religiosa, ravvisando in essa gli estremi del caso fortuito - da annoverarsi come un fattore esterno creato dal terzo, non conoscibile, né eliminabile dalla P.A. con immediatezza, neppure adottando la più diligente attività di manutenzione. Per le considerazioni che seguono, nel corpo del testo, cfr. A. SCALERA, Dalla "res" al custode: verso la contrattualizzazione della responsabilità ex art. 2051 c.c.?, in commento al provvedimento, in Corr.giur., 2020, pp. 479- 482.

⁵⁵ In riferimento al caso concreto, la Corte sottolinea che l'ente pubblico, essendo a conoscenza della processione religiosa tradizionale, avrebbe potuto prevenire il danno, mediante l'apposizione di transenne o di cartelli che segnalassero il pericolo costituito dal manto stradale scivoloso.

Senza dubbio, la soluzione interpretativa della Suprema Corte è del tutto originale, in quanto elabora una nuova ricostruzione della responsabilità da cose in custodia. Il modello formulato dalla pronuncia sposta il «baricentro» della responsabilità dalla *res* custodita al custode o meglio all'attività del medesimo; imperniandosi sull'obbligo di custodia, il cui «inadempimento» farebbe nascere la responsabilità del custode, a meno che questi non provi il caso fortuito, ossia di essersi trovato nell'impossibilità giuridica di adempiere.

La soluzione si allontana sia dalla tesi della responsabilità oggettiva, sia da quella della «responsabilità aggravata», dando luogo ad un'interpretazione dell'art. 2051 c.c. che accosta il regime ivi disciplinato al modello delineato dall'art. 1218 c.c. Nello schema raffigurato dal provvedimento, l'inadempimento dell'obbligo custodiale finisce col rappresentare perfino un elemento costitutivo della fattispecie ex art. 2051 c.c., alla stregua di quanto accade per l'inadempimento delle obbligazioni, ai fini dell'insorgere della responsabilità contrattuale.

L'operazione ermeneutica, condotta dalla Cassazione, è confutabile⁵⁶, sia in quanto, di fatto, determina «un'interpretatio abrogans» della norma che si incentra sulla *res* custodita che provoca l'evento lesivo; sia per le conseguenze sul piano processuale, in quanto si assiste ad un alleggerimento della posizione del danneggiante e ad un aggravamento degli oneri di allegazione e prova a carico del danneggiato.

Quest'ultimo, oltre a dover provare il nesso di causalità tra la cosa e l'evento lesivo, dovrà anche dedurre l'inadempimento del custode, individuando gli elementi dai quali desumere la prevedibilità dell'evento dannoso e la violazione degli obblighi di vigilanza. Il custode, differentemente, ai fini dell'esclusione della responsabilità, non dovrà dimostrare che l'evento lesivo è stato determinato da un fattore esterno alla *res*, ma più semplicemente di aver fatto tutto ciò che era possibile in termini di custodia.

Da ultimo, in linea con la pronuncia commentata⁵⁷, la Suprema Corte (sez. VI), con l'ordinanza 2 maggio 2022, n. 13729⁵⁸, ha avvalorato l'obbligo di custodia che si concretizzi in obblighi di vigilanza, controllo e diligenza che impongano al custode di adottare tutte le misure idonee per prevenire e impedire la produzione di danni a terzi; per porre, di seguito, in capo a costui la prova del caso fortuito in termini particolarmente rigorosi⁵⁹.

4. I «nuovi» danni da sistemi di intelligenza artificiale: riconducibilità agli schemi di responsabilità civile vigenti nel nostro ordinamento *versus* riforma legislativa.

⁵⁶ Si condividono le osservazioni critiche di A. SCALERA, op.ult.cit., pp. 482 ss.

⁵⁷ L'ordinanza richiama Cass.civ., sez. 3, ord., 12 maggio 2020 n. 8811.

⁵⁸ Pubblicata in italiure.giustizia.it

⁵⁹ La Cassazione ha condannato il Comune per danno da cosa in custodia, per un caso di caduta del ciclista per avvallamento stradale, affermando che la condotta del danneggiato non integri gli estremi del caso fortuito (come sostenuto in primo ed in secondo grado), per il solo fatto che la presenza di sconnessioni su una strada extraurbana sia una situazione non eccezionale e, pertanto, prevedibile dall'utente e, tanto più, rilevabile per la sua dimensione e per l'orario in cui era avvenuto il sinistro. La Cassazione ha, così, sottolineato che «ragionando diversamente, tutti i custodi di strade potrebbero permettersi di lasciarle non riparate a tempi indefiniti, ovvero astenersi dalla custodia, perché gli avvallamenti possono essere percepiti materialmente da chi passa nelle ore luminose del giorno, soltanto negli orari notturni «risorgendo» la custodia».

La fattispecie di cui all'art. 2051 c.c. costituisce, negli ultimi anni, oggetto di interpretazioni innovative in merito ad un altro profilo del tutto nuovo. La dottrina si pone il quesito della riconduzione delle ipotesi di responsabilità civile per i danni derivanti da sistemi di intelligenza artificiale nell'alveo dei modelli tradizionali di responsabilità civile extracontrattuale vigenti nel nostro ordinamento, ponendo particolare attenzione alle responsabilità "speciali" disciplinate nel codice civile, tra le quali propriamente la responsabilità da cosa in custodia⁶⁰.

Nell'affrontare la tematica, è nodale osservare, in via preliminare, che le nuove forme di tecnologia digitale, più o meno automatizzate, possono dar luogo ad una pluralità di scenari dannosi completamente diversi, rispetto a quelli tradizionalmente affrontati a livello giurisprudenziale⁶¹. Ciò accade non soltanto quando i danni siano provocati dai robot che compiano attività che potrebbero essere svolte dagli esseri umani, ma anche quando siano cagionati da intelligenze artificiali, dotate di capacità di autoapprendimento, le cui scelte siano assunte in base all'elaborazione di un algoritmo⁶².

Queste ultime si connotano per l'attitudine ad assumere decisioni autonome che conseguano ad un processo di adattamento c.d. *self learning*: il sistema intelligente si confronta con la realtà e si trasforma coerentemente con i dati esperienziali acquisiti nel tempo⁶³, elaborando decisioni e comportamenti che potrebbero non essere previsti in fase di progettazione e rappresentare, invece, il risultato di interazioni inaspettate tra i componenti del sistema o con il contesto nel quale operino⁶⁴.

Tali decisioni e comportamenti sono complessi, opachi, incontrollabili ed imprevedibili e, pertanto, non facilmente accertabili e possono condurre

⁶⁰ Il «sistema di intelligenza artificiale» è definito «un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici» dall'art. 3, lett. a) della Proposta di Regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, formulata nella Risoluzione del 20 ottobre 2020, recante raccomandazioni alla Commissione europea su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)). Tra i numerosi contributi sulle rilevanti questioni giuridiche sollevate dall'impiego dell'intelligenza artificiale, nei più svariati settori, cfr. P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), Rapporti civilistici e intelligenze artificiali: attività e responsabilità, Napoli, 2020, passim; ID. (a cura di), Il trattamento algoritmico dei dati tra etica, diritto e economia, Napoli, 2020, passim; G. ALPA (a cura di), Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile, Pisa, 2020, passim; U. RUFFOLO (a cura di), Intelligenza artificiale. Il diritto, i diritti, l'etica, Torino, 2020, passim; A. SANTOSUOSSO, Intelligenza e diritto. Perché le nuove tecnologie sono una grande opportunità per il diritto, Milano, 2020, passim; S. FARO, T.E. FROSINI, G. PERUGINELLI (a cura di), Dati e algoritmi. Diritto e diritti nella società digitale, Bologna, 2020, passim; D. BUZZELLI, M. PALAZZO (a cura di), Intelligenza artificiale e diritti della persona, Pisa, 2022, passim; M. TAMPIERI, L'intelligenza artificiale e le sue evoluzioni. Prospettive civilistiche, Padova, 2022, passim.

⁶¹ Cfr. A. AMIDEI, Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo, in Giur.it., 2021 p. 100.

⁶² Cfr. L. COPPINI, Robotica e intelligenza artificiale: questioni di responsabilità civile, in Politica del diritto, 2018, p. 722. È imprescindibile la puntualizzazione che non si può parlare di un'unica intelligenza artificiale, ma deve diversamente parlarsi di intelligenze artificiali al plurale, giacché le stesse possono differenziarsi, a seconda dei tipi di machine learning o di agenti software, più o meno autonomi.

⁶³ Cfr. U. SALANITRO, Intelligenza artificiale e responsabilità: la strategia della Commissione Europea, in Riv.dir.civ., 2020, p. 1247.

⁶⁴ Cfr. L. COPPINI, op.cit., p. 721. Più precisamente, l'art. 3, lett. b) della Proposta di Regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, cit., definisce «autonomo» il «sistema basato sull'intelligenza artificiale che opera interpretando determinati dati forniti e utilizzando una serie di istruzioni predeterminate, senza essere limitato a tali istruzioni, nonostante il comportamento del sistema sia legato e volto al conseguimento dell'obiettivo impartito e ad altre scelte operate dallo sviluppatore in sede di progettazione».

all'erroneità degli *output*, a potenziali discriminazioni (si pensi al *credit scoring* che incide sulle decisioni delle banche di erogare il credito) ed alla compromissione delle libertà e dei diritti fondamentali della persona, quali la sicurezza degli individui, la loro salute, la vita privata e la protezione dei dati personali, l'integrità, la dignità, l'autodeterminazione⁶⁵.

Sorge allora il problema della responsabilità civile, dal momento che non esiste, allo stato attuale, una normativa *ad hoc* e si avverte, in maniera sempre più impellente, non solo l'esigenza di garantire una spinta deterrente nei confronti dei potenziali *tortfeasors*, ma altresì il bisogno di approntare un efficace sistema di tutele, al fine di evitare che l'impiego di tecnologie intelligenti possa implicare una diminuzione di sicurezza e di responsabilità rispetto a quella tradizionale (c.d. equivalenza funzionale). Nel perseguire tale obiettivo, si deve principalmente rispondere al quesito di portata giuridica, nonché etica, di chi e a quale titolo sia il soggetto responsabile delle condotte autonome dei sistemi intelligenti e, di riflesso, dei danni dalle stesse cagionati, al fine allocarli nel modo più opportuno e, cioè, su colui che sia meglio in grado di minimizzarli⁶⁶.

L'individuazione del danneggiante assume particolare importanza in tale ambito, dal momento che è inevitabile che la responsabilità venga condivisa tra più soggetti che intervengano nel "ciclo di vita" dei sistemi di intelligenza artificiale, creandolo, eseguendone la manutenzione o controllandone i rischi associati⁶⁷.

Si rende, a tal uopo, doveroso scegliere il metodo da seguire, al fine di identificare il soggetto cui imputare i danni, nei confronti del quale il danneggiato possa azionare la propria pretesa risarcitoria. Due sono fondamentalmente gli approcci seguiti dalla letteratura giuridica.

Parte della dottrina, al fine di individuare nuovi centri di imputazione della responsabilità, ha riconosciuto una nuova condizione di soggettività giuridica, quanto meno parziale, ai sistemi di intelligenza artificiale⁶⁸. Sussisterebbe, in tali

⁶⁵ Sul punto cfr. M. GAMBINI, Responsabilità civile e controlli del trattamento algoritmico, in: P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), Il trattamento algoritmico dei dati tra etica, diritto e economia, op.cit., p. 314; sull'erroneità degli output, D. DI SABATO, Strumenti riparatori e risarcitori, ivi, p. 338. Autorevolmente P. PERLINGIERI, Relazione conclusiva, ivi, p. 383, puntualizza come l'esigenza di ovviare all'opacità del procedimento algoritmico si avverta in ogni settore e che il rischio digitale si pone tanto come collettivo, quanto individuale. Avendo specifico riguardo alla protezione dei dati personali «nell'era dell'intelligenza artificiale», arguta dottrina (T.E. FROSINI, La privacy nell'era dell'intelligenza artificiale, in DPCE online, 1/2022, pp. 282 ss.), dopo aver posto in evidenza che quest'ultima pone nuove questioni giuridiche riferite alla privacy, rimarca che il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, c.d. Regolamento generale sulla protezione dei dati personali, non è compatibile con i modelli attuali di gestione algoritmica dei flussi di dati personali che determinano decisioni in vari ambiti.

⁶⁶ Sul punto si v. la "Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità", 19 febbraio 2020, (COM (2020), 64 final), p. 19; cfr. le argute riflessioni di G. COMANDÉ, Multilayered (Accountable) Liability for Artificial Intelligence, in S. LOHSS, R. SCHULZE, D. STAUDENMAYER (a cura di), Liability for Artificial Intelligence and the Internet of Things, Baden-Baden, 2019, p. 169.

⁶⁷ Cfr. G. CAPILLI, I criteri di interpretazione della responsabilità, in G. ALPA, (a cura di) Diritto e intelligenza artificiale, op.cit., p. 477.

⁶⁸ Cfr., ex multis, G. SARTOR, Gli agenti software: nuovi soggetti del ciberdiritto?, in Contr. e impr., 2002, 2, p. 483 ss.; G. TEUBNER, I soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi, Napoli, 2019, passim e la prefazione al volume di P. FEMIA, Soggetti responsabili. Algoritmi e diritto civile, ivi, pp. 5 ss. Sul tema cfr. anche D. DI SABATO, Gli smart contracts: robot che gestiscono il rischio contrattuale, in Contr.impr., 2017, p. 389; M.L. LACRUZ MANTECÓN, Robots y personas. Una aproximación jurídica a la subjetividad cibernética, Reus, Madrid, 2020.

termini, il vantaggio di limitare la responsabilità dei programmatori e degli utilizzatori dei servizi del nuovo potenziale soggetto, al fine di promuovere il progresso tecnologico; sotto un altro punto di vista, la soggettività sarebbe connessa alla formazione di un patrimonio ovvero alla costituzione di un fondo assicurativo dedicato, obbligando gli operatori, che si ritenga debbano sopportare il rischio, ad effettuare i conferimenti. La ricostruzione è stata avallata dalla letteratura giuridica, evidenziando che non sarebbe impossibile sotto il profilo giuridico-concettuale, potendosi ricavare il riconoscimento della soggettività giuridica dal modello delle persone giuridiche o da quello dei patrimoni separati⁶⁹.

Tale soluzione è stata ventilata inizialmente anche dalle Istituzioni europee, sulla scia di un più ampio dibattito, riguardante il riconoscimento della soggettività giuridica alle macchine che ha occupato, da tempo, gli studiosi di filosofia morale e di diritto⁷⁰.

Nonostante ciò, autorevoli voci dottrinali hanno espresso argomentazioni fortemente critiche, condivise da chi scrive, sostenendo che debba respingersi l'idea del riconoscimento della "personalità elettronica" ai sistemi di intelligenza artificiale, dal momento che finisce con l'esaltare, in maniera esorbitante, le prerogative delle macchine che, seppur intelligenti, sono, in ogni caso, creazione dell'uomo, rispondono integralmente alla programmazione da costui prevista di fatto e sono incapaci di autodeterminazione e di libertà di scelta⁷¹. Di qui, il corollario che esse possono essere oggetti e non soggetti di diritto, con la conseguenza che non vi sarà spazio per un *tertium genus* di responsabilità.

Di imprescindibile rilevanza è la circostanza che tale opzione, dopo un'apertura iniziale a livello europeo, da parte del Parlamento, nella Risoluzione 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (cit.), è stata progressivamente abbandonata, prima dal Comitato economico e sociale europeo che ha esposto perplessità di carattere giuridico ed etico⁷² e successivamente dal Parlamento europeo stesso che ha espressamente chiarito che i sistemi di intelligenza artificiale non

⁶⁹ Cfr. P. SERRAO D'AQUINO, La responsabilità civile per l'uso di sistemi di intelligenza artificiale nella Risoluzione del Parlamento Europeo del 20 ottobre 2020 "Raccomandazioni alla Commissione sul regime della responsabilità civile e intelligenza artificiale", § 1, in www.giustiziainsieme.it/it/news/127-main/dirittoeinnovazione/, § 2.

⁷⁰ L'opportunità di attribuire una "personalità elettronica" ai robot, capaci di autoapprendimento (self-learning), è stata vagliata dalla Risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, (2018/C 252/25), Considerando 59, lett. f).

⁷¹ Tra i numerosi autori, cfr. A. BERTOLINI, Robots as Products: the case for a realistic analysis of robotics applications and liability rules, in *Law Innov. Technol.*, 2013, 1, pp. 214 ss.; L. COPPINI, op.cit., pp. 722 ss.; M. COSTANZA, L'intelligenza artificiale e gli stilemi della responsabilità civile, in *Giur. it.*, 2019, pp. 1686 ss.; M. INFANTINO, La responsabilità per danni algoritmici: prospettive europeo continentali, in *Resp.civ.prev.*, 2019, pp. 1762 ss.; U. RUFFOLO, La responsabilità da artificial intelligence, algoritmo e smart product: per i fondamenti di un diritto dell'intelligenza artificiale self learning, in *ID.* (a cura di), *Intelligenza artificiale. Il diritto, i diritti e l'etica*, op.cit., pp. 93 ss.; G. FINOCCHIARO, Intelligenza artificiale e responsabilità, in *Contr.impr.*, 2020, pp. 713 ss.; F. NADDEO, Intelligenza artificiale: profili di responsabilità, in *Comparazione e diritto civile*, 2020, p. 1161; L. ULISSI, I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, op.cit., p. 436; G. COMANDÉ, Intelligenza artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell'IA e il problema della responsabilità, in *Analisi Giuridica dell'Economia*, 2019, p. 175.

⁷² Si v. il Parere del Comitato economico e sociale europeo su "L'intelligenza artificiale. Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società", (2017/C 288/01), punto 3.33.

possiedono né una personalità giuridica, né una coscienza umana e che il loro compito consiste nel servire l'umanità⁷³.

Seguendo tale impostazione, le tecnologie emergenti andrebbero, in definitiva, trattate come beni e la responsabilità incomberebbe, a seconda delle circostanze del caso concreto, su un soggetto specifico, individuo o ente, tra i molteplici attori coinvolti nella produzione, nell'operatività o nell'impiego dei sistemi intelligenti.

Il giurista deve pertanto interrogarsi se e sulla base di quali presupposti la responsabilità gravi, in particolare, sull'ideatore-autore-progettista dell'algoritmo veicolante l'apprendimento; ovvero su colui che lo utilizzi o lo "produca" o lo incorpori in un prodotto oppure in un componente dello stesso; oppure, sull'utilizzatore (*user*) o sul "titolare" (a vario titolo) ovvero sul "custode" del dispositivo digitale⁷⁴.

Tra coloro cui imputare la c.d. "responsabilità da algoritmo", i soggetti suddetti assumono una posizione preminente per le ragioni che seguono⁷⁵.

Mutuando le considerazioni di attenta dottrina, si premetta⁷⁶ che l'algoritmo, quale creazione intellettuale, pur non comparando come componente separato del prodotto finale, attribuisce "l'anima" al *software* di un'intelligenza artificiale, al quale conferisce l'attitudine ad apprendere. L'algoritmo, invero, entra in modo dinamico nella configurazione del prodotto che lo incorpora, condizionandone il suo modo di essere ed il divenire e «forgiandone o alterandone la "*mentalité*" ed il ruolo (con)causale nei suoi "atti" e comportamenti futuri». L'intelligenza artificiale diventa "mutante", grazie all'algoritmo ed è proprio questo aspetto che assume rilevanza primaria nei sistemi di intelligenza artificiale *self-learning* che evolvono, in relazione alla propria esperienza dalla quale apprendono direttamente. Tutto ciò rende più complicato produrre beni potenzialmente non dannosi, giacché è la presenza stessa dell'intelligenza artificiale che si evolve, imparando dall'esperienza, che finisce col risultare essere un "difetto", quando il processo di autoapprendimento appaia, ad ogni modo, idoneo ad indirizzare il bene verso la causazione di effetti dannosi. Ciò accade quando alla capacità di evolvere con l'autoapprendimento non si accosti la presenza di "blocchi" o limiti interni, adatti ad inibire future "deviazioni" dell'intelligenza artificiale (o comunque del dispositivo intelligente che lo incorpora) che potrebbero realizzare comportamenti dannosi.

Ciò detto, nell'operazione di imputabilità della c.d. "responsabilità da algoritmo", la prima considerazione da fare è che l'"autore" dello stesso potrebbe

⁷³ Si fa riferimento alla Proposta di Regolamento del Parlamento europeo e del Consiglio del 20 ottobre 2020 sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale (considerando 6), cit. Lo sviluppo di tecnologie emergenti solleva importanti questioni di carattere etico che sono state oggetto di esame dal parte del Parlamento europeo che, lo stesso giorno, ha emanato la Risoluzione recante raccomandazioni alla Commissione, concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)), sulla quale cfr. le notazioni di M. CASTILLA BAREA, La universidad ante los desafíos éticos de la inteligencia artificial. Reflexiones a propósito del nuevo «marco europeo de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas», in *EduNovatic 2020, Conference Proceedings: 5th Virtual International Conference on Education, Innovation and ICT*, December 10 - 11, 2020, pp. 630 ss.

⁷⁴ Cfr. U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, op.cit., p. 1691.

⁷⁵ Cfr. G. CAPILLI, op.cit., p. 477, precisa che è inevitabile che la responsabilità possa essere condivisa tra i soggetti che abbiano contribuito alla realizzazione del prodotto dotato di intelligenza artificiale, quali il progettista dell'algoritmo, l'editore del software, il proprietario del database, l'assemblatore/produttore, il fornitore di rete ed, in alcuni casi, anche il proprietario o l'utente.

⁷⁶ Per le riflessioni che seguono, cfr. U. RUFFOLO, op. ult.cit., pp. 1691-1700.

essere un soggetto diverso dal “produttore” di un’entità artificiale intelligente che lo incorpori in un prodotto intelligente ovvero in un suo componente. Ebbene l’algoritmo, destinato per sua natura ad essere incorporato nel “prodotto”, potrebbe essere inteso come un mero progetto, una mera idea o formula, vale a dire un’entità non ancora adeguata a divenire componente fisica di un prodotto o di parte di esso (quali il *software* di cui sia munito); l’ideatore dell’algoritmo si configurerebbe, così, come un semplice “fornitore” di idee o progetti e sarebbe, dunque, problematico immaginare una sua responsabilità autonoma. Sotto un diverso angolo di visuale, l’ideazione dell’algoritmo potrebbe essere valutata quale ‘componente’ immateriale, caratterizzante il sistema di intelligenza artificiale. In tale ottica, si potrebbe reputare “produttore” non solo il produttore del complessivo *software* che lo incorpori, ma anche l’inventore dell’algoritmo, nella veste di produttore di un “componente” del prodotto intelligente; potrebbe, così, sorgere in capo a quest’ultimo, oltre alla responsabilità contrattuale verso il proprio committente, in maniera correlata, la responsabilità extracontrattuale verso i terzi danneggiati dal prodotto difettoso intelligente.

Ulteriore aspetto da valutare è che i danni provenienti da sistemi di intelligenza artificiale *self-learning* potrebbero derivare da *bias* imputabili agli “insegnamenti” ricevuti direttamente o indirettamente dall’“addestratore”, figura identificabile in colui che “addestrì” un’entità artificiale intelligente o la esponga ad esperienze che siano congrue ad indirizzarlo ovvero ad istruirlo. In tale ipotesi, si porrebbe la questione della sua responsabilità, quantomeno concorrente con quella del produttore di un’entità artificiale intelligente e/o con quella dell’ideatore dell’algoritmo, se distinto da quest’ultimo.

Si può, infine, prevedere l’imputabilità della responsabilità per i danni cagionati da dispositivi digitali in capo all’utente, al titolare o al custode, in ragione della relazione di custodia con il bene che rappresenta il fondamento della responsabilità da cosa in custodia, ex art. 2051 c.c.

Una volta identificati i soggetti potenzialmente responsabili, a seconda delle ipotesi, è, come ovvio, necessario definire il regime di imputazione e la natura della responsabilità loro imputabile⁷⁷.

La dottrina ha individuato due possibili direzioni da seguire⁷⁸. Ci si è domandati⁷⁹ se lo strumentario giuridico esistente nel nostro sistema giuridico sia congruo a rispondere alle innumerevoli sfide che la nuova realtà fenomenica dell’intelligenza artificiale pone, dandosi luogo ad un adeguamento, in via interpretativa, delle norme civilistiche sulla responsabilità civile e della disciplina della responsabilità da prodotto difettoso⁸⁰; oppure se, in assenza di soluzioni appropriate alle criticità emergenti, sia essenziale la previsione di nuovi paradigmi di tutela, da introdurre per mezzo di riforme legislative di rilievo che dettino nuove regole e/o modifichino quelle esistenti⁸¹.

⁷⁷ Cfr. I. GIUFFRIDA, Liability for AI Decision-Making: Some Legal and Ethical Considerations, in *Fordham Law Review*, 2019, 88, 2, p. 443.

⁷⁸ Si v. i riferimenti della dottrina citata in nota 71.

⁷⁹ Cfr. E. SEVERINO, N. IRTI, Dialogo su diritto e tecnica, Roma-Bari, 2001, pp. 28 ss.; G. ALPA, Prefazione, in ID. (a cura di), *Diritto e intelligenza artificiale*, op.cit., p. 14.

⁸⁰ Di tale avviso, cfr., ex multis, G. FINOCCHIARO, op.cit., pp. 713 ss.; U. RUFFOLO, La responsabilità da artificial intelligence, algoritmo e smart product, op.cit., pp. 96 ss.; L. COPPINI, op.cit., p. 739.

⁸¹ Cfr. G. TEUBNER, op.cit., pp. 26 ss.; A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, Robot e diritto: una prima ricognizione, in *Nuova giur.civ.comm.*, 2021, pp. 494 ss.; R.M. AGOSTINO, Intelligenza artificiale e processi decisionali, in *Mercato Concorrenza Regole*, 2020, p. 373; G. COMANDÉ, Intelligenza artificiale e

In linea con l'importante mutamento di opinione del Parlamento europeo e della posizione espressa dal Governo italiano, con le proposte degli esperti del MISE⁸², si ritiene che, in assenza di una normativa *ad hoc*, prima di decidere se sia necessaria una riforma legislativa, sia primario compito dell'interprete valutare l'idoneità del nostro sistema giuridico a rispondere alle nuove problematiche poste dalle tecnologie digitali emergenti.

A tal fine, si dovranno profilare le potenziali situazioni di conflitto che possano essere causate dai sistemi di intelligenza artificiale, contemplando anche la gradualizzazione e la diversificazione delle attività dagli stessi svolte⁸³; esaminare i regimi vigenti di responsabilità civile e vagliare la sussistenza di soluzioni confacenti al caso concreto, in ordine alla natura e ai criteri di imputazione della responsabilità civile.

Nello svolgimento di tale operazione, l'interprete dovrà procedere ad un'interpretazione sistematica ed assiologica *evolutiva*⁸⁴ della disciplina attuale sulla responsabilità civile, ponendo attenzione alle *prospettive de jure condendo* in ambito europeo e tener conto del profilo inscindibile dell'assiologia dei valori del nostro sistema ordinamentale.

Per individuare la disciplina «più adeguata» al caso concreto, sarà determinante operare un bilanciamento⁸⁵ dei contrapposti interessi dei soggetti implicati nella produzione e nell'operatività dei sistemi intelligenti, da un lato, e dei destinatari dei comportamenti e delle decisioni dei sistemi stessi, dall'altro, alla luce dei valori imposti dalla Carta Costituzionale ed a livello europeo, vale a

responsabilità tra liability e accountability, op.cit., p. 170; C. LAENZA, Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio, in *Resp.civ. prev.*, 2021, p. 118.

⁸² Se inizialmente il Parlamento europeo, con la Risoluzione del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, cit., esortava la Commissione all'adozione di un intervento legislativo innovativo sulle questioni giuridiche attinenti allo sviluppo e all'impiego della robotica e dell'intelligenza artificiale; in un secondo momento, con la Risoluzione del 12 febbraio 2019, relativa a una politica industriale europea globale in materia di robotica e intelligenza artificiale (2018/2088 (INI)), il Parlamento europeo ha diversamente chiesto alla Commissione di riesaminare i regimi esistenti di responsabilità correttamente funzionanti, allo scopo verificarne la congruità; inoltre, nell'allegato A della Risoluzione del 20 ottobre 2020, recante raccomandazioni alla Commissione europea su un regime di responsabilità civile per l'intelligenza artificiale, cit., nel formulare gli obiettivi della suddetta proposta di regolamento sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, ha dichiarato che, invece di sostituire i regimi esistenti di responsabilità correttamente funzionanti, è opportuno operare gli adeguamenti necessari per l'intelligenza artificiale. Tale approccio è stato condiviso, in assenza di una normativa *ad hoc*, dal Governo italiano, con le "Proposte per una strategia nazionale per l'Intelligenza Artificiale", elaborate, a luglio 2020, dal Gruppo di esperti dell'innovazione tecnologica, istituito presso il Ministero dello Sviluppo Economico, punto 5.1.2. Al riguardo, cfr. C. PERLINGIERI, Responsabilità civile e robotica medica, in *Tecnologie e diritto*, 2020, p. 162 s.

⁸³ Cfr. C. PERLINGIERI, op.cit., p. 165, la quale conduce un'attenta analisi della tematica della responsabilità civile nel campo della robotica medica.

⁸⁴ Seguendo l'influente insegnamento di Pietro Perlingieri. Tra i numerosi contributi dell'Autore, cfr. P. PERLINGIERI, L'interpretazione della legge come sistematica ed assiologica: il broccardo in *claris non fit interpretatio*, il ruolo dell'art. 12 disp.prel. codice civile e la nuova scuola dell'esegesi, in *Rass.dir.civ.*, 1985, pp. 990 ss.; ID., Interpretazione ed evoluzione dell'ordinamento, *Riv.dir.priv.*, 2011, pp. 160 ss.

⁸⁵ Ci si pone in linea con l'indirizzo di P. PERLINGIERI, (Formazione dei giudici e Scuola superiore della magistratura, in *Giust.proc.civ.*, 2007, p. 313) che sottolinea che il giudice deve individuare la disciplina «più adeguata» al caso concreto, non fermandosi al dato letterale della 'legge formale', ma calandola invece all'interno del contesto storico-giuridico attuale ed operando altresì un bilanciamento degli interessi e dei principi e dei valori normativi che il fatto stesso ha espresso. Sulla «ragionevolezza» quale «canone ermeneutico ed argomentativo», «filo conduttore» di ogni ragionamento giuridico, per il contemperamento di principi ed interessi, in coerenza col sistema giuridico di riferimento e tutti i suoi valori, cfr. G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, pp. 16-29, p. 43, p. 135.

dire della primazia della persona umana sulle ragioni del mercato⁸⁶. Tutto ciò, come sottolineato dalle Istituzioni europee nei suoi numerosi provvedimenti di *soft law* ed in quelli di *hard law* in corso di approvazione, in una prospettiva che sappia coniugare la promozione del progresso tecnologico, che condurrà ad indubbi vantaggi alla collettività ed ai soggetti individualmente, con le esigenze di sicurezza dei sistemi di intelligenza artificiale e di una tutela effettiva dei diritti e delle libertà fondamentali⁸⁷.

5. L'invocabilità del regime della responsabilità da cose in custodia.

Nel ricondurre i “nuovi” danni da sistemi di intelligenza artificiale agli schemi di responsabilità civile vigenti nel nostro ordinamento, possono entrare in gioco due aspetti⁸⁸.

Il primo riguarda la responsabilità del produttore, visto che le tecnologie dell'intelligenza artificiale, incorporate in beni o servizi, possono determinare nuovi rischi per la sicurezza degli acquirenti o degli utenti; il secondo attiene alla responsabilità contrattuale o extracontrattuale che è soggetta alle discipline di rilevanza generale nei singoli Stati membri dell'Unione europea, talvolta improntate a principi molto distanti tra loro.

Rilevanza centrale assume quindi, *in primis*, la disciplina europea della responsabilità da prodotto difettoso che concerne il risarcimento dei danni cagionati da difetti di fabbricazione di un prodotto, introducendo un regime di responsabilità oggettiva che prescinde dall'accertamento della colpa⁸⁹.

La disciplina potrebbe essere applicata, ricomprendendosi i sistemi di intelligenza artificiale nella nozione di “prodotto” (ai sensi dell'art. 2 della direttiva e dell'art. 115, comma 1, Cod.Cons. che lo definiscono come «ogni bene mobile, anche se forma parte di un altro bene mobile o immobile») e raffigurando la sussistenza del difetto (ai sensi degli artt. 6 della direttiva e 117, cod.cons. che qualificano un prodotto “difettoso” «quando non offre la sicurezza che ci si può legittimamente attendere tenuto conto delle circostanze») in un errore di progettazione, di programmazione (nel qual caso verrebbe in rilievo l'algoritmo) o di costruzione⁹⁰.

Avendo prioritario riguardo ai sistemi di intelligenza artificiale *self-learning*, dalla qualificazione dell'algoritmo quale “componente” (immateriale) del

⁸⁶ Cfr. M. GAMBINI, op.cit., p. 314.

⁸⁷ Cfr. A. PAJNO, M. BASSINI, G. DE GREGORIO, M. MACCHIA, F.P. PATTI, O. POLICINO, S. QUATTROCOLO, D. SIMEOLI, P. SIRENA, AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista, in www.biodiritto.org, p. 2.

⁸⁸ In tal senso, cfr. U. SALANITRO, op.cit., p. 1253.

⁸⁹ La disciplina è attualmente dettata dalla direttiva comunitaria 85/374/CE del Consiglio del 25 luglio 1985 sulla responsabilità per danni da prodotti difettosi, ormai confluita in Italia nel Codice del Consumo, negli artt. 114 ss. La direttiva si inserisce nell'ambito di un quadro normativo europeo di riferimento, nel quale rientrano provvedimenti che sono espressione dell'attuazione del principio di precauzione, quale strumento per gestire l'incertezza, facendo sì che la responsabilità da danno da prodotto difettoso sia traslata ai soggetti produttori (U. IZZO, La precauzione nella responsabilità civile, Padova, 2004, p. 1).

⁹⁰ Sul punto e per le riflessioni che seguono, cfr. L. COPPINI, op.cit., pp. 727-729; U. RUFFOLO, Intelligenza artificiale, machine learning e responsabilità da algoritmo, op.cit., pp. 1693 s., p. 1698. Sul ruolo che la responsabilità da prodotto difettoso è adeguata a svolgere nel governo dei nuovi rischi attinenti allo sviluppo delle tecnologie digitali, si v. anche R. MONTINARO, Responsabilità da prodotto difettoso e tecnologie digitali tra *soft law* e *hard law*, in *Persona e mercato*, 2020/4, pp. 365 ss.

dispositivo intelligente scaturirebbe la configurabilità della responsabilità dell'ideatore dell'algoritmo, se diverso dal produttore dell'entità artificiale intelligente che lo incorpori, in applicazione della norma che statuisce la responsabilità sia del produttore che realizzi il prodotto finito, sia del produttore della materia prima o di un "componente" dello stesso (art. 3 della direttiva e dell'art. 115, comma 2 *bis* Cod.cons.). La responsabilità dell'inventore dell'algoritmo sarebbe distinta da quella del produttore del dispositivo che lo incorpori e sussisterebbe nei confronti del soggetto che subisca un pregiudizio cagionato da un errore di apprendimento. La responsabilità dell'ideatore dell'algoritmo concorrerebbe con quella del produttore, in linea con l'impostazione improntata dalla Direttiva che prevede la responsabilità cumulativa e non alternativa dei soggetti facenti parte della catena produttiva, con l'obiettivo di offrire effettiva tutela ai consumatori⁹¹.

Si consideri, tuttavia, che il paradigma della responsabilità da prodotto difettoso non offre risposte esaurienti per tutti gli scenari di "nuovi danni" provocati dalle intelligenze artificiali, in quanto applicabile nelle sole ipotesi in cui i pregiudizi siano cagionati da un errore di progettazione, di programmazione o di costruzione dei sistemi intelligenti⁹².

È d'uopo, pertanto, indagare l'invocazione delle tradizionali regole civilistiche agli altri casi che possano prospettarsi.

Si rilevi innanzitutto che se, per un verso, l'art. 2043 c.c. assume primario rilievo, dal momento che, in quanto previsione generale, connotata dal carattere di atipicità, è applicabile a qualsivoglia tipologia di illecito ed è confacente alle evoluzioni delle tecnologie, senza richiedere, di per sé, alcun adattamento ai fini del suo impiego; per altro verso, la struttura della norma risulta inappropriata a

⁹¹ Auspicano un intervento normativo di riforma della direttiva che preveda espressamente l'algoritmo quale componente del prodotto finale, cfr. L. COPPINI, *op.cit.*, pp. 728, 739; F. NADDEO, *op.cit.*, p. 1161.

⁹² Si rimarchi, vieppiù, che la disciplina della responsabilità del produttore solleva una serie di perplessità sull'idoneità a far fronte a tutte le sfide poste dall'intelligenza artificiale. Le perplessità sollevate dalla dottrina attengono a più profili. Si dubita precipuamente che i moderni prodotti di intelligenza artificiale, quantomeno i più avanzati, possano rientrare nella tradizionale definizione di «prodotto», dal momento che i sistemi di deep learning (apprendimento automatico) e di full automation (automazione completa) agiscono in piena autonomia, secondo processi non sempre controllabili da parte dei produttori. Per un attento esame della questione cfr. ex multis, I. ZURITA MARTÍN, *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Reus, Madrid, 2020, passim; recensito da F. J. JIMÉNEZ MUÑOZ, in *Actualidad Jurídica Iberoamericana* N° 14, febrero 2021, pp. 1141 ss.; C. LAENZA, *op.cit.*, p. 1018; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, in *Study Requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies*, Bruxelles, 2020, p. 56; U. RUFFOLO, *Responsabilità da produzione e gestione dell'a.i. self-learning*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, *op.cit.*, pp. 233 ss. Assume pertanto pregnante rilievo l'iniziativa della Commissione europea che, il 28 settembre 2022, ha presentato la proposta per una direttiva del Parlamento europeo e del Consiglio sulla responsabilità per prodotti difettosi (Brussels, 28.9.2022 COM(2022) 495 final 2022/0302 (COD)), nell'ambito di un pacchetto di due proposte di direttive che dovranno essere approvate dal Parlamento europeo e dal Consiglio, finalizzato ad adeguare le norme sulla responsabilità civile all'economia circolare, all'era digitale ed all'impatto delle catene globali del valore, garantendo l'allineamento necessario tra questi due strumenti giuridici necessari. La prima propone la revisione della disciplina dettata dalla direttiva sulla responsabilità per danno da prodotti difettosi, ponendosi gli obiettivi di dare alle imprese la certezza giuridica e la parità di condizioni di cui necessitano per investire in prodotti nuovi ed innovativi e di garantire ai soggetti danneggiati da prodotti difettosi un elevato livello di tutela di cui abbiano bisogno, al fine di incentivare l'impiego di prodotti digitali. La Commissione europea ritiene che la modernizzazione della direttiva europea che, per quasi quarant'anni, ha assicurato la sicurezza legale ai cittadini, fornendo loro gli strumenti per la richiesta di un risarcimento di danni causati da prodotti difettosi, sia necessaria per aggiornare le regole al nuovo contesto di trasformazione verde e digitale, in particolar modo per adattare alle nuove tecnologie, come l'intelligenza artificiale.

coprire l'ampia fenomenologia dei danni da sistemi intelligenti, per una serie di ragioni. In primo luogo, il danneggiato si troverebbe di fronte a difficoltà probatorie nel dimostrare la sussistenza dei presupposti della responsabilità, in riferimento non solo all'elemento oggettivo del nesso di causalità tra l'attività del sistema intelligente e l'evento dannoso, ma soprattutto riguardo all'elemento soggettivo della colpevolezza del danneggiante⁹³.

In aggiunta⁹⁴, la presenza di tecniche sempre più sofisticate, alla quali collaborino distinti attori, rende sempre più complessa l'individuazione dell'autore del danno che, in maniera progressiva, acquisisce quasi un carattere di anonimato, con la conseguenza che potrebbe ricorrere il pericolo dei c.dd. "danni anonimi". Le problematiche connesse all'imputazione della responsabilità, in forza del criterio della colpevolezza, hanno indotto la dottrina a concentrarsi sulla figura del danneggiato e a cercare soluzioni per impedire che le conseguenze negative, derivanti dalle attività delle intelligenze artificiali, siano da questi sopportate. A tale scopo, si è proceduto all'individuazione dei soggetti cui imputare la responsabilità, indipendentemente dall'accertamento della sussistenza di un comportamento colposo, valutando, viceversa, la posizione di "prossimità al rischio" dai medesimi assunta, dalla quale far derivare la possibilità di evitarlo oppure, ad ogni modo, di amministrarlo.

Parte della dottrina ha richiamato le disposizioni disciplinanti le tradizionali ipotesi di responsabilità vicaria, relative al danno cagionato da soggetti diversi dal chiamato a risarcire.

Alcuni autori⁹⁵ hanno fatto riferimento al regime dettato dall'art. 2048 c.c., facendo emergere la responsabilità del programmatore o comunque del soggetto che insegni al sistema di intelligenza artificiale i comportamenti da tenere, equiparandoli alla posizione del precettore, nella sua nozione "astratta" di figura preposta ad istruire gli allievi, ed assimilando il sistema intelligente ad un allievo/apprendista. Secondo tale indirizzo, i primi dovrebbero rispondere dei danni causati dal sistema intelligente, a meno che non provino di non aver potuto impedire il fatto.

La tesi è confutabile, dovendosi escludere il ricorso all'art. 2048 c.c., nonché all'art. 2047 c.c., dato che tali norme sono dirette a regolamentare le responsabilità discendenti dal controllo o dall'educazione di particolari "tipi" di esseri umani, statuendo così una disciplina molto settoriale⁹⁶.

Taluni autori⁹⁷ hanno proposto l'applicazione analogica dell'art. 2049 c.c., delineando la responsabilità dell'imprenditore per i danni provocati da un sistema intelligente che sia stato preposto allo svolgimento di mansioni connesse all'attività imprenditoriale, di norma svolte dai lavoratori. Gli elementi costitutivi della fattispecie sarebbero individuabili in una specie di rapporto di preposizione

⁹³ Cfr. U. SALANITRO, op.cit., p. 1247; A. AMIDEI, op.cit., p. 96; F. NADDEO, op.cit., p. 1151.

⁹⁴ Per le considerazioni che seguono, cfr. D. DI SABATO, op.cit., p. 341.

⁹⁵ Cfr. M. COSTANZA, "Robot e impresa", in U. RUFFOLO (a cura di), "Intelligenza artificiale e responsabilità", Milano, 2017, p. 112 s.; A. SANTOSUOSSO, M. TOMASI, "Diritto, scienza, nuove tecnologie", Padova, 2021, p. 333 e ss.; U. PAGALLO, "The law of robots. Crimes, contracts and torts", New York, 2013, p. 128 s. ritiene che tale regime sia preferibile ad altri di responsabilità extracontrattuale, unitamente all'art. 2050 c.c.

⁹⁶ Così U. RUFFOLO, "Intelligenza artificiale, machine learning e responsabilità da algoritmo", op.cit., p. 1698). In posizione critica si v. anche L. COPPINI, op.cit., p. 726; G. FINOCCHIARO, "Intelligenza artificiale e diritto. Intelligenza artificiale e protezione dei dati personali", in Giur. It., 2019, p. 1657.

⁹⁷ Cfr. M. COSTANZA, "Robot e impresa", op.cit. p. 112 s. Si v. anche G. TEUBNER, op.cit. la cui proposta è formulata sul piano sociologico, oltre che giuridico.

e nel nesso di causalità tra lo svolgimento delle mansioni ed il danno provocato al terzo.

Cionondimeno, si è opportunamente sostenuto che il ricorso all'art. 2049 c.c., seppure stimolante, appare inconciliabile con il nostro ordinamento, perché la sua specialità ne impedisce l'estensione oltre i confini del comportamento umano. La *ratio* della norma consiste nella responsabilizzazione del committente, per una determinata ipotesi di errore dell'intelligenza (umana) del suo commesso e sarebbe complicato interpretare estensivamente la norma in riferimento ai danni causati dal comportamento o dalle decisioni di sistemi non umani, a causa di un difetto della loro intelligenza artificiale⁹⁸.

Si intende, di seguito, incentrare l'attenzione sul richiamo del regime della responsabilità da cose in custodia.

L'interpretazione evolutiva dell'art. 2051 c.c. va condotta in via sistematica, avendo riguardo allo spazio di operatività delle "responsabilità speciali" previste nel codice civile, nonché della regolamentazione della responsabilità da prodotto difettoso.

Si prendano, dunque, le mosse dall'esame dell'applicabilità, in tale contesto, della disciplina della responsabilità per l'esercizio di attività pericolose, di cui all'art. 2050 c.c. Parte della letteratura giuridica ha richiamato tale norma, partendo dalla presunzione che l'impiego dell'intelligenza artificiale rappresenti un'attività pericolosa, per il semplice utilizzo di sistemi intelligenti⁹⁹. Si reputa che, qualora si consenta ad un automa dotato di capacità adattative e di apprendimento di interagire con un uomo, non esista alcuna sicurezza che lo stesso non possa tenere comportamenti lesivi dei diritti dei terzi¹⁰⁰. Il ricorso all'art. 2050 c.c. avrebbe inoltre il pregio di attribuire al soggetto danneggiato una possibile strada alternativa rispetto alla responsabilità per prodotto difettoso, al fine di ottenere il ristoro dei danni subiti¹⁰¹.

Non si condivide tale soluzione, visto che l'intelligenza artificiale non è intrinsecamente pericolosa e non le si addice tale attributo, dal momento che, essendo il simbolo della tecnica, è, per ciò stesso, più affidabile dell'uomo, rappresentando, d'altra parte, un mezzo correttivo o integrativo delle imprecisioni umane¹⁰². Al contrario, potrebbe accadere che la pericolosità non concerna l'attività svolta dai sistemi intelligenti in sé, quanto, piuttosto, le interazioni del sistema con il mondo esterno. Pertanto potrebbe succedere che un'attività produttiva, ritenuta fino ad oggi non pericolosa, lo divenga con l'ingresso dell'intelligenza artificiale nel processo di produzione o direttamente nel prodotto: si pensi, ad esempio, alla circolazione dei veicoli che, potendo assumere

⁹⁸ Cfr. U. RUFFOLO, "Intelligenza Artificiale, *machine learning* e responsabilità da algoritmo", op. cit., p. 1698.

⁹⁹ Cfr. L. COPPINI, op.cit., p. 735 afferma che si potrebbe reputare che sia divenuta pericolosa l'attività di produzione di macchine ad elevata automazione «in funzione dei nuovi pericoli di fallibilità del prodotto» ed applicare l'art. 2050 c.c., imputando la responsabilità allo sviluppatore dell'intelligenza artificiale. Cfr. anche M. SCIALDONE, Il diritto dei robot: la regolamentazione giuridica dei comportamenti non umani, in E. PIETRAFESA, F. MARZANO, T. MEDICI (a cura di), La rete e il fattore C: Cultura, Complessità, Collaborazione, Volume II, Roma, Stati Generali dell'Innovazione, 2016, p. 76; A. SANTOSUOSSO, M. TOMASI, op.cit., pp. 329 ss.

¹⁰⁰ Cfr. C. LAENZA, op.cit., p. 1018 s.

¹⁰¹ Cfr. A. AMIDEI, Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea, in Giur.it., 2019, pp. 1725 ss.

¹⁰² Cfr. M. COSTANZA, L'intelligenza artificiale e gli stilemi della responsabilità civile, op.cit., p. 1688.

connotati di pericolosità, potrebbe essere attratta dalla disciplina dell'art. 2050 c.c.¹⁰³.

Può allora sostenersi che la disciplina della responsabilità da attività pericolose sia invocabile, in via interpretativa, in concorrenza con quella della responsabilità da prodotto difettoso, al fine di imputare la responsabilità per i danni causati da sistemi intelligenti al produttore di un bene che incorpori l'intelligenza artificiale e, qualora non coincida con quest'ultimo, all'autore dell'algoritmo che conferisca al dispositivo la capacità di apprendere¹⁰⁴. Si giunge a tale conclusione, sulla base della premessa che la nostra giurisprudenza continua ad accordare, come concorrente¹⁰⁵, la tutela offerta dal regime di cui all'art. 2050 c.c. anche nelle ipotesi di danno da prodotto difettoso, qualora la sua fabbricazione o la sua distribuzione si riveli qualificabile come attività pericolosa¹⁰⁶.

Facendo riferimento alla responsabilità da cosa in custodia, si puntualizzi che l'art. 2051 c.c. va letto unitamente all'art. 2052 c.c., relativo alla responsabilità per i danni cagionati da animali¹⁰⁷, dato che, in entrambe le norme, il criterio di imputazione sussiste nella custodia con il limite del caso fortuito. Secondo parte della dottrina¹⁰⁸, l'interprete potrebbe imputare la responsabilità da intelligenza artificiale all'utilizzatore o al titolare oppure al custode, richiamando, a sua discrezione, l'art. 2052 oppure l'art. 2051 c.c., a seconda che si configuri il dispositivo intelligente quale un'entità dinamica ed evolutiva come un animale, oppure in una logica naturalistica che sottolinei che lo stesso non è né un animale, né un essere umano, ma rientra viceversa nella categoria delle cose in senso proprio¹⁰⁹.

In realtà, il richiamo all'art. 2052 c.c. va respinto¹¹⁰, considerato che, seppure la norma sia attuabile in astratto, dal momento che il comportamento degli animali è imprevedibile come quello dei dispositivi intelligenti¹¹¹; da un altro punto di vista, mentre, nel primo caso, il proprietario effettua un controllo sulla capacità di reazione dell'animale, per mezzo dell'addomesticamento; diversamente, il

¹⁰³ Cfr. U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, op.cit., p. 1696.

¹⁰⁴ Cfr. U. RUFFOLO, op.ult.cit., p. 1700.

¹⁰⁵ Si ricordi che sia la normativa europea, sia quella nazionale prevedono che alla responsabilità del produttore si cumulano quelle previste da tutte le altre norme.

¹⁰⁶ Il cumulo delle due discipline assumerebbe peculiare connotazione, in relazione all'alta incidenza nel settore dell'intelligenza artificiale del c.d. rischio da sviluppo che, come noto, rappresenta una causa di esclusione della responsabilità per danno da prodotto difettoso. Il rischio da sviluppo, quando sia molto elevato, potrebbe costituire una situazione specifica di attività qualificabile come pericolosa, proprio in quanto diretta a produrlo. Tale circostanza legittimerebbe l'applicazione dell'art. 2050 c.c., soprattutto in settori innovativi e a rapida evoluzione, quale quello dell'intelligenza artificiale, in cui sovente le conoscenze tecniche, relative alla potenziale difettosità di un dispositivo intelligente, sono assenti al momento della sua commercializzazione e sopravvengono successivamente, quando il prodotto è già sul mercato e sono tali da classificarlo come difettoso. Si condividono le argomentazioni di U. RUFFOLO, op.ult.cit., pp. 1684, 1697.

¹⁰⁷ Cfr. U. RUFFOLO, op.ult.cit., p. 1699, parla dell'art. 2052 c.c. come "norma fotocopia" dell'art. 2051 c.c.

¹⁰⁸ Per le osservazioni sull'applicabilità degli artt. 2051 e 2052 c.c. in tale contesto, cfr. L. COPPINI, op.cit., p. 734; A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, op.cit., p. 495; U. RUFFOLO, op.ult.cit., p. 1699; M. SCIALDONE, op.cit., p. 78; GRUPPO DI ESPERTI MISE, *Proposte per una strategia italiana per l'intelligenza artificiale*, cit., p. 50; M. RATTI, *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, in *Contr.impr.*, 2020, pp. 1174 ss.

¹⁰⁹ Cfr. L. FORT, V. LEVA, *Intelligenza artificiale, responsabilità civile e interpretazione analogica*, in *www.biodiritto.org*, 2020, 8, p. 2.

¹¹⁰ Cfr. F. NADDEO, op.cit., p. 1158; M. SCIALDONE, op.cit., p. 79. Contra A. BERTOLINI, *Robots as Products*, op. cit., p. 227 fa leva sulla differenza tra animale e dispositivo intelligente.

¹¹¹ Cfr. M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 333 ss.

titolare/utilizzatore/custode di tali dispositivi, oltre a non conoscerne, di base, i meccanismi di funzionamento e di reazione al mondo esterno, ha una limitata possibilità di incidere sui loro comportamenti e sulle loro decisioni¹¹².

L'invocazione del regime della responsabilità da cose in custodia ha costituito oggetto di svariate critiche.

Si è affermato che l'articolo 2051 c.c. fa riferimento, in sostanza, ad una *res* «inanimata» e che rappresenterebbe, perciò, un'entità lontana dai dispositivi intelligenti che sono capaci di comportamenti e decisioni, senza la supervisione umana¹¹³. Si è anche sostenuto¹¹⁴ che il parametro della custodia potrebbe risultare inidoneo, in considerazione della circostanza che la custodia di un dispositivo intelligente, soprattutto se autonomo, sarebbe eccessivamente complessa e squilibrata per il custode che potrebbe non essere in grado di controllarlo. Ancora, qualora il titolare/utilizzatore/custode fosse citato in giudizio, la prova dell'esimente del caso fortuito, concernente l'imprevedibilità della decisione o del comportamento del dispositivo, potrebbe divenire insormontabile¹¹⁵.

Pur tuttavia, si crede che l'art. 2051 c.c., nella sua accezione di responsabilità oggettiva, sia applicabile quando il dispositivo intelligente non costituisca un mezzo di causazione del pregiudizio, per mezzo di un'autonoma azione del titolare/utilizzatore/custode, quanto, viceversa, fonte stessa del danno. Il richiamo della norma al caso in esame sarebbe, difatti, ragionevole, perchè il dispositivo intelligente ha una natura evolutiva ed autonoma, caratteristica che lo distingue dagli esseri inanimati ed il danno sarebbe, in realtà, insito nel dinamismo intrinseco della "cosa intelligente"¹¹⁶.

In aggiunta, l'art. 2051 c.c. sarebbe complementare all'art. 2050 c.c., pur dovendosi ribadire che il regime della responsabilità della cosa in custodia ha il pregio di prescindere dalla prova della pericolosità o della difettosità del bene in custodia¹¹⁷.

Deve, in ogni modo, sottolinearsi che l'imputabilità della responsabilità in capo all'utilizzatore, al titolare o al custode del dispositivo digitale dipenderà dalla qualificabilità della relazione tra costoro e lo stesso come rapporto di "custodia", ossia dalla sussistenza o meno del "potere di governo" che tali soggetti esercitino sulla "cosa"¹¹⁸, e dalla sussistenza o dalla perdita della possibilità di controllarne le condizioni di rischio¹¹⁹. L'art. 2051 c.c. non sarà applicabile quando il

¹¹² Cfr. A. LIOR, *AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy*, in *Mitchell Hamline Law Review*, 2020, 46, 5, 2, pp. 1060-1062.

¹¹³ Cfr. M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità*, op.cit., p. 1687; G. SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Dir.Inf. Informatica*, 2003, pp. 55 ss.

¹¹⁴ Cfr. L. FORT, V. IEVA, op.cit., p. 3.

¹¹⁵ Cfr. L. FORT, V. IEVA, op.cit., p. 15 che rimarcano che quanto detto inciderebbe sulle scelte economiche dei consumatori che, in qualità di utilizzatori finali, sarebbero disincentivati ad acquistare i prodotti suddetti.

¹¹⁶ Cfr. M. RATTI, op.cit., pp. 1174 ss.

¹¹⁷ Cfr. A. SANTOSUOSSO, M. TOMASI, op.cit., p. 329. Secondo A. PROCIDA MIRABELLI DI LAURO, *Intelligenze artificiali e responsabilità civile*, in A. PROCIDA MIRABELLI DI LAURO, M. FEOLA (a cura di), *Diritto delle obbligazioni*, Napoli, 2020, p. 520, vi sarebbe la possibilità, da parte del danneggiato, di proporre il "concorso" tra gli artt. 2050 e 2051 c.c. che lascerebbe al giudice la possibilità di qualificare la fattispecie, ai sensi dell'una o dell'altra norma, avendo riguardo al caso concreto.

¹¹⁸ Si v. supra § 1, nota 5.

¹¹⁹ Per le argomentazioni che seguono, relative all'imputazione della responsabilità ex art. 2051 c.c., cfr. U. SALANITRO, op.cit., pp. 1257 ss. che richiama G. WAGNER, *Robot liability*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019, pp. 49 ss.

dispositivo rappresenti un sistema chiuso, nel quale il produttore dell'*hardware* non permetta l'impiego di *software* di aziende che non siano specificamente autorizzate; d'acché, in tale ipotesi, il titolare/utilizzatore/custode non ha alcun controllo sulle condizioni di rischio del dispositivo. Ne discende che, nel sistema chiuso, l'eventuale alleggerimento di responsabilità di tali soggetti potrebbe essere compensata dall'aggravamento, in termini di responsabilità, della posizione del produttore del dispositivo, perché si tratta del soggetto idoneo, in maggior misura, a minimizzare il rischio: costui è, infatti, in grado di controllarlo integralmente e di gestirlo, anche per mezzo di strumenti assicurativi oppure traslando sul prezzo del bene il costo del rischio. La disciplina della responsabilità da cosa in custodia sarà, viceversa, applicabile, quando ci si trovi di fronte ad un sistema aperto, nel quale l'utilizzatore, il custode o il titolare del prodotto eserciteranno un certo grado di controllo e potranno modificare le condizioni di rischio, accedendo a servizi o prodotti *software* che siano offerti da altri imprenditori¹²⁰.

Si reputa che il regime della responsabilità da cosa in custodia possa essere anche richiamato, ai fini dell'imputazione della responsabilità in capo a chi "addestri" un'entità artificiale intelligente o la esponga, in ogni caso, ad "esperienze", idonee ad istruirla ovvero ad indirizzarla, quantomeno in via concorrente con la responsabilità del produttore del dispositivo digitale e/o con quella dell'ideatore dell'algoritmo, se distinto da quest'ultimo¹²¹. L'insorgere della responsabilità, ai sensi dell'art. 2051 c.c., deriverebbe dalla circostanza che tale soggetto utilizza o gestisce la "cosa" munita di intelligenza artificiale *self-learning*, indirizzandola verso una *mentalità*, capace di sconfinare in comportamenti malevoli o devianti, senza, tuttavia, prevedere meccanismi inibitori. L'addestratore sarebbe responsabile dei danni provocati "dalla cosa" intelligente, giacché i comportamenti della stessa, seppure non indirizzati da tale soggetto, sarebbero sicuramente il frutto e la conseguenza del suo insegnamento o dell'apertura del dispositivo ad esperienze da questi condotte. Secondo tale impostazione, l'addestratore sarebbe chiamato a rispondere anche per i danni derivanti da un imprevedibile mutamento di atteggiamento del dispositivo intelligente, visto che da quest'ultimo "custodito". All'"addestratore" potrebbe, inoltre, applicarsi l'art. 2050 c.c., qualora ne ricorrano i presupposti.

In via conclusiva, si rimarchi che l'art. 2051 c.c. è stato richiamato dalla dottrina anche per i danni provocati dai veicoli autonomi¹²²: si pensi al caso in cui, a causa di un difetto della tecnologia di riconoscimento degli oggetti, un'auto a guida autonoma possa identificare in maniera erranea un oggetto sulla strada e provocare un incidente, cagionando lesioni e danni materiali. Al riguardo, bisogna differenziare tra l'ipotesi in cui il veicolo circoli sotto il controllo del conducente ed il caso in cui, sebbene vi sia un conducente alla guida, il dispositivo gli si

¹²⁰ Cfr. U. SALANITRO, op.cit., p. 1258.

¹²¹ Si condivide la ricostruzione di U. RUFFOLO, op.ult.cit., pp. 1698, 1700.

¹²² Tra i contributi sul tema, cfr., ex multis, M.C. GAETA, Liability rules and self-driving cars. The evolution of tort law in the light of new technologies, Napoli, 2019 passim; F.P. PATTI, The European Road to Autonomous Vehicles, 43 FORDHAM INT'L L.J. 125 (2019), pp. 125 ss.; A. ALBANESE, La responsabilità civile per i danni da circolazione di veicoli ad elevata automazione, in Europa dir.priv., 2019, pp. 995 ss.; L. GATT, I. CAGGIANO, M.C. GAETA, Italian Tort Law and Self-Driving Cars: State of art and Open Issues, in B.H. OPPERMAN, J. STENDER-VORWACHS (a cura di), Autonomes Fahren. Technische Grundlagen, Rechtsprobleme, Rechtsfolgen, München, 2020, pp. 239 ss.; A. LEPORE, I.A. e responsabilità civile. Robot, autoveicoli e obblighi di protezione, in Tecnologie e diritto, 2021, pp. 2724 ss.

sostituisca in tutto o in parte, compiendo mansioni più o meno importanti, a seconda delle quali la responsabilità di tale soggetto potrebbe essere esclusa o limitata¹²³. Nel primo caso, qualora si verificano danni, si può configurare la responsabilità del conducente, ai sensi dell'art. 2054 c.c. Nel secondo caso, qualora si decida di non applicare l'art. 2054 c.c. all'automazione intelligente, si potrebbe richiamare l'art. 2051 c.c., dal quale far derivare, in ragione della relazione fattuale di custodia del veicolo, l'imputazione della responsabilità al proprietario guidatore ovvero al proprietario ed al guidatore.

In concorso con la responsabilità del proprietario e del conducente, si potrebbe raffigurare la responsabilità del produttore, ovvero dell'ideatore dell'algoritmo, se distinto da quest'ultimo, a norma sia della disciplina della responsabilità da prodotto difettoso, sia di quella della responsabilità da attività pericolose, qualora si ritenga che l'attività di produzione di macchine a elevata automazione sia divenuta pericolosa, a causa dei corrispondenti nuovi pericoli di fallibilità del prodotto¹²⁴.

Conclusioni.

In via conclusiva, se, per un verso, l'applicazione della disciplina della responsabilità aquiliana ai nuovi scenari dannosi solleva rilevanti difficoltà dal punto di vista probatorio, rendendo particolarmente gravosa la posizione processuale del soggetto danneggiato; per altro verso, si reputa senza dubbio condivisibile l'indirizzo interpretativo che, al fine di risolvere le problematiche connesse all'imputazione della responsabilità dei soggetti coinvolti nel "ciclo di vita" dei sistemi di intelligenza artificiale, invoca l'applicabilità di taluni regimi di responsabilità oggettiva, riconducibili ai modelli tradizionali di responsabilità civile.

Più precisamente, risultano idonee a garantire efficaci strumenti di tutela per i soggetti che subiscano danni provocati da sistemi di intelligenza artificiale sia la disciplina della responsabilità da attività pericolose, sia precipuamente la disciplina della responsabilità da cosa in custodia, oltre che la disciplina della circolazione dei veicoli.

La responsabilità civile, ex art. 2050 c.c., potrà essere imputata, in concorrenza con quella della responsabilità da prodotto difettoso, al produttore del bene che incorpori l'intelligenza artificiale e all'ideatore dell'algoritmo, qualora con coincida con costui, solamente quando le interazioni dei sistemi intelligenti rendano pericolosa l'attività dagli stessi svolta; nonché all'addestratore dell'algoritmo, quando ne ricorrano i presupposti.

La disciplina della responsabilità da cose in custodia sarà applicabile, ai fini dell'imputazione della responsabilità, in capo al titolare/utilizzatore/custode, unicamente quando il dispositivo rappresenti un "sistema aperto", nonché in capo

¹²³ Cfr. L. COPPINI, op.cit., p. 734. Si v. anche U. RUFFOLO, *Intelligenza artificiale e automotive: le responsabilità da veicoli self driving e driverless*, ID. (a cura di), *Intelligenza artificiale*, op.cit., pp. 153 ss.

¹²⁴ Cfr. L. COPPINI, op.cit., p. 735; analogamente A. BERTOLINI, *Robots as Products*, op.cit., pp. 227 ss. Per l'applicazione della responsabilità da prodotto ai veicoli autonomi, cfr. C. BOSCARATO, *Robotics, Innovation and Law*, in A. SANTOSUOSSO (a cura di), *The challenge of Innovation in Law*, Pavia, 2015, p. 230. Sulla potenziale pericolosità dell'attività, in tale ambito, cfr. U. RUFFOLO, E. AL MUREDEN, *Autonomous vehicles e responsabilità nel nostro sistema e in quello statunitense*, in *Giur.it.*, 2019, pp. 1704 ss., p. 1711.

all' "addestratore" di un'entità artificiale intelligente, quantomeno in via concorrente con la responsabilità del produttore del dispositivo digitale e/o con quella dell'ideatore dell'algoritmo, se distinto da quest'ultimo.

Come specificato, tale disciplina è complementare a quella della responsabilità da attività pericolose.

Si rammenti infine che, in riferimento ai danni provocati dai veicoli autonomi, la responsabilità civile sarà imputabile in capo al proprietario e/o al conducente, applicando o l'art. 2051 c.c. oppure l'art. 2054 c.c., a seconda delle circostanze, potendo concorrere con la responsabilità di tali soggetti altresì la responsabilità del produttore, dell'ideatore dell'algoritmo, nonché dell'"addestratore", in forza delle disposizioni normative *supra* richiamate.



Beyond Bitcoin: Understanding Legal Boundaries of Blockchain Technology

ALESSIO DI AMATO

Full Professor of Business Law at University of Salerno

VINCENZO ORSINI

Postdoctoral Researcher of Business Law at University of Salerno

Abstract

The current legal uncertainty surrounding blockchain technology can discourage innovators from implementing new blockchain applications. Consequently, it can limit the development of the technology and, ultimately, hinder the growth of this new market. Therefore, this article aims to highlight and address, from a practical standpoint, the prominent legal challenges faced by innovators. The main technical components and applications of blockchain technology – such as crypto-assets, distributed ledgers, and smart contracts – are used as reference points for the analysis. First, the article classifies crypto-assets and specifies (1) when they fall within the scope of banking and finance regulation; and (2) when they fall within the scope of the MiCa Regulation proposal (also describing its principles and functioning). Secondly, it investigates the evidential value of distributed ledgers, assesses how they could be exploited in private law matters, and examines the recent proposal of amendment to the eIDAS Regulation. Lastly, it clarifies under which conditions a smart contract can be legally binding and the practical consequences.



Keywords: blockchain law, crypto-assets; MiCa Regulation; distributed ledgers; eIDAS; smart contracts.

Summary: [Introduction.](#) – [1. Brief Notes on Regulated Crypto-assets.](#) – [2. The MiCA Regulation Proposal.](#) – [3. The Evidential Value of Distributed Ledgers.](#) – [4. Giving Smart Contracts a Legal Framework.](#)

Introduction.¹

Scholars started investigating bitcoin, blockchain and related technologies in 2014, no later than five years after the launch of the bitcoin protocol.² Ever since then, the literature in the field has rapidly increased due to the capability of blockchain technology of ensuring security and transparency in no-trust environments. Even though the general public focused mainly on cryptocurrencies, computer scientists, entrepreneurs, and academics, realized that blockchain technology could have had many more applications. The base assumption is that, at its core, blockchain is ‘a specific type of database that uses certain cryptographic functions to achieve the requirements of data integrity and identity authentication’.³ Therefore, blockchain technology shall primarily be intended as a technical tool to ensure the reliability of the information contained in a database, a tool that could have multiple applications in several industries other than banking and finance.⁴

While traditional centralised databases for registering and transferring assets tend to be expensive and inflexible – since they need to be controlled or supervised – the blockchain could significantly reduce infrastructure costs by adopting a ledger distributed among a peer-to-peer network. However, blockchain technology in its purest form (e.g., bitcoin) ignores external legal requirements, and shall be integrated with new features to become compliant with the law.⁵ Moreover, the legal system itself is not prepared for a paradigm shift from centralised to distributed systems.⁶ Hence, developers and organizations

¹ This paper is the result of the joint work of Prof. Alessio Di Amato and Dr. Vincenzo Orsini, that defined together its aim, structure, and content. The drafting effort, however, was divided between Prof. Di Amato, that wrote the introduction, and Dr. Orsini, that wrote the following paragraphs.

² For a systematic review of blockchain research in the business literature, see J Frizzo-Barker and others, 'Blockchain As A Disruptive Technology For Business: A Systematic Review' (2020) 51 International Journal of Information Management, 2.

³ J Bacon and others, 'Blockchain Demystified: A Technical And Legal Introduction To Distributed And Centralised Ledgers' [2018] Richmond Journal of Law & Technology, 5-6.

⁴ UK Government Chief Scientific Adviser, 'Distributed Ledger Technology: Beyond Block chain' (2016), 4.

⁵ C Reed and others, 'Beyond Bitcoin—Legal Impurities And Off-Chain Assets' (2018) 26 International Journal of Law and Information Technology, 160-162.

⁶ The decentralised nature of blockchain technology makes it difficult not only to apply the existing regulation, but also to understand how the blockchain can be regulated in an effective way. See, G P La Sala, 'Intermediazione, Disintermediazione, Nuova Intermediazione: I Problemi Regolatori', *Diritto del Fintech* (CEDAM 2020), 7-8. Nonetheless, authors generally believe that the blockchain will follow the same regulatory curse of the Internet since also the latter was difficult to regulate at the beginning. Meanwhile, it seems that the blockchain is governed by the private and technical set of rules generated by smart contracts and decentralized organization, that seems to constitute a new 'lex cryptographia'.

See, A Wright and P De Filippi, 'Decentralized Blockchain Technology And The Rise Of Lex Cryptographia' [2015] SSRN Electronic Journal, 51-56; P Hacker and others, *Regulating Blockchain: Techno-Social And Legal Challenges* (Oxford University Press 2019), 16-19; K Becker, 'Blockchain Matters—Lex Cryptographia And The Displacement Of Legal Symbolics And Imaginaries' (2022) 33 Law and Critique, 118-122.

could find it extremely difficult and expensive to comply with legal and regulatory requirements. Here stands the main obstacle for innovators: those willing to embrace blockchain technology and implement new solutions for their businesses may have hard times understanding the legal boundaries and, ultimately, may disregard the idea completely.

Thus, this article aims to provide a framework for better understanding those legal and regulatory requirements and navigate the legal system. The analysis will be structured using the main technical components and applications of blockchain technology (such as tokens, distributed ledgers, and smart contracts), as reference points. First, the article will classify crypto-assets, clarify when they fall within the scope of banking and finance regulation and try to specify if other laws could find application. Secondly, it will investigate the evidential value of the distributed ledger for registering and transferring assets and highlight the current obstacles to the adoption of blockchain for assets that exist outside the blockchain itself (off-chain assets). Lastly, it will analyse the legal value of smart contracts and their interaction with traditional contracts. Considering that smart contracts are, essentially, computer programs that run on a blockchain, it is necessary to define under which conditions they can be legally binding and how can they be enforced.

1. Brief Notes on Regulated Crypto-assets.

Blockchain technology allows to create, in a digital environment, rival goods (i.e., goods that may only be possessed by a single user at a time).⁷ Those goods are named crypto-assets and, in their purest form, are nothing more than 'a chain of digital signatures' and were meant to be used as a payment system.⁸ Notwithstanding, tokens are not all the same, being primarily the developer that defines function and features of a token or a set of tokens. The market is continuously evolving and counts a wide variety of applications and cases.⁹ In fact, since the introduction of the bitcoin protocol, many types of crypto-assets have been developed, ranging from stable coins, that are crypto-assets whose value refers to fiat currencies or other assets, to non-fungible tokens (NFTs), that are being used to commodify digital assets, like images or even tweets.¹⁰

⁷ Most goods in economics are rival because they cannot be used by different people at the same time (e.g., a hammer), whereas data (e.g., a digital image) can normally be used by any number of people simultaneously, without being diminished. This is the reason why, before the emergence of blockchain technology, digital goods were considered necessarily non-rival goods. See, C I Jones and C Tonetti, 'Nonrivalry And The Economics Of Data' (2020) 110 American Economic Review, 2819-2820.

⁸ The purpose of the bitcoin protocol emerges from the title of the white paper itself, that suggests the idea of a new electronic payment system. See, S Nakamoto, 'Bitcoin: A Peer-To-Peer Electronic Cash System' (2009) <<https://bitcoin.org/bitcoin.pdf>> accessed 1 July 2018, 2.

⁹ For a taxonomic deconstruction of blockchain-based technologies, see P Tasca and C J Tessone, 'A Taxonomy Of Blockchain Technologies: Principles Of Identification And Classification' (2019) 4 Ledger, 8.

¹⁰ A non-fungible token is a crypto-asset that represents an intangible and unique digital item like a particular piece of digital art, music, video, etc. Differently from other crypto-assets, that are standardized, NFTs are unique and not fungible. The market for NFTs recently boomed [The EU Blockchain Observatory & Forum, 'Demystifying Non-Fungible Tokens' (2021) 13] raising several questions among legal scholars. See, G Frezza, *Arte E Diritto Fra Autenticazione E Accertamento* (Edizioni scientifiche italiane 2019); T M Evans, 'Cryptokitties, Cryptography, and Copyright' (2019) 47 AIPLA Q J, 219; I E Okonkwo, 'NFT, Copyright And Intellectual Property Commercialization' (2021) 29 International Journal of Law and Information Technology; A Guadamuz, 'The Treachery Of Images: Non-Fungible Tokens And Copyright' (2021) 16 Journal of

Because of the variety of crypto-assets, there may be a lack of clarity as to the legal and regulatory framework that finds application in each different case. On one hand, 'there is not a "one size fits all" solution when it comes to legal qualification'.¹¹ Depending on function and features of a certain crypto-asset, its legal qualification may be different and, consequently, the applicable legal regime. On the other hand, many crypto-assets are still unregulated in the EU. Even though some Member States developed bespoke laws for crypto-assets, and the EU is currently working on a legal framework in the areas of tokenisation and smart contracts, the only European law that applies transversally to any kind of token is the fifth anti-money laundering Directive (hereinafter, AMLD5).¹² It is possible, nevertheless, to identify certain types of crypto-assets that are, already at this stage, regulated; and to try to anticipate the outlines of the European legal framework on crypto-assets.

Preliminarily, it is important to highlight is that the terms 'token', 'cryptocurrency', 'virtual currency' and 'crypto-asset' are often used improperly as synonyms. The word 'token' has mainly a technical meaning and does not have any legal connotation. It can be used to describe the entire family of technical instruments issuable via the blockchain (cryptocurrencies, for instance, are only a species of tokens).¹³ Conversely, virtual currencies have been explicitly defined by the fifth anti-money laundering Directive as a 'digital representation of value [...] which can be transferred, stored and traded electronically' [art. 3(18)] – a broader definition that disregard completely the adoption of blockchain technology. In other words, virtual currencies are not necessarily issued in the technical form of tokens, and the notion does not encompass every type of token. For this reason, here it will be preferred the term 'crypto-asset', a term that has been recently adopted in the EU Regulation proposal on Markets in Crypto-assets (hereinafter, MiCa) to identify any type of token, issued using blockchain technology, that is representative of value or rights [art. 3(1)(2)].

Moreover, it is worth mentioning that while some blockchains, like bitcoin, are constituted solely of crypto-assets that have been mined (i.e., produced validating transactions), some others offer part of them for sale. In the first case, every crypto-asset is previously produced via mining and, only after, sold on a secondary market such as an exchange platform. In the latter case, the developers of a blockchain presale some crypto-assets to promote their network and fund their project:¹⁴ this procedure is called Initial Coin Offering, or ICO.¹⁵ A

Intellectual Property Law & Practice; J A T Fairfield, 'Tokenized: The Law Of Non-Fungible Tokens And Unique Digital Property,' (2022) 97 Indiana Law Journal; S Hecker and M Vanzetti, 'L'«Originale» Nell'arte Come Concetto Mutevole Nel Tempo E Nell'ambito Della Sua Attuale Tutela' [2022] Arte e Diritto; C Trevisi, R M Visconti and A Cesaretti, 'Non-Fungible Tokens (NFT): Business Models, Legal Aspects, And Market Valuation' [2022] Media Laws.

¹¹ ESMA, 'Advice On Initial Coin Offerings And Crypto-Assets' (2019), 4.

¹² European Union Directive 2018/843/EU of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43.

¹³ 'Crypto Basics' (Coinbase, 2022) <<https://www.coinbase.com/it/learn/crypto-basics/what-is-a-token>> accessed 5 September 2022.

¹⁴ In other words, the developer of a project issue tokens that offers in exchange for other cryptocurrencies like BTC or ETH. For an outline of ICOs, see: European Parliamentary Research Service, 'Understanding Initial Coin Offerings. A New Means Of Raising Funds Based On Blockchain' (2021).

¹⁵ The legal challenges of ICOs have been addressed by many authors. Among others, see: I M Barsan, 'Legal Challenges Of Initial Coin Offerings (ICO)' (2017) 3 Revue Trimestrielle de Droit Financier; J Enyi and

programmer, for instance, could decide to finance the development of a software project by offering for sale some of the coins that, in the future, he will accept as payment. In this way, he will be able to directly profit from the issuance of crypto-assets and employ those resources in the project.

The sharp rise of ICOs imposed financial supervisory authorities from all around the globe to clarify if, and when, securities laws find application. The first investigation in the matter dates back to 2017, when the U.S. Securities and Exchange Commission (hereinafter, SEC) published its report about the Decentralized Autonomous Organization, or DAO, which represents a cornerstone in the brief ICO history.¹⁶ The SEC stated, for the first time, that certain crypto-assets can fall within the scope of US securities laws and regulations if they pass the 'Howey test', thereby qualifying as 'investment contracts'.¹⁷ In order to pass the test, a crypto-asset should represent '[1] an investment of money in a common enterprise [2] with a reasonable expectation of profits [3] to be derived from the entrepreneurial or managerial efforts of others'.¹⁸ As a consequence, those who offer and sell 'security-like' crypto-assets must comply with the laws regarding public offerings, and those who engage in the activities of an exchange must register as national securities exchanges.¹⁹

Since the test should be undertaken on a case-by-case basis, its correct interpretation become crucial for understanding the nature of any crypto-asset. Consequently, the SEC decided to release a public statement containing a 'Framework for "Investment Contract" Analysis of Digital Assets' in which it

Y Le Ngoc Dang, 'Regulating Initial Coin Offerings ("Cryptocrowdfunding")' [2017] *Butterworths Journal of International Banking and Financial Law*; P Hacker and C Thomale, 'Crypto-Securities Regulation: Icos, Token Sales And Cryptocurrencies Under EU Financial Law' (2018) 15 *European Company and Financial Law Review*; D Boreiko, G Ferrarini and P Giudici, 'Blockchain Startups And Prospectus Regulation' (2019) 20 *European Business Organization Law Review*; D A Zetzsche and others, 'The ICO Gold Rush: It's A Scam, It's A Bubble, It's A Super Challenge For Regulators' (2019) 60 *Harvard International Law Journal*; F Annunziata, 'Speak, If You Can: What Are You? An Alternative Approach To The Qualification Of Tokens And Initial Coin Offerings' (2020) 17 *European Company and Financial Law Review*; P Maume, 'Initial Coin Offerings And EU Prospectus Disclosure' (2020) 31 *European Business Law Review*.

¹⁶ In brief, the DAO was meant to be a virtual investment fund executed on a blockchain. To raise funds among investors, its promoters sold "DAO Tokens", crypto-assets that would have granted voting power in the DAO and given access to future earnings. Unfortunately, before the DAO could start operating, a hacker used a flaw in the DAO software to steal part of the funds previously raised (valued approximately \$150 millions) and led the SEC to start an investigation to determine why so many people were allowed to invest in something that so closely resembled a company. Since Ethereum was forced to restore DAO investors, the SEC decided not to prosecute the promoters of the DAO - Securities Exchange Commission, 'Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO', Release n. 81207 of 25th July 2017.

¹⁷ *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

¹⁸ *Ibid.*

¹⁹ Cryptocurrency laws and regulations, at this stage, vary state by state. Some state governments have adopted a favourable approach to crypto-related activities, exempting crypto-assets from state securities laws or banking laws, while others adopted a more restrictive approach, requiring some sort of authorization (e.g., 'BitLicense' in New York). For an overview, see: 'Cryptocurrency Laws And Regulations By State' (*Bloomberg law*, 2022) <<https://pro.bloomberglaw.com/brief/cryptocurrency-laws-and-regulations-by-state/>> accessed 29 June 2022. At the Federal level, up until now, initiatives have been relegated to administrative levels (SEC, CFTC, IRS, OCC, FinCen). Different bills, however, have been proposed but still have not passed: (i) the 'Token Taxonomy Act', that specifies that digital tokens, such as those used in virtual currencies, are not securities for regulatory purposes and provides for the tax treatment of virtual currencies; (ii) the 'Consumer Safety Technology Act', which requires various agencies to explore the use of emerging technologies in the context of consumer products and safety; and lately (iii) the 'Lummis-Gillibrand Responsible Financial Innovation Act', whose ambitious aim is to define guidelines for the crypto-assets space, providing also a taxonomy and specific rules for stable-coins.

explained the elements of the test.²⁰ It specified, first, that the definition of ‘money invested’ is broad and includes any type of consideration (including cryptocurrencies); secondly, that both dividends, periodic payments and capital gains can be considered as ‘profit’; and thirdly, that the ‘reliance on the effort of others’ should be assessed through an objective inquiry. This inquiry should focus on the ‘reasonableness’ of the expectation of the investor, and on the ‘essentiality’ of the managerial effort of promoters, sponsors or third parties (to be essential, it should affect the success or failure of the initiative). Ultimately, the SEC clarified that ‘price appreciation resulting solely from external market forces (such as general inflationary trends or the economy) impacting the supply and demand for an underlying asset generally is not considered “profit” under the Howey test’.

In the meantime, the European Securities and Markets Authority (ESMA) warned that ‘where the coins or tokens qualify as financial instruments it is likely that the firms involved in ICOs conduct regulated investment activities’.²¹ Besides, it highlighted that it is duty of the firms to consider if some EU rules – such as the Prospectus Directive²², the Markets in Financial Instruments Directive II (hereinafter, MiFID II)²³, the Alternative Investment Fund Managers Directive (AIFMD)²⁴, or the Fourth Anti-Money Laundering Directive (AMLD4)²⁵ – may apply. Nonetheless, it did not clarify when a crypto asset qualifies as a security under the EU law.

The issue was faced more recently by the ESMA when it released an ‘Advice on Initial Coin Offerings and Crypto-Assets’.²⁶ There, it confirmed the applicability of the EU financial rules to crypto-assets that qualify as ‘transferable securities’ or other types of MiFID financial instruments. As known, the EU law does not provide a distinctive definition of ‘financial instrument’ but, instead, lists those who fall into the category at Section C of Annex I of the MiFID II: ‘transferable securities’, ‘money market instruments’, ‘units in collective investment undertakings’, and several derivative instruments. Consequently, those who are involved in ICOs should pay close attention to the list and, particularly, to the interpretation of ‘transferable securities’.²⁷

²⁰ Securities and Exchange Commission, ‘Framework For “Investment Contract” Analysis’ (2019).

²¹ The Supervisory Authority issued two different warnings: one on the risks of ICOs for investors and another one on the rules applicable to firms involved in ICOs - European Securities and Markets Authority, ‘Esma Highlights ICO Risks For Investors And Firms’ (2017) <<https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms>> accessed 8 June 2022.

²² European Council Directive 2003/71/EC of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC [2002] OJ L 345/64.

²³ European Union Directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L 173/349.

²⁴ European Union Directive 2011/61/EU of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 [2011] OJ L 174/1.

²⁵ European Union Directive 2015/849/EU of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L 141/73.

²⁶ ESMA, ‘Advice On Initial Coin Offerings’ (11).

²⁷ The qualification of crypto-assets as transferable securities is a highly debated topic. See, I M Barsan, ‘Legal Challenges’ (15); P Hacker and C Thomale, ‘Crypto-Securities Regulation’ (15); D Boreiko, G Ferrarini and P Giudici, ‘Blockchain Startups’ (15); F Annunziata, ‘Speak, If You Can’ (15); P Carrière, ‘Le “Criptoalute” Sotto La Luce Delle Nostrane Categorie Giuridiche Di “Strumenti Finanziari”, “Valori Mobiliari”

As noted by some authors, the definition of ‘transferable security’ given by Article 4(1)(44) of MiFID II follows formal and substantive criteria.²⁸ Formally, it includes ‘those classes of securities which are negotiable on the capital market’. Hence, it requires the crypto asset to be standardized, transferable and negotiable. Substantially, it exemplifies transferable securities with traditional assets such as shares, bonds, and some derivatives. Thus, even though some authors disagree²⁹, it is commonly accepted that crypto-assets should resemble the examples provided by the law in order to be considered as transferable securities. However, it is worth noticing that a survey among financial supervisory authorities revealed that the actual classification of crypto-assets as transferable securities can differ among Member States because of the different implementation of the EU law at national level.³⁰

What is clear is that, depending on how they are structured, crypto-assets may fall outside of the scope of the existing rules and hence outside of the regulated space. Crypto-assets that do not qualify as financial instruments, at this stage, are only partially regulated in the EU. Although some Member States, such as Malta and France, established bespoke regimes both for issuers and third-party service providers (e.g., exchanges or custodians), the EU law only focuses on anti-money laundering measures.³¹ In fact, the AMLD5 brings exchange platforms and wallet providers under the control of the national competent authorities and imposes on them Customer Due Diligence obligations.³² They must, therefore, identify customers and monitor their business relationships in order to report any suspicious activity so that competent authorities can intervene.

For this reason, many started to classify crypto-assets in such a way as to

E “Prodotti Finanziari”; Tra Tradizione E Innovazione’ [2019] Rivista di Diritto Bancario; K Langenbucher, ‘Building A Capital Market – The Final Report Of The High Level Forum On The EU Capital Market Union’ (2020) 17 European Company and Financial Law Review; A Minto, ‘The Legal Characterization Of Crypto-Exchange Platforms’ (2021) 22 Global Jurist. Some authors argue that cryptocurrencies should be considered as money or intangible goods: C Pernice, *Digital Currency E Obbligazioni Pecuniarie* (Edizioni scientifiche italiane 2018); T de Graaf, ‘The Qualification Of Bitcoins As Documentary Intangibles’ (2019) 27 European Review of Private Law; M Cian, ‘La Criptoaluta Alle Radici Dell’Idea Giuridica Di Denaro Attraverso La Tecnologia: Spunti Preliminari’ (2019) 72 Banca borsa tit. cred.; V Orsini, ‘Della Natura Giuridica Delle Criptoalute’ [2021] Diritto del mercato assicurativo e finanziario.

²⁸ P Hacker and C Thomale, ‘Crypto-Securities Regulation’ (15), 645-696.

²⁹ D Boreiko, G Ferrarini and P Giudici, ‘Blockchain Startups’ (15), 678-680.

³⁰ ESMA, ‘Advice On Initial Coin Offerings’ (11).

³¹ Outside the EU, Liechtenstein has also adopted a bespoke regime for crypto-assets (the Token and Trusted Technology Service Provider Act).

³² The early intervention in the anti-money laundering space was determined by a case that gained the attention of the Financial Action Task Force (FATF): on Tuesday 1st October 2013, the US authorities closed ‘Silk Road’, the most famous online black-market in the world. It sold any kind of illegal goods, such as drugs and weapons, and was famous for being completely anonymous. Silk Road was situated in the dark web and guaranteed non-traceability of the users by allowing payments only via Bitcoin. For the full story, see: J Bearman, ‘The Rise And Fall Of Silk Road, Part I’ [April 2015] Wired <<https://www.wired.com/2015/04/silk-road-1/>> and, ‘The Rise And Fall Of Silk Road, Part II’ [May 2015] Wired <<https://www.wired.com/2015/05/silk-road-2/>> both accessed 28 June 2022. The event alerted the FATF that, in 2014, published a report where it warned of the risk posed by virtual currencies and, in 2015, published its guidance for a risk-based approach to virtual currencies: Financial Action Task Force, ‘Guidance For A Risk-Based Approach to Virtual Currencies’ (FATF 2015) <<http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>> accessed 28 June 2022. The EU took action immediately afterwards, starting the process that led to the AMLD5: EU Commission, ‘Communication COM (2016) 50 to the Council and the Parliament on an Action Plan to further step up the fight against the financing of terrorism’ (2 February 2016).

distinguish ‘security like tokens’ from ‘currency like tokens’ (like Bitcoin).³³ Nonetheless, the most adopted classification³⁴ is probably the one developed by FINMA, the Swiss financial market supervisory authority.³⁵ It identified three categories of crypto-assets by economic function: cryptocurrencies, security tokens and utility tokens. Cryptocurrencies are tokens that ‘have no further functions or links to other development projects [and may] become accepted as a means of payment’.³⁶ Their scarce supply should help them retain value and, consequently, make them employable as electronical payment instruments (hence the name cryptocurrencies) but their volatility often prevents them to achieve this function.³⁷ Security tokens are those that resemble traditional financial instruments (like shares, bonds or derivatives) and, as such, fall within the scope of securities laws.³⁸ The category of utility tokens, instead, is residual and includes every crypto-asset that does not fall within the first two categories.³⁹

2. The MiCA Regulation Proposal.

Risks and opportunities of this unregulated space, that includes both cryptocurrencies and utility tokens, led the EU Commission to adopt, in 2020, a ‘digital finance package’ composed of both a strategy and legislative proposals on crypto-assets and digital resilience.⁴⁰ On one side, the Commission recognized that the lack of regulation, combined with the market expansion, poses significant risks on the holders of crypto-assets in terms of investor protection, market integrity and financial stability.⁴¹ Furthermore, bespoke national laws on crypto-assets could determine market fragmentation, hinder the

³³ The distinction was identified by I M Barsan, ‘Legal Challenges’ (15), 56-59.

³⁴ Because of the expansion of the crypto-assets market, many other classifications have been developed through the years as to consider also ‘stable-coins’, ‘central bank digital currencies’ and ‘non-fungible tokens’. The British Financial Conduct Authority, for instance, identifies: (i) exchange tokens; (ii) utility tokens; (iii) security tokens; (iv) e-money tokens. See, FCA, ‘Guidance On Cryptoassets’ (2019) PS19/22. The Bank of Italy, instead, classifies: (i) virtual currencies; (ii) payment tokens, that include (a) stable-coins, (b) central bank digital currencies, and (c) non-convertible digital coins; (iii) security tokens; (iv) utility tokens. See, C Gola and A Caponera, ‘Aspetti Economici E Regolamentari Delle «Cripto-Attività»’ (2019) 484 *Questioni di Economia e Finanza*.

³⁵ FINMA, ‘Guidelines For Enquiries Regarding The Regulatory Framework For Initial Coin Offerings (ICO)’ (2018).

³⁶ FINMA, ‘FINMA Publishes ICO Guidelines (Press Release)’ (2018) 2.

³⁷ ECB Crypto-Assets Task Force, ‘Crypto-Assets: Implications For Financial Stability, Monetary Policy, And Payments And Market Infrastructures’ (2019) ECB Occasional Paper Series No 223, 9.

³⁸ FINMA, ‘Guidelines’ (35) 5-6; ESMA, ‘Advice On Initial Coin Offerings’ (11) 18-21.

³⁹ FINMA, ‘Guidelines’ (35) 5.

⁴⁰ Even though the MiCa Regulation is still not effective, some authors have already commented the proposal: D A Zetzsche and others, ‘The Markets In Crypto-Assets Regulation (MiCA) And The EU Digital Finance Strategy’ [2020] SSRN Electronic Journal; F Annunziata, ‘Verso Una Disciplina Europea Delle Cripto-Attività. Riflessioni A Margine Della Recente Proposta Della Commissione UE’ [2020] *Diritto bancario. Approfondimenti*; V P Carrière, ‘Crypto-Assets: Le Proposte Di Regolamentazione Della Commissione UE. Opportunità E Sfide Per Il Mercato Italiano’ [2020] *Diritto bancario. Approfondimenti*; R Lener and L Furnari, ‘Cripto-Attività: Prime Riflessioni Sulla Proposta Della Commissione Europea. Nasce Una Nuova Disciplina Dei Servizi Finanziari “Crittografati”?’ [2020] *Diritto bancario. Approfondimenti*; M Lucchesi, ‘Crypto-Assets: The Draft “MiCA” Regulation Aims For A New EU Regulation’ (2021) 179 *International Business Law Journal*.

⁴¹ EU Commission, ‘Communication COM/2020/591 final to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions on an Action Plan on a Digital Finance Strategy for the EU’ (24 September 2020) §4.4.

development of a digital single market, and limit the possibilities for businesses to scale up at a European level.⁴² On the other side, the EU saw the opportunity to create a safe and friendly environment for blockchain start-ups by removing legal uncertainty, reducing operating costs and boost investors' confidence in the market.⁴³

The digital finance package is aimed at regulating those crypto-assets which are not already governed by EU legislation and at proposing a pilot regime for market infrastructures that are considering the idea of adopting blockchain technology to clear and settle transactions.⁴⁴ The package, therefore, comprises different legislative proposals:

- Regulation on Markets in Crypto-assets (hereinafter, MiCa)⁴⁵;
- Directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341⁴⁶ – as to include crypto-assets;
- Regulation on a pilot regime for market infrastructures based on distributed ledger technology⁴⁷;
- Regulation on digital operational resilience for the financial sector (DORA)⁴⁸.

Security-like crypto-assets will still be governed by financial laws (in the clarified version), while the others will be regulated by the MiCa Regulation. On one side, to clarify the existing legal framework, the proposed Directive specifies that the category of 'financial instruments' defined by the MiFID II includes such instruments 'issued by means of distributed ledger technology' [art. 6 (1)]. On the other side, the MiCa Regulation excludes from its material scope those financial instruments [art. 2 (2)(a)] and requires firms to produce a legal opinion stating that their crypto-assets cannot be qualified as such [art. 16 (2)(d)]. Furthermore, the MiCa Regulation excludes from its scope crypto-assets issued by central banks acting in their monetary authority capacity [art. 2 (3)(a)].

The MiCa Regulation is mainly focused on stable coins, that recently emerged as a peculiar type of crypto-assets which seek to solve the volatile nature of cryptocurrencies.⁴⁹ Facebook and many players of the financial industry, for instance, started developing a stable coin pegged to several fiat currencies and

⁴² *Ibid.* §4.1.

⁴³ *Ibid.* §4.2.

⁴⁴ *Ibid.*

⁴⁵ Proposal for a European Union Regulation COM/2020/593 final of 24 September 2020 on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 [2020].

⁴⁶ Proposal for a European Union Directive COM/2020/596 final of 24 September 2020 amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341[2020].

⁴⁷ Proposal for a European Union Regulation COM/2020/594 final of 24 September 2020 on a pilot regime for market infrastructures based on distributed ledger technology [2020].

⁴⁸ Proposal for a European Union Regulation COM/2020/595 final of 24 September 2020 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 [2020].

⁴⁹ For an introduction to the topic, see: A Delivorias, 'Stablecoins. Private-Sector Quest For Cryptostability' [2022] European Parliamentary Research Service. On the legal issues posed by stable-coins, see: D W Arner, R Auer and J Frost, 'Stablecoins: Risks, Potential And Regulation' (2020) 905 BIS Working Papers; M Dell'Erba, 'Stablecoins In Cryptoeconomics. From Initial Coin Offerings (Icos) To Central Bank Digital Currencies (CBDC)' (2020) 22 New York University Journal of Legislation and Public Policy; J Cheng, 'How To Build A Stablecoin: Certainty, Finality, And Stability Through Commercial Law Principles' [2020] Berkeley Business Law Journal.

usable across the internet via social media platforms.⁵⁰ The mechanics of stable coins are not uniform: some are pegged to one or more fiat currencies or commodities (off-chain collateralized), some are pegged to other cryptocurrencies (on-chain collateralized), some implement algorithmic tools that adapt the supply to the market price (non-collateralized), and some others use hybrid or alternative mechanisms.⁵¹ By incorporating features designed to stabilise their value over time, stable coins may reach wider adoption as payment instruments and, ultimately, pose a serious threat to financial stability.⁵² The idea that the Euro, as payment system, may be eventually challenged by one or more stable coins led the EU to take action and regulate this space.

For this reason, the MiCa Regulation proposal essentially establishes two different regimes, a general one and another one specifically tailored on stable coins. Crypto-assets, in general, are defined as 'a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology' [art. 3 (1)(2)]. A definition that should be interpreted 'as widely as possible' in order to encompass every unregulated crypto asset (Recital 8). Two specific subcategories of stable coins are then defined and regulated separately: (1) 'asset-referenced tokens', which are stable coins pegged to 'several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets'; and (2) 'e-money tokens' which are stable coins pegged to a single fiat currency.⁵³ Algorithmic stable coins, that automatically adjust the supply according to the demand, should not be considered as asset-referenced tokens (Recital 26).

The main aim of the general regime is to ensure that issuers of crypto-assets act fairly and professionally, that crypto-assets services providers are reliable and resilient, and that market abuses are deterred and sanctioned.

The first set of rules regards issuers. To provide enough transparency and adequate assurances to purchasers, issuers of crypto-assets willing to start a public offering or to be admitted on an exchange platform should be, first of all, legal entities [art. 4 (1)(a)]. Secondly, issuers should draft a white paper, notify it to the supervisory authorities and publish it on their website [art. 4 (1)(b-d)]. Thirdly, marketing communications should be fair, clear and not misleading, and be communicated to the same authorities [art. 6-7]. Fourthly, funds received by the issuer during a public offering that is limited in time should be kept in escrow

⁵⁰ D A Zetsche, R P Buckley and D W Arner, 'Regulating LIBRA: The Transformative Potential Of Facebook'S Cryptocurrency And Possible Regulatory Responses' (2019) 44 European Banking Institute Working Paper Series.

⁵¹ M Dell'Erba, 'Stablecoins In Cryptoeconomics' (49), 10-15.

⁵² G7 Working Group on Stablecoins, 'Investigating The Impact Of Global Stablecoins' (2019) 12-14.

⁵³ The proposal establishes a different and stricter regime for 'asset-referenced tokens' (ARTs) and 'e-money tokens' (EMTs) due to their potential to become widely accepted as payment instruments (Recital 25). Issuers of ARTs, for instance, before launching a public offering or being admitted on a trading platform, should be authorized by the supervisory authority and their white papers should be approved prior to publication. Furthermore, at the crossroads of the regulation stand several rules regarding the stabilisation mechanism and the reserve assets backing the value of such crypto-assets. Issuers of EMTs, instead, should be either authorized as credit institutions or electronic money institutions and holders of EMTs should have a redemption right, at par value, of the fiat currency which the EMT is pegged to. Additional requirements and supervisory rules are then provided for 'significant' ARTs and EMTs, that are those exceeding certain thresholds defined by the EBA (e.g., market cap) that pose greater risks to financial stability.

by a credit institution or an authorised crypto asset service provider [art. 9]. Fifthly, those who purchase a crypto asset directly from the issuer should be provided with a right to withdrawal for a limited period of time [art. 12]. Lastly, issuers should act honestly, fairly and professionally, avoid conflicts of interests, and follow the most appropriate standards of security [art. 13].

A cornerstone of the legal regime is certainly the provision of a white paper, whose purpose is to inform prospective purchasers about functions, characteristics and risks of the crypto asset offering.⁵⁴ Even though the business practice makes blockchain start-ups already draft white papers, the MiCa Regulation proposal requires their notification to the supervisory authorities (but not their approval), provides explicit liability rules, and standardizes their content.⁵⁵ In fact, every white paper should contain information about the issuer, about the project, about the offering of crypto-assets or their admission to exchange platforms, about the rights and obligations attached to the crypto asset, about the technology employed and about the risks faced by purchasers [art. 5]. Furthermore, every marketing communication should be consistent with the content of the white paper [art. 6 (c)]. It is worth noting that cryptocurrencies like bitcoin and Non-Fungible-Tokens (NFTs) are exempt from the obligation to draft a white paper [art. 4 (2)].⁵⁶

The second set of rules involves crypto asset service providers. Often, crypto-asset holders are threatened by cybersecurity incidents involving exchange platforms⁵⁷, incidents that may cost millions of Euros in losses, undermine market confidence and, eventually, hinder financial stability.⁵⁸ Since the extent of those issues or risks is partially determined by the inexistent regulatory framework⁵⁹, the MiCa Regulation proposal attempts to mitigate them by creating a bespoke regime for crypto asset service providers. The proposal enlists, at art. 3 (1)(9), eight types of services that can be provided by such operators. The services can be grouped in two categories (Recital 12): the first one identifies the activities of trading platforms, exchanges, and wallet providers; the second one includes placing crypto-assets, receiving and transmitting orders, executing those orders and providing advice on crypto-assets. In order to provide those services on a professional basis, crypto asset service providers should be legal entities and should be authorized from the national supervisory authority. The ESMA updates

⁵⁴ P P Pirani, 'Gli Strumenti Della Finanza Disintermediata: «Initial Coin Offering» E «Blockchain»' [2019] *Analisi Giuridica dell'Economia*, 332-337.

⁵⁵ D A Zetsche and others, 'The Markets In Crypto-Assets Regulation' (40), 11-13.

⁵⁶ There are some notable exemptions from the obligation to draft a white paper: the most traditional ones regard private offerings (addressed to fewer than 150 people or solely to qualified investors) and offerings under the threshold of 1 million (over 12 months), and resemble those provided by the Prospectus Regulation; the most innovative ones, instead, regard crypto-assets that are offered for free, crypto-assets automatically created through mining, and crypto-assets that are unique and not fungible. Consequently, cryptocurrencies like bitcoin and Non-Fungible-Tokens (NFTs) will not be entirely governed by the MiCa Regulation proposal but only by title V, on crypto asset service providers, and by title VI, on the prevention of market abuses. Such exemptions seem to be justified by the fact that, in those cases, a proper offering does not take place because crypto-assets are either given for free, produced or individually negotiated and, therefore, their acquisition does not pose the same risk of information asymmetry.

⁵⁷ A Alkhalifah and others, 'A Taxonomy Of Blockchain Threats And Vulnerabilities', *Blockchain for Cybersecurity and Privacy* (2022).

⁵⁸ Financial Stability Board, 'Crypto-Asset Markets. Potential Channels For Future Financial Stability Implications' (2018), 8-12.

⁵⁹ MiCa Regulation Proposal, 4-5. See also OICV-IOSCO, 'Issues, Risks And Regulatory Considerations Relating To Crypto-Asset Trading Platforms' (2020), 3-5.

a register of crypto asset service providers.

The MiCa Regulation proposal requires crypto asset service providers to ‘act honestly, fairly and professionally in accordance with the best interests of their clients’ [art. 59 (1)] and, in particular, to warn their clients about risks and not to provide misleading information. Members of the management and those who own, directly or indirectly, a relevant stake in the business should have the necessary good repute and competence and should take all reasonable steps to ensure continuity and regularity in the performance of their crypto-asset services, both from an organizational and technical standpoint [art. 61]. Any crypto asset service provider should have in place prudential safeguards, in form of funds or an insurance policy, of an amount equal to the highest between the minimum capital requirements specified by annex IV per type of service (ranging from EUR 50.000 to 150.000) and one quarter of the fixed overheads of the preceding year [art. 60]. Moreover, providers should safekeep crypto-assets, passwords to access those crypto-assets, and any other fund belonging to their clients while avoiding their use without express consent. Finally, the proposal entails specific obligations for the provision of certain services related to crypto-assets.

The last – but not less important – set of rules concerns market abuses. In fact, certain behaviours could destabilize crypto asset prices, cause huge losses to their holders, and jeopardize users’ confidence in markets of crypto-assets (Recital 64). Hence, the MiCa Regulation proposal – considering that many crypto-assets fall outside the scope of the Market abuse Regulation⁶⁰ and that its entire application could be disproportionate – lays down specific rules to deter abuses. First, issuers should disclose inside information concerning the public in a ‘complete, correct, and timely manner’ unless it remains confidential, or may prejudice or mislead the public [art. 77]. Secondly, nobody in possession of inside information should use such information to deal with crypto-assets or to make recommendations to others [art. 78] and, thirdly, any conduct that may constitute market manipulation is prohibited [art. 80].

3. The Evidential Value of Distributed Ledgers.

Having already examined the legal framework of crypto-assets, it is now time to point the attention towards another central element of blockchain technology, the distributed ledger. As it is known, the distributed ledger is a core component of the blockchain because it ensures that the information stored in the blockchain remains untampered. In fact, by sharing encrypted copies of the ledger across multiple nodes, the blockchain safeguards its integrity against external attacks.⁶¹

A distributed ledger (more in general, a blockchain) plays mainly an evidential role since it provides and safeguards information.⁶² The bitcoin protocol, for instance, uses the distributed ledger to record any bitcoin transaction and,

⁶⁰ European Union Regulation No 596/2014 of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC [2014] OJ L 173/1.

⁶¹ J Bacon and others, ‘Blockchain Demystified’ (3), 12-13.

⁶² E Mik, ‘Blockchains As Transacting Platforms?’, *Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2019) 169; M Finck, *Blockchain Regulation And Governance In Europe* (Cambridge University Press 2019) 1.

consequently, to keep trace of bitcoins' entitlement history, making sure that it does not get hacked.⁶³ A distributed ledger, however, could custody any kind of information (even a document or an image). It works as a traditional database but, being distributed across multiple nodes, ensures the integrity of the data concerning that information. Hence, businesses could employ blockchain technology to record and preserve any kind of information (e.g., to keep track of their inventories or to safeguard important documents), developing the features that best suit their needs.⁶⁴

The evidence that can be provided by the distributed ledger falls within two broad categories: evidence about entitlement and evidence about attributes.⁶⁵ In the first case, the distributed ledger serves the purpose of recording any transaction of a certain asset intercurrent between participants of the blockchain. It, therefore, should give evidence about the person entitled to dispose of a certain asset: as a traditional land register records the ownership history of real estate, a distributed ledger can record the entitlement history of tokens, like with the bitcoin protocol.⁶⁶ In the latter case, the distributed ledger records additional information – such as the characteristics of an asset or a person – and its modifications. Documents, images, health data, and so forth, fall all within this category of evidence. Obviously, the two categories of evidence can be offered simultaneously. Blockchains that store non-fungible tokens, for instance, produce both evidence of entitlement and evidence of attributes of those specific tokens (representative of digital assets like images or texts).⁶⁷

The evidential features of the blockchain largely depend on the information stored by the distributed ledger. Whether the information refers to something that exists only on the blockchain (on-chain assets), the blockchain can be said to be 'pure'.⁶⁸ The bitcoin protocol, for instance, can be considered as a 'technologically "pure" system' because its electronic coins are intangible and exist only as digital entities. Moreover, any right over bitcoins is solely entitled by the distributed ledger itself and they would cease to exist if every copy of the ledger is erased. Conversely, whether the information refers to something or someone existing in the real world (off-chain assets), the blockchain can be said to be 'impure'. Off-chain assets exist outside the blockchain and can have either tangible form, like real estate or cars, or intangible form, like intellectual property rights or shares of a company. Both tangible and intangible off-chain assets can survive the peril of the blockchain because they have a legal existence in the real world. Rights in such assets are determined by the law and the blockchain is not the only evidence about those assets.

Off-chain assets pose a relevant issue to those willing to implement a blockchain. Since rights in such assets are determined by the law and not by the system itself, any modification not included in the distributed ledger could lead to

⁶³ S Nakamoto, 'A Peer-to-Peer Electronic Cash System' (8), 1.

⁶⁴ An early overview of the possibilities offered by blockchain technology was given by the bestselling book D Tapscott and A Tapscott, *Blockchain Revolution* (Penguin 2018).

⁶⁵ C Reed and others, 'Beyond Bitcoin' (5), 165.

⁶⁶ *Ibid.*

⁶⁷ A brief introduction to NFTs has been provided *supra* [10].

⁶⁸ C Reed and others, 'Beyond Bitcoin' (5), 161-164.

a mismatch between the reality of facts and that depicted by the blockchain.⁶⁹ A judgement, for example, could impact on the ownership of an off-chain asset. In such a case, because of the technical safeguards of blockchain technology, it would be very difficult – if not impossible – to rectify the distributed ledger. Therefore, the blockchain should be implemented in such a way as to give someone the authority to modify the information stored in the distributed ledger.⁷⁰ Otherwise, nobody would have the power to technically reverse any transaction because that power would be necessarily distributed among the nodes of the network.

Assuming nonetheless that distributed ledgers can preserve data integrity and perform an evidential function from a technical standpoint, their significance remains to be investigated from a legal standpoint in the European framework. The legal significance of distributed ledgers may not be a relevant problem to 'pure' blockchain systems because on-chain assets are created by the system, and it is the system itself that provides technical rights in such assets. Neither would be a relevant problem if the distributed ledger is adopted, within a single organization, just to ensure integrity of data collected for internal purposes (e.g., to track the inventory) because the ledger does not serve an evidential function outside the organization. However, the problem gains utmost importance if off-chain assets and third parties are involved. In fact, despite the technical safeguards provided by blockchain technology, the legal system may not recognize any value to the information stored in the distributed ledger and it would not provide any evidence in a legal sense.⁷¹

Hence, it is time to investigate under which conditions distributed ledgers can truly play an evidential role for off-chain assets. As a general premise, it is necessary to highlight that not every activity that has legal effects can be freely executed by private individuals. Many activities are of exclusive competence of the State and can be performed only by governmental bodies or qualified professionals using predetermined technical instruments. It is the case, for example, of real estate transactions: in every European Member State registering ownership of and charges on land involve qualified professionals and land registers held by governmental bodies.⁷² This kind of activities falls, at least partially, under the scope of public law and implementing distributed ledgers in such matters would certainly require law amendments and tailored technical solutions to provide any legal effect.

The evidential function of distributed ledgers could be more easily exploited in

⁶⁹ J Bacon and others, 'Blockchain Demystified' (3), 32-33; E Mik, 'Smart Contracts: Terminology, Technical Limitations And Real World Complexity' (2017) 9 Law, Innovation and Technology, 11.

⁷⁰ In terms of structure, blockchains can show great differences, the main one being probably between public (permissionless) and private (permissioned) blockchains. Public blockchains allow everyone to obtain a copy of the distributed ledger and participate in the consensus mechanism employed to update the distributed ledger. Governance, therefore, is distributed democratically among the users of the network. Private blockchains, instead, adopt an access control layer (ACL) that requires users to be authorized in order to access the network. Since developers preserve some form of governance, the blockchain loses its complete decentralization and resembles more traditional software applications. See, M Finck, *Blockchain Regulation* (62) 195-198; ESMA, 'Advice On Initial Coin Offerings' (11), 10-11.

⁷¹ It has already been advocated that information stored on a distributed ledger may not constitute property. See, L Sagar, *The Digital Estate* (Sweet & Maxwell 2018) chapter 4.

⁷² European University Institute, 'Real Property Law And Procedure In The European Union' (2005).

private law matters because of the principle of freedom of contract.⁷³ As it is known, individuals are free to decide whether and with whom they want to enter into a contract and, more importantly, its content (within the boundaries of the law). Parties, therefore, are capable of determining the terms of their agreement and its legal effects. In these matters, they can also decide to adopt a technical instrument like blockchain technology and its distributed ledger. In substance, the distributed ledger could be employed either to record the contract, as to preserve its content, or be recalled by the contract itself as a source of information (to measure the performance agreed, the occurrence of some conditions, etc.). The parties, for instance, could rely on the information stored on the distributed ledger to determine the price to be paid in exchange of some goods or services offered.

Those interested in implementing a blockchain, however, should pay attention to the form required by the law to conclude the contract. As it is known, contracts can be both concluded – implicitly – by conduct, or – expressly – by word of mouth or in writing. The general rule is that contracts can be concluded informally, as the parties prefer. However, specific rules, depending on the matter and on the country, impose the written form either as evidence or as a validity requirement.⁷⁴ When the law requires the written form, distributed ledgers could not produce any legal effect unless they are able to satisfy the legal requirement of the written form. Therefore, it is necessary to assess whether a distributed ledger, in abstract, can satisfy this requirement.

To solve the problem, it is necessary to give a bit of context. From an historical standpoint, the legal requirement of the written form was developed around paper documents. In fact, paper documents – either manuscript or simply signed – have two main features: (1) through the signature, they can provide evidence about the identity of the signatory and about its intention to adopt the content of the document; and (2) they are difficult to counterfeit because, in most cases, experts can verify both handwriting and modifications on those documents. Conversely, many electronic documents are modifiable without leaving traces, and cannot be uniquely attributed to one person. This is the reason why, facing the emergence of e-commerce and the transition from paper documents to electronic documents, the European legal system had to find tailored solutions to identify parties and ensure integrity of electronic documents.⁷⁵

The main piece of legislation in this regard is the eIDAS Regulation⁷⁶ that, succeeding Directive 1999/93/EC, is modelled around electronic signatures and trust services. On one side, electronic signatures are utilised to preserve data integrity due to their technical capability to cipher electronic documents. On the other side, ‘trust service providers’ (Certification Authorities and Registration Authorities) are appointed responsible for verifying identities and issuing ownership certificates of electronic signatures. In other words, flaws of electronic documents are solved by using electronic signatures in combination with trust service providers both to authenticate parties and to secure electronic

⁷³ Some authors investigated aspects of contract and property laws as to determine whether digital assets are capable of acquiring *erga omnes* status. See, R Kulms, ‘Blockchains: Private Law Matters’ [2020] Singapore Journal of Legal Studies, 63-89.

⁷⁴ E McKendrick, *Goode On Commercial Law* (Penguin 2010) 80.

⁷⁵ C Reed, ‘What Is A Signature?’ (2000) 3 Journal of Information Law & Technology.

⁷⁶ European Union Regulation No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73.

documents.

The eIDAS Regulation states also the principle whereby ‘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’ [Art. 46]. However, not all electronic documents are considered equal by the Regulation because it takes a tiered approach to legal value. In fact, the evidential strength changes according to the electronic signature attached to the document: the higher the guarantees offered by the signature, the stronger the evidential value will be. The simplest ‘electronic signature’ is any data ‘used by the signatory to sign’, such as plain text or an image of the signature [art. 3(10)]. An ‘advanced electronic signature’ is uniquely linked to the signatory and to the data signed therewith ‘in such a way that any subsequent change in the data is detectable’ [art. 26(1)(d)]. A ‘qualified electronic signature’ is an advanced electronic signature issued by a qualified trust service provider that meets the technical requirements laid down by the eIDAS Regulation. Being the safest, the qualified electronic signature produces ‘the equivalent legal effect of a handwritten signature’ [art. 25(2)]. Consequently, electronic documents signed with this kind of signature are the only ones that meet the requirement of the written form. Other electronic documents will produce legal effects only if the written form is not a validity requirement.

Since ‘electronic documents’ are defined by the eIDAS Regulation as ‘any content stored in electronic form, in particular text or sound, visual or audiovisual recording’ [art. 3(35)], distributed ledgers could well be considered as such.⁷⁷ Hence, they would be admissible as evidence in legal proceedings as any other electronic document and, likewise, their evidential strength would rely on electronic signatures. Therefore, the implementation of electronic signatures in distributed ledgers needs to be analysed further.

As it is known, blockchains already employ public-key cryptography, that is the same technology adopted by many advanced and qualified electronic signatures. The system works by generating for each user a pair of linked keys (constituting a digital signature): the private key can be used to sign, while the public key can be used to authenticate the signatory and verify the integrity of the data. The difference is that, whereas e-signatures are uniquely attributed to a real-life person by a trust service provider, blockchains only need to authenticate users on a technical level (to identify users allowed to interact with the distributed ledger).

Nonetheless, blockchains do not operate all in the same way, and a distinction should be drawn between permissionless and permissioned ledgers.⁷⁸ In permissionless ledgers everyone can join the network, and every user remains anonymous. In the bitcoin protocol, for instance, everyone is allowed to anonymously set up a wallet and create the keys required to send and receive bitcoins. Thus, the set of keys would never be capable of identifying users and the distributed ledger would have a weak evidential value.

⁷⁷ F Sarzana di S. Ippolito and M Nicotra, *Diritto Della Blockchain, Intelligenza Artificiale E Iot* (IPSOA 2018) 51.

⁷⁸ *Supra* [70]. Moreover, H Eenmaa-Dimitrieva and M J Schmidt-Kessen, ‘Regulation Through Code As A Safeguard For Implementing Smart Contracts In No-Trust Environments’ (2017) 13 EUI Working Papers, 10-16.

In permissioned ledgers, instead, access is restricted solely to the members that have been approved by some form of centralized authority. This access control layer, hence, could be designed as to require user identification.⁷⁹ In this case, users would be uniquely linked to the signature required to interact with the distributed ledger as with an advanced electronic signature. An organization willing to implement its own distributed ledger, for instance, could assign a pair of keys to each customer after the upload and live verification of his identification document. In this case, any piece of information stored in the distributed ledger by the customer, such as a purchase order, would have a strong evidential value. However, in order to meet the legal requirement of the written form, the organization would have to rely on qualified trust service providers (or register itself as such) and attribute qualified electronic signatures to its users.

However, adapting the rules designed for e-signatures for blockchain applications, is not an easy task. For this reason, the EU Commission has recently proposed an amendment to the eIDAS Regulation that attempts to cope with distributed ledgers.⁸⁰ An 'electronic ledger' (to use the proposal's words) is there recognized to combine 'time stamping of data and their sequencing with certainty about the data originator similar to e-signing with the additional benefit of enabling a more decentralized governance that is suitable for multi-party cooperation', and to 'help companies saving costs by making multiparty coordination more efficient, safer and [to facilitate] regulatory supervision'. The regulation of electronic ledgers, thus, becomes of 'paramount' importance to give legal effect to the transactions contained within the ledger itself.⁸¹

The proposal distinguishes between simple 'electronic ledgers', that are tamper proof records of data, and 'qualified electronic ledgers', that are also created by a qualified trust service provider by implementing technologies that ensure the requirements set forth in the Regulation. Hence, it first recognizes the legal value of all electronic ledgers and, secondly, states that 'a qualified electronic ledger shall enjoy the presumption of the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering within the ledger [art. 45(h)]. As a consequence, the certification as qualified trust service providers should provide that legal certainty needed for use cases where the distributed ledger needs to meet the requirement of the written form. Using the words of the European legislator, a qualified electronic ledger 'creates a reliable audit trail for the provenance of commodities in cross-border trade, supports the protection of intellectual property rights, enables flexibility markets in electricity, provides the basis for advanced solutions for self-sovereign identity and supports more efficient and transformative public services' (Recital 34).

⁷⁹ The adoption of permissioned ledgers in the financial system to solve the issue of digital identification and representation is analysed taking as an example Diem, the stable-coin sponsored by Meta by G A Jafari and M C Gruber, 'The Case Of Diem: A Distributed Ledger Technology-Based Alternative Financial Infrastructure Built By A Centralised Multisided Platform' (2021) 4 Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 324-326.

⁸⁰ Proposal for a European Union Regulation COM(2021) 281 final of 3 June 2021 amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity [2021].

⁸¹ C Sorge and M Leicht, 'Blockchain-Based Electronic Time Stamps And The Eidas Regulation: The Best Of Both Worlds' (2022) 19 SCRIPT-ed; R Garavaglia, 'Cambia Il Regolamento Eidas E Nascono I Gestori Qualificati Di Registri Distribuiti' (*Pagamenti Digitali*, 2021) <<https://www.pagamentidigitali.it/payment-regulation/eidas/>> accessed 8 June 2022.

4. Giving Smart Contracts a Legal Framework.

The most famous application of blockchain technology is almost certainly that of smart contracts, whose name and possible implementations have sparked an intense debate among legal scholars.⁸² In fact, smart contracts aspire to be contracts written in programming language that enable computers to autonomously execute them.⁸³ In other words, self-performing contracts. However, the reality is that they are just computer programs that run on a blockchain. Therefore, it is necessary to analyse their legal value and their relationship with traditional contracts and, more specifically, to define under which conditions they can be legally binding and how can they be enforced.⁸⁴

The idea of autonomous (smart) contracts is not new. Nick Szabo coined the term in 1997 by giving an example: as a vending machine takes coins and dispense product and change fairly, so could computers engage in any exchange of valuables controlled by digital means.⁸⁵ The basic idea was to embed contractual clauses in hardware and software as to make breach of contract expensive. In this way, once the parties define the terms of the contract, those are converted into a computer program that automatically checks if some conditions are met and provides the expected performance. At this point, the contract could autonomously enforce itself without any intervention (hence becoming 'smart').

The difference between traditional contracts and smart 'contracts' stands in the fact that a smart contract would not only be concluded, but also performed, electronically. In traditional contracts, conclusion and performance are two very different moments. First, the parties agree to be bounded and, only afterwards, they execute the contract. If one of the parties is not willing to perform, the process can be very inefficient and consuming: the other party has to institute legal action for breach of contract and demand, before the Court, its enforcement. In smart contracts, conversely, the breach of contract would be impossible. Since

⁸² Among many others, P Cuccuru, 'Beyond Bitcoin: An Early Overview On Smart Contracts' (2017) 25 International Journal of Law and Information Technology, 188; P Cuccuru, 'Blockchain Ed Automazione Contrattuale. Riflessioni Sugli Smart Contracts' [2017] Nuova giur. civ. comm., 107; D Di Sabato, 'Gli Smart Contracts: Robot Che Gestiscono Il Rischio Contrattuale' [2017] Contr. impr., 386; C Clack, V A Bakshi and L Braine, 'Smart Contract Templates: Foundations, Design Landscape And Research Directions' [2017] arXiv:1608.00771v3; K E C Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts And The Social Workings Of Law' (2017) 3 Engaging Science, Technology, and Society, 1; E Mik, 'Smart Contracts: Terminology, Technical Limitations And Real World Complexity' (2017) 9 Law, Innovation and Technology, 269; R De Caria, 'The Legal Meaning Of Smart Contracts' (2018) 26 European Review of Private Law, 731; M Giuliano, 'La Blockchain E Gli Smart Contracts Nell'innovazione Del Diritto Del Terzo Millennio' [2018] Diritto dell'informazione e dell'informatica, 989; M Durovic and F Lech, 'The Enforceability Of Smart Contracts' (2019) 5 The Italian law journal, 493; C Miraglia and V Orsini, 'Gli Smart Contract Tra Falsi Miti E Teoria Generale', *Temi di diritto civile* (Brasil Multicultural 2019), 119; P De Filippi, C Wray and G Sileno, 'Smart Contracts' (2021) 10 Internet Policy Review, 2. An extensive study has been recently published by UK Law Commission, 'Smart Legal Contracts Advice To Government' (2021).

⁸³ E Mik, 'Smart Contracts' (82), 3-5.

⁸⁴ Some authors argue that smart contracts 'should be considered as self-sufficient legally-binding agreements' because they 'do clearly create obligations which stand independently from the digital code'. See, R De Caria, 'The Legal Meaning Of Smart Contracts' (82), 746-749.

⁸⁵ N Szabo, 'Smart Contracts: Building Blocks For Digital Markets' (Fon.hum.uva.nl, 1996) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 8 June 2022.

smart contracts are self-performing, there would not be (at least theoretically) any necessity for public enforcement.⁸⁶ One party, for instance, could never deliberately fail to pay, because the programming code would autonomously provide for it.

In recent years, contracts started to show an increasing degree of automation.⁸⁷ It might be enough to recall how Uber determines the price of a ride and automatically pays the driver, or how streaming platforms like Netflix allow users to access their content only under payment. Nonetheless, it was not until the launch of the Ethereum platform in 2014 that the expression 'smart contracts' was evoked again and became popular. In fact, as it is known, the Ethereum platform was conceived in a Turing-complete programming language as to allow anyone to deploy decentralized applications called 'smart contracts' and to receive payments in its native cryptocurrency, 'ether'.⁸⁸

The dual spirit of cryptocurrency scheme and software development platform was the key for the revival of the idea of smart contract. On one side, the implementation of smart contracts in a blockchain framework helps to prevent unilateral changes to the contractual scheme and is particularly helpful in no-trust environments. On the other side, the possibility to arrange payments in cryptocurrency avoid interferences of banking intermediaries in the execution of the smart contract (payment orders, for instance, cannot be revoked).

The expression 'smart contracts' could be misleading because it might induce to think that they are the digital equivalent for traditional contracts.⁸⁹ It is oversimplistic to think that any contractual clause could be expressed as an algorithm and that, consequently, any contract could be traduced into a computer program.⁹⁰ Even though code and contract can – at least theoretically – overlap, it is very difficult to establish whether a software can be considered as a legally binding contract. Therefore, it is of paramount importance to clarify the fundamental elements that qualify, from a legal standpoint, a contract and verify whether, and to what extent, they can be represented in programming code.⁹¹ The code governing the smart contract could well be unable to meet the requirements imposed by the law and, consequently, result only in a piece of code that automates a performance. 'The technology of smart contracts does not constitute a new contract law; instead, the interpretation and validity of smart contracts has to be assessed against the backdrop of existing contract law'.⁹²

A contract is 'an agreement between private parties creating mutual obligations enforceable by law'.⁹³ It is a legally binding agreement because

⁸⁶ P Cuccuru, 'Beyond Bitcoin' (82), 186-188.

⁸⁷ Contractual implications of the automation of contracts are analysed in detail by M D'Ambrosio, *Arbitraggio E Determinazione Algoritmica Dell'oggetto* (Edizioni scientifiche italiane 2020).

⁸⁸ See, 'What Is Ethereum?' (ethereum.org) <<https://ethereum.org/en/what-is-ethereum/>> accessed 6 July 2022.

⁸⁹ G Finocchiaro, 'Il Contratto Nell'era Dell'intelligenza Artificiale' [2018] *Rivista trimestrale di diritto e procedura civile*, 441-460.

⁹⁰ Some authors even claim that 'smart contracts fail to take the social complexities of contracting into account' and that 'contracts operate as social resources, through and against which people manage their relationships, and within which legal obligations and social expectations are intricately interwoven and mutually constitutive'. See, K E C Levy, 'Book-Smart, Not Street-Smart' (82), 10.

⁹¹ M Giuliano, 'La Blockchain E Gli Smart Contracts' (82), 1027.

⁹² J Oster, 'Code Is Code And Law Is Law—The Law Of Digitalization And The Digitalization Of Law' (2021) 29 *International Journal of Law and Information Technology*, 14.

⁹³ E Peel and G H Treitel, *Treitel On The Law Of Contract* (Sweet & Maxwell/Thomson Reuters 2020).

parties can rely on the law and its agents to enforce it. In case of breach, the Court can put the innocent party in the position he would have been in had the contract been properly performed.⁹⁴ The agreement, however, shall meet the requirements set by the applicable law.⁹⁵ Requirements vary across legal systems and countries but, in principle, the fundamentals are mutual assent, adequate consideration, capacity, and legality. In some cases (like financial transactions), formalities like the written form can also be required. Hence, the smart contract should not infringe the law (for instance, by selling access to hacked software), involve adequate consideration, and – more importantly – be stipulated with mutual assent. Parties should agree to be legally bound through an offer and an acceptance: either via digital means (e-mails, click-wrap agreements, etc.) or implicitly (one party makes available the smart contract and the other consciously executes it).

For the sake of clarity, it might be helpful to divide smart contracts in ‘smart contract code’ and ‘smart legal contracts’.⁹⁶ A smart contract can be considered as ‘smart contract code’ when it is only a software that automates a performance and requires a separate contract to set the terms (for instance, a computer program that automates an insurance contract). In this case, the use of the word ‘contract’ is inappropriate and does not bring any legal implication since the contractual terms will have to be found elsewhere (contract and code are separated). A smart contract can be considered, instead, as a ‘smart legal contract’ when the software is, autonomously, a legally binding contract (contract and code overlap). The contract here is not only performed but also represented by programming code because the legal requirements are satisfied.

A smart contract code, requiring parties to separately stipulate a traditional contract, falls under the ‘external model’ of smart contract.⁹⁷ In fact, the contractual terms that are legally binding are external to the smart contract itself: the parties first stipulate the contract (orally, in writing, or digitally) and then execute the smart contract code as to automate the performances. Conversely, in a smart legal contract, parties enter into an agreement by simply using the program (for instance, sending a certain amount of cryptocurrency to the wallet of the smart contract). Therefore, it can be said described as an ‘internal model’ of smart contract: the contractual terms are the algorithms constituting the smart contract itself. The whole contractual scheme is represented by algorithms. Fictionally, one party makes an offer by making available the smart contract while the other accepts by activating it. Using the computer program, the party agrees to its rules and accept its outcomes.

The internal model is not suitable for all contracts because the contractual

⁹⁴ Robinson v Harman [1848] 18LJ Ex 202.

⁹⁵ UK Law Commission, ‘Smart Legal Contracts’ (82), 39-73, for instance, outlines the requirements for a legally binding contract under the law of England and Wales and discuss how these requirements might be satisfied in the context of smart legal contracts.

⁹⁶ Distinction proposed by Josh Stark in ‘Making Sense Of Blockchain Smart Contracts’ (CoinDesk) <<https://www.coindesk.com/making-sense-smart-contracts/>> accessed 1 July 2022. Later, it has been adopted by C Clack, V A Bakshi and L Braine, ‘Smart Contract Templates’ (82), 6. Recently, it has been used as the foundation of UK Law Commission, ‘Smart Legal Contracts’ (82).

⁹⁷ The idea that smart contracts may fall either within the internal model of smart contract or the external one has been laid out by ISDA Linklaters, ‘Smart Contracts And Distributed Ledger – A Legal Perspective’ (ISDA Linklaters 2017) <<https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf>> accessed 8 June 2022.

scheme needs to be easily understandable. The smart contract should be able to show the necessary information which is material to an acceptee for making an informed assessment, just like a vending machine displays both the product and the price. Since the party makes an offer by making available the smart contract, the offer must include all the key terms of the contract. Otherwise, as it is known, it will classify as an advertisement. However, the programming code is not always inspectable and is not comprehensible by everyone.⁹⁸ Thus, the offer should be simple enough as to be acceptable by tacit or implicit consent. Complex contractual schemes could be binding only if additional information is provided and, consequently, need to adopt the external model of smart contract.

Moreover, every clause of the contract should be susceptible of being translated into programming language. First, not everything that has legal relevance can be executable by computer programs because they cannot 'encode references to general standards or general clauses' (like the principle of good faith).⁹⁹ Even though AI technology would enable it, traditional software is not capable of interpreting or guessing.¹⁰⁰ Nonetheless, AI would introduce a margin of error that is unacceptable for blockchains. Secondly, only operational aspects of a contract (those regarding some sort of action, like a cryptocurrency transfer) can be automated. Consequently, an internal model of smart contract would be draftable only with unambiguous terms and operational aspects.¹⁰¹

Nonetheless, the external model of smart contract presents some disadvantages due to the fact that the contractual scheme and the smart contract code are detached. Once activated, the smart contract executes the performance autonomously and cannot be interrupted. This means that any contractual issue (e.g., null and void contract) has no consequences on the execution of the software. The performance, in this case, would be legally invalid but computationally correct.¹⁰² Consequently, it would not be rectifiable unless an opposite transaction is recorded on the blockchain, or the blockchain itself is designed as to allow rectification in specific cases. In fact, 'the alteration would invalidate the hash of the block containing the record, and also the hashes of all subsequent blocks'¹⁰³. This means that, in case of breach, the Court would not have the power to directly interfere with the smart contract but would have to use other remedies such as damages. The internal model of smart contract, however, would suffer of the same issue in case of programming errors.

⁹⁸ P Cuccuru, 'Beyond Bitcoin' (82), 188-189.

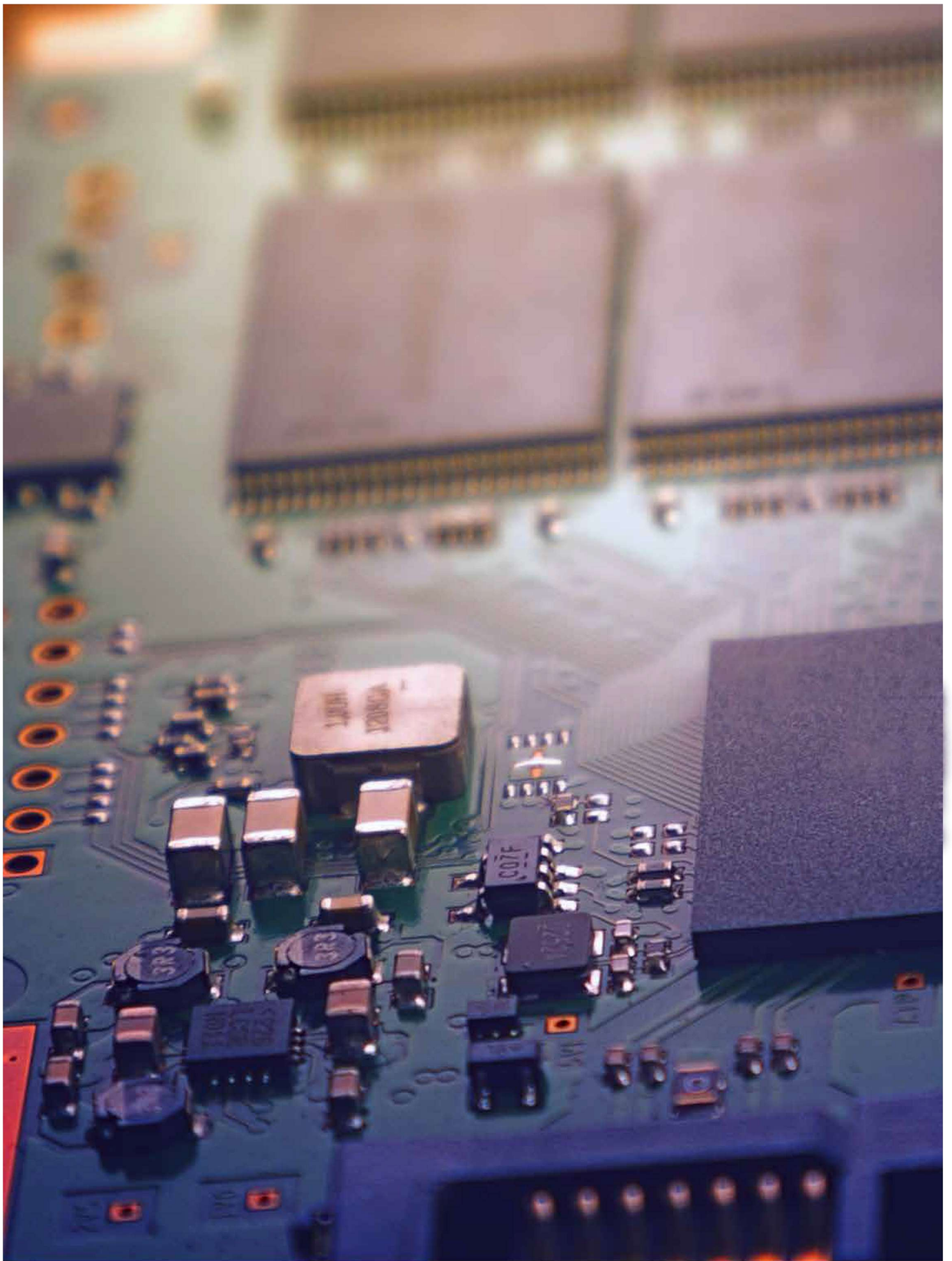
⁹⁹ *Ibid.*, 189-190.

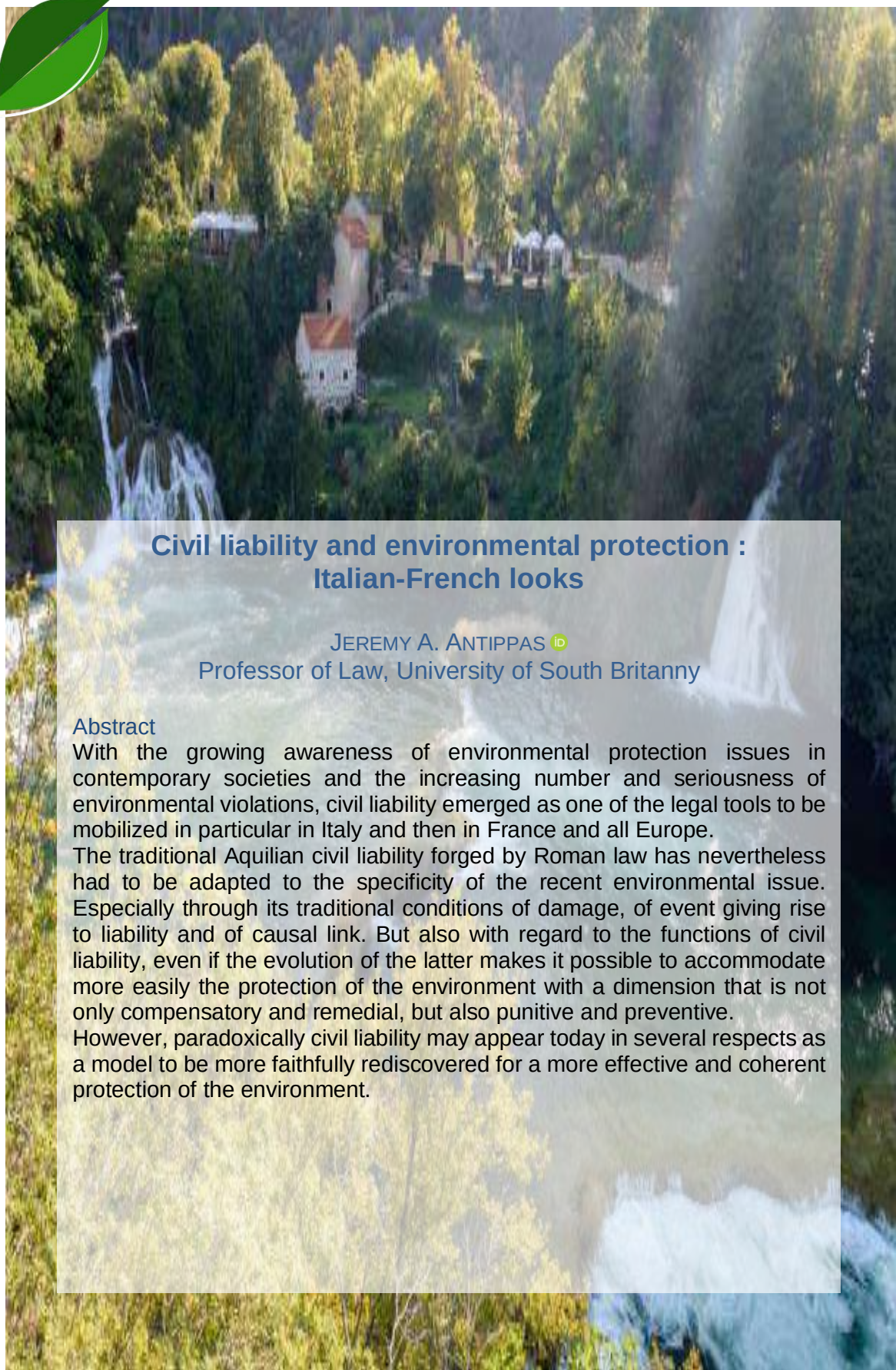
¹⁰⁰ Some authors advocate that '[p]redictive capabilities created by big data and artificial intelligence increasingly allow parties to draft contracts that fill their own gaps and interpret their own standards without adjudication' - A J Casey and A Niblett, 'Self-Driving Contracts' [2017] SSRN Electronic Journal, 1.

¹⁰¹ C Clack, V A Bakshi and L Braine, 'Smart Contract Templates' (82) 5-11.

¹⁰² It is even argued that 'smart legal contracts may actually increase instances of defective performance, given the scope for the code to perform in ways the parties did not expect or intend'. See, UK Law Commission, 'Smart Legal Contracts' (82) 102-155, that extensively analyses the remedies applicable (also in practice) by British Courts.

¹⁰³ C Reed and others, 'Beyond Bitcoin' (5) 22.





Civil liability and environmental protection : Italian-French looks

JEREMY A. ANTIPPAS 

Professor of Law, University of South Brittany

Abstract

With the growing awareness of environmental protection issues in contemporary societies and the increasing number and seriousness of environmental violations, civil liability emerged as one of the legal tools to be mobilized in particular in Italy and then in France and all Europe.

The traditional Aquilian civil liability forged by Roman law has nevertheless had to be adapted to the specificity of the recent environmental issue. Especially through its traditional conditions of damage, of event giving rise to liability and of causal link. But also with regard to the functions of civil liability, even if the evolution of the latter makes it possible to accommodate more easily the protection of the environment with a dimension that is not only compensatory and remedial, but also punitive and preventive.

However, paradoxically civil liability may appear today in several respects as a model to be more faithfully rediscovered for a more effective and coherent protection of the environment.



Keywords: adaptation; associations; civil liability; conditions; comparison; environment; French law; functions; Italian law; ministry of Environment; person liable; plaintiff; pollution; protection.

Summary: [1. Introduction.](#) – [2. Part I: The adaptation of civil liability made for environmental protection.](#) – [3. Part II: The adaptation of environmental liability to make on the model of civil liability.](#)

1. Introduction.¹

*'La maison brûle et nous regardons ailleurs'*² ('The house is burning and we are looking elsewhere') declared the President of the French Republic Jacques Chirac twenty years ago. Pollution and global warming are indeed destroying our planet and its inhabitants. However, for several decades the occupants of the house who will have to leave it sooner or later to the next generations have been turning to various legal instruments. Different mechanisms appear indeed likely to ensure a protection of the environment on a public scale: – taxation, police, penalization, or recourses in annulment of certain administrative acts in front of pollution.

For example, in France in the recent case of Grande Synthe of July 1, 2021³ the French Council of State annulled the refusal of the regulatory authority to take the additional measures necessary to curb the curve of greenhouse gas emissions produced on the national territory as being incompatible with the trajectory of reduction of these emissions set by decree (of April 21, 2020). The French Council of State also ordered the enactment of such measures within a certain period of time (nine months), in accordance with two international texts in particular: the United Nations Framework Convention on Climate Change (UNFCCC) of May 9, 1992 (which sets as its objective, in Article 1, to 'stabilize greenhouse gas concentrations in the atmosphere at a level that would prevent dangerous anthropogenic interference with the climate system') ; and the famous Paris Agreement, of December 12, 2015 on the occasion of the 21st Conference of the Parties of the UNFCCC (which aims in particular in its Article 2 to contain 'the increase in global average temperature well below 2° C above pre-industrial levels and continuing the action taken to limit the increase in temperature to 1.5° C above pre-industrial levels').

Civil liability, especially extra-contractual liability, which did not necessarily appear to be the most obvious in this area, is also from a legal standpoint one of the possible ways of protecting the environment. In this respect, Italy preceded France: the Court of Auditors in several decisions of the early 1970ies handed down in connection with abuses in the Abruzzo National Park held public officials liable, initially administratively, toward the

¹ This text is the translation of an oral communication performed in Italian by its author for the Benincasa University of Naples and its Center of research ReCEPL, on April 20th, 2022, at the invitation of Professor Ilaria CAGGIANO, whom the undersigned thanks very much.

² Le Monde, 2002/09/02.

³ CE, 2021/07/01, n 427301.

public authority.⁴ In the case of the Scarlino Red Mud⁵ it also held responsible the civil servants who had authorized the dumping of toxic waste.⁶

Then, the environmental protection by the judges was done through the use of the right of ownership (art. 844 of the Italian Civil Code) and the classic civil liability (art. 2043 and seq. of the Italian Civil Code).

For example, the Italian Court of cassation has held strict civil liability, i.e. without the need to prove a fault or a fraud, for damages resulting from dangerous activities under Article 2050 of the Civil Code regarding the production, transportation, management and disposal of pollutant products.⁷

Similarly, article 2051 of the Civil Code has sometimes been used to hold the custodial strict liability, for instance by the Tribunal of Venice referring at *'la previsione dell'art. 2051 c. c., inusuale per le ipotesi di danno ambientale, ma non del tutto esclusa'*⁸ ('the provision of art. 2051 c. c., unusual for environmental damage hypotheses, but not entirely excluded').

There are sentences in the opposite sense, like the one of the Tribunal of Milan ruling that : *'è da escludere, in base al principio di specialità, che con riferimento al danno ambientale possa trovare applicazione la disciplina di cui all'art. 2043 c.c. e, tantomeno, la disciplina della responsabilità da attività pericolose ex. art. 2050 c.c. e da custodia di cui all'art. 2051 c.c.'*⁹ ('it is to be excluded, based on the principle of specialty, that with reference to environmental damage can be applied the discipline of art. 2043 civil code and, even less, the discipline of liability for dangerous activities under art. 2050 c.c. and from custody under art. 2051c.c.').

However, as regards the right of *ownership* as a means of combating environmental damage, this appears relevant only insofar there is an harm to an owner.

Besides, this requires exceeding a certain threshold of tolerability, which is variable in particular according to the different persons and the local situations. The Italian Council of State in fact ruled that *'la valutazione diretta a stabilire se i rumori restino compresi o meno nei limiti della norma, deve essere riferita, da un lato alla sensibilità dell'uomo medio e, dall'altro, alla situazione locale'*¹⁰ ('the evaluation intended to establish whether or not the noise is within the limits of the norm must be carried out according to the sensitivity of the average person, on the one hand, and the local situation, on the other').

The Italian Constitutional Court for its part quite early on marginalized the right of ownership as an instrument of environmental liability, judging that art. 844 of the Civil Code is not *'uno strumento adeguato a risolvere i gravi problemi creati dall'inquinamento (...) la legge è, infatti, destinata a risolvere il conflitto tra proprietari di fondi vicini'*¹¹ ('a suitable instrument for solving the serious problems

⁴ Corte dei Conti, 1973/05/15, n 39; 1975/12/20, n 108; 1979/10/08, n 61; 1980/02/15, n 868.

⁵ Corte dei Conti, 1979/10/08, n 61.

⁶ This solution is perhaps a little more difficult to imagine in France where, in order to engage the personal liability of public agents, it is necessary according to the *Pelletier* jurisprudence (1873/07/30, n 00035) to prove a personal fault, understood as being of great seriousness or wilfulness, which is not always verifiable in the case of a discharge of waste in the professional context.

⁷ Cass. civ. Sec. I, 1995/09/01, n 9211.

⁸ Trib. Ven., Sec. III, 2010/04/02.

⁹ Trib. Mil., Sec. II, 2010/09/16.

¹⁰ Cons. Stato, Sez. IV, n 2109/2018.

¹¹ Corte Cost., 1974/07/23, n 247.

created by pollution (...) the rule is, in fact, intended to resolve the conflict between owners of neighboring land...') and therefore that '[il] contenuto del diritto di proprietà non [poteva] essere utilizzato per giudicare della liceità di immissioni che rechino pregiudizio anche alla salute umana o all'integrità dell'ambiente naturale, alla cui tutela è rivolto in via immediata tutto un altro ordine di norme di natura repressiva e preventiva'¹² ('[the] content of the right of ownership [could] not be used to judge the lawfulness of emissions that also harm human health or the integrity of the natural environment, to the protection of which a completely different order of norms of a repressive and preventive nature is immediately dedicated').

Some authors advocated a right to the environment under Article 2 of the Constitution, ruling that ' *La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo (...)* ' ('The Republic recognizes and guarantees the inviolable rights of Man (...)'), independently of the right to property and even of the right to health.¹³

Beyond the personal rights, traditional civil liability was also used to protect environment. The Italian Court of Cassation for example was able to conclude to the application not only of civil liability but of strict liability for damage resulting from dangerous activities, governed by art. 2050 of the Civil Code.¹⁴ Similarly, custodian liability of article 2051 of the same Code was sometimes used.¹⁵

The Italian law n 349 (1986/07/18), which created the Ministry of Environment, also defines environmental damage by referring to the fact of altering, deteriorating or destroying the environment in whole or in part; it entrusts the ordinary judge with the competence to deal with it. This law makes environmental liability a particular civil liability, as the Constitutional Court confirmed in relation to the 1986 law: ' *La responsabilità che si contrae è correttamente inserita nell'ambito e nello schema della tutela aquiliana*'¹⁶ ('The liability that is contracted correctly inserted into the field and scheme of aquilian liability').

However, although it defined environmental damage for the first time in legislation, currently this law largely referred to other special laws as regards the events giving rise to liability.

Special texts were adopted that made liability easier to enforce. In particular, the decree-law called 'Ronchi decree' n 22/1997 (1997/02/05) concerning environmental sanitation, or the decree-law n 224/2003 concerning the deliberate release of genetically modified organisms (GMO) into the environment. Today is in force the decree-law n 152 2006/04/03, that created the Italian Environmental Code, of which part sixth deals with '[la] tutela risarcitoria contro i danni all'ambiente' ('compensatory protection against environmental damages'), following the European Parliament and Council directive 2004/35/EC of 21 April 2004 on prevention and remedy in matters of environmental liability (OJ L 143/56).

Indeed, the protection of the environment through civil liability in particular and the treatment of environmental damage is also a European concern. The aforementioned European directive of 2004 institutes an obligation to repair

¹² *Ibid.*

¹³ S Patti, 'Diritto dell'ambiente e tutela della persona' (1980) I (1) *Giurisprudenza Italiana* 859; A. Postiglione, 'L'azione civile in difesa dell'ambiente' [1987] *Rivista Trimestrale di Diritto Pubblico* 303.

¹⁴ Cass., civ. Sez. I, 1995/09/01, n 9211.

¹⁵ Trib. Ven. Sez. III, 2010/02/04 (n 8). Compare: Trib. Mil., Sez. II, 2010/09/16 (n 9).

¹⁶ Corte Cost., 1987/12/30, n 641/1987.

certain ecological damages, such as those caused to water, soil, species and protected natural habitats. The international Court of Justice also recognized environmental damage as such in 2018.¹⁷

In France, following the European text, an Environmental Charter was adopted in 2005, and given of constitutional value. Then the law n 2008-757 of (2008/08/01) relating to environmental liability and the law n 2016-1087 (2016/08/08) for the reconquest of biodiversity, nature and landscapes. The latter establishes new provisions in the French Civil Code itself¹⁸ in the area of liability, immediately following those relating to Aquilian liability.

In the meantime the damage caused to the environment as such, which in France is called '*préjudice écologique pur*' ('pure ecological damage'), i.e. independent of that (material, moral, economic...) caused to people themselves, had to be identified. In 2012, the French Court of Cassation after the sinking of the oil tanker Erika in 1999 off the Atlantic coast mentioned the '*atteinte directe ou indirecte portée à l'environnement, sans répercussion sur un intérêt humain particulier mais affectant un intérêt collectif légitime*'¹⁹ ('direct or indirect damage to the environment, without repercussion on a particular human interest but affecting a legitimate collective interest').

Therefore, one may wonder whether civil liability offers actually a legal framework adapted to the protection of the environment.

On this regard, if civil liability had to adapt itself for the protection of the environment (Part I), environmental liability that results of it seems to have to and to be likely in return to adapt itself even more on the model of civil liability for a better protection of the environment (Part II).

2. Part I : The adaptation of civil liability made for environmental protection.

Formally, while environmental liability has integrated the French Civil Code since 2016, the Italian Environmental Code organizing environmental liability is distinct from the Civil Code. The fact remains that this specific code governs a liability that, as in France, flows into civil liability while involving an adaptation of the latter to achieve the objective of protection of the environment. This can be seen from the conditions (A) and the functions (B) of environmental liability.

A) Conditions

Damage to the environment. First, like the classical civil liability, Part Six of the Italian Environmental Code refers to a damage. Through the legal definition of environmental damage, one perceives however a priori the directly protected legal object: the environment. It is then immediately clear that it deals with a specific type of damage that indeed can be caused to the entire community, whereas the damage of both the Italian Civil Code (of which art. 2043 refers to

¹⁷ *Costa Rica v Nicaragua*, ICJ 2018/02/02 n 150 Rec. ICJ, 15. See also: Y Kerbrat, Sandrine Maljean-Dubois, 'La reconnaissance du préjudice écologique par la Cour internationale de justice' (2018) 3, *Revue Droit Environnement*, 265.

¹⁸ M. Hautereau-Boutonnet, 'Le Code civil: un code pour l'environnement?' (2021) 23 *Rec. Dalloz* 1280.

¹⁹ Cass., crim., 2012/09/25, n 10-82.938. See also: Aude-Solveig Epstein, 'La réparation du préjudice écologique en droit commun de la responsabilité civile', (2016) 21 *Rec. Dalloz* 1236-1240.

'others' too) and the French Civil Code (of which art. 1240 mentions 'others') is caused to one or several specific person(s).

The Italian Council of State thus decided that *'La responsabilità ex art. 2043 cod. civ. si distingue nettamente dall'azione prevista dagli art. 309 e seguenti del d.lgs n. 152 del 2006, in quanto quest'ultima (...) è finalizzata a tutelare il valore 'ambiente', che costituisce l'oggetto di uno specifico interesse pubblico rispetto ai casi di danno o anche di semplice minaccia di danno ambientale'*²⁰ ('The liability under Art. 2043 [of] the Civil Code is clearly distinguished from the action provided for in Art. 309 et seq. of Legislative Decree n 152 of 2006, in that the latter (...) is aimed at protecting the value 'environment', which is the object of a specific public interest with respect to cases of damage or even of mere threat of environmental damage').

However, the main difficulty with respect to environmental damage lies less on its object than on its subject : the 'victim'. In fact, in Italian law as in French law the environment does not constitute a person. Neither are its elements. This is different from many foreign laws in which a river, a tree or a mountain can be endowed with legal personality.²¹ These laws are generally more focused on the collective aspect. In our more individualistic laws, Mother Nature does not constitute a person in the legal sense, any more than do her components (fauna, flora, sites, ambient air, water...). One could thus at first sight be astonished that she can be a victim of a damage in the legal sense of the term in spite of the attacks which can effectively be caused to her, without being able to act in justice.

One could then more surely think of the damage caused to human beings because of the attacks to Nature or to its elements.

It is moreover historically one of the first reflexes of the law in the 'individualistic' societies: in Italy, the Court of Cassation had from the 1970ies, as recalled, used the right of property before civil liability to protect the owners or holders of legally protected interests.

French judges also mobilized the concept of personal damage.²² The damage was thus legally considered as that caused not so much to Mother Nature as to her children: mankind.

However, a major difficulty with this reading grid, which can function when at least two persons are at stake, becomes inoperative when it is not a question of a dispute between two persons holding competing rights.

The damage to the environment as such had therefore subsequently to be identified : in 2012, it was defined by the French Court of Cassation in the Erika case, after that, the French Civil Code in turn enshrined this environmental damage itself since 2016.

However, in the definition of this type of damage we see that the reference to human beings is not totally absent.

In fact, in French law (Art. 1247 C civ.) it deals with *'une atteinte non négligeable aux éléments ou aux fonctions des écosystèmes ou aux bénéfices collectifs tirés par l'homme de l'environnement'* ('a non-negligible damage to the

²⁰ Cons. Stato, 2021/02/08, n 1166.

²¹ See for instance : Mathilde Hautereau-Boutonnet, 'Faut-il accorder la personnalité juridique à la nature ?' (2017) 18 Rec. Dalloz 1040

²² For example, for water: CAA Nantes, 2009/12/01, n 07NT03775; for air: CE 2017/07/12, n 394254; for light pollution: CE 2018/03/28, n 408974.

elements or functions of the ecosystems or to the collective benefits that Man derives from the environment').

In Italian law also, the Environmental Code provides from the outset - art. 2: '*Finalità*' ('Finality') - : '*Il presente decreto legislativo ha come obiettivo primario la promozione dei livelli di qualità della vita umana, da realizzare attraverso la salvaguardia ed il miglioramento delle condizioni dell'ambiente e l'utilizzazione accorta e razionale delle risorse naturali*' ('The primary objective of this decree-law is the promotion of the quality of human life, to be achieved through the safeguarding and improvement of environmental conditions and the conscious and rational use of natural resources'). It also rules at Art. 300 '1. *È danno ambientale qualsiasi deterioramento significativo e misurabile, diretto o indiretto, di una risorsa naturale o dell'utilità assicurata da quest'ultima*' ('1. Environmental damage is any significant and measurable deterioration, direct or indirect, of a natural resource or of the utility secured by it'). Then, in a section on the implementation of the precautionary principle Art. 301 states : '*In applicazione del principio di precauzione (...), in caso di pericoli, anche solo potenziali, per la salute umana e per l'ambiente, deve essere assicurato un alto livello di protezione*' ('In application of the precautionary principle (...) in case of dangers, even only potential ones, for human health and for the environment, a high level of protection must be ensured'). Again, for the sanction of restoration, art. 306 a. 4 of the Legislative Decree 152/2006 states : '*Nelle attività di ripristino ambientale sono prioritariamente presi in considerazione i rischi per la salute umana*' ('In the activities of environmental restoration, the risks for human health are taken into consideration in priority').

This reflects a certain existential difficulty of environmental damage – harm to environment or harm to human beings through environment ? - and could thus raise doubts about the consideration of this environmental damage *per se*.

The utility ensured by the natural resource can be one for the ecosystem - for example, the flora and fauna can be deteriorated by a damage to the air or the ground - but also of course for the human beings themselves since the environment is also theirs.

The Environmental Code also gives categories of environmental damage in accordance to the European Parliament and Council Directive 2004/35/EC : '*the deterioration, in comparison with the original conditions, caused to: a) protected species and natural habitats (...) b) inland waters (...) c) coastal waters and those included in the territorial sea (...) d) land*'. But still, the withdrawn utility of the environment can of course also be to the benefit of human beings themselves since the environment in general is naturally also that of mankind in particular.

As it was recalled by an Italian author : '*L'inquinamento (...) colpisce indistintamente le persone, le cose e la natura*'²³ ('Pollution (...) indiscriminately affects people, things and Nature').

By the way, in France a kind of class action has been provided for the benefit of environmental associations for the reparation of bodily and material harm, that is to say in case of personal harms, resulting from damage caused to the

²³ B Pozzo, 'Danno ambientale: nuove prospettive nel codice dell'ambiente', in F Alcaro, C Fenga, E Moscatti, and others, *Valori della persona e modelli di tutela contro i rischi ambientali e genotossici* (Firenze University Press 2008) 48. See also: R Tommasini, 'Codice dell'ambiente et tutela della persona tra diritti individuali e interessi collettivi', *ibid*, 367-372.

environment²⁴, but not for the reparation of the latter itself.

Moreover, one may wonder whether environmental damage corresponds to an extrapatrimonial or, conversely, a patrimonial conception. The Italian Court of Audit had taken the decision to refer to the '*bellezze naturali del Parco Nazionale d'Abruzzo*'²⁵ ('natural beauties of the Abruzzo National Park'), but had also clearly considered in the Scarlino red muds case environmental damage to be the injury of a collective asset, and thus a '*danno erariale*'²⁶ that is to say a 'fiscal damage' harming public finances.

When the Italian Court of Cassation recognized in 1995 its competence by integrating the matter into civil liability, ruling on facts prior to the specific law of 1986, it nevertheless emphasized its particularity due to its specific object : an asset that is not in commerce.²⁷

It seems therefore to be both a public and private and patrimonial and extrapatrimonial damage.

It appears more precisely that it is above all an extrapatrimonial damage, in particular in the absence of possibility of transfer, seizure or disposal of the environment as such at the disposal of all, but in no way it excludes the fact that the elements of the environment may have an economic value or an impact on private or public patrimonies.

In fact, this is what emerges from a decision of the Italian Constitutional Court, which (also for facts prior to the specific law of 1986) recognized an economic value of the environment, ruling that '*la tendenza dei rischi ambientali naturali a deteriorarsi impone una disciplina che eviti gli sprechi e i danni sicché si determina una economicità e un valore di scambio del bene (...) Questo consente di dare all'ambiente e quindi al danno ambientale un valore patrimoniale*'²⁸ ('the tendency scarcity of natural environmental resources imposes a discipline that avoids waste and damage so that an affordability and exchange value of the asset is determined (...). This allows the environment and thus environmental damage to be given a patrimonial value').

One may also ask whether we should consider a monistic or pluralistic conception of environmental damage : should we consider that there is one or that there are multiple environmental goods and therefore as many potential environmental harms? In Paolo MADDALENA's opinion²⁹, environmental goods are different but linked together, so there would be only one unitary economic and legal good.

The Italian Constitutional Court³⁰ actually considers the environment from a legal point of view as a unitary good, although different components could be protected separately.

The Italian Court of Cassation³¹ also holds that the environment, itself considered, constitutes a good of a public nature, unitary and intangible.

²⁴ Article 89 of French Law n 2016-1547 of November 18, 2016 on the modernization of Justice for the 21st century (C. env., art. L. 142-3-1).

²⁵ Corte Conti, Sez. I, 1975/12/20, n 108.

²⁶ Corte Conti, Sez. I, 1979/10/08, n 61.

²⁷ Cass. Civ. Sez. I, 1995/09/01, n 9211

²⁸ Corte Cost., 1987/12/30, n 641/1987.

²⁹ P Maddalena, 'Il danno all'ambiente tra il giudice civile e il giudice contabile' [1987] Riv. Crit. Dir. Priv., 44.

³⁰ Corte Cost., 1987/12/17, n 641; Corte Cost., 1992/02/24, n 67.

³¹ Cass. Civ. 2008/04/17, n 10118.

According to Alessandro AMATO³², the environment is therefore a synthetic good, superimposed, as shown by especially by Article 19 of Law 349/1986 with the creation of the Ministry of Environment .

However, the Italian legislature, if it considers the environment (in the singular), deals with a '*danno all'ambiente*' ('damage to the environment') in the formula of Part Sixth of the Italian Environment Code, and the French one with '*un préjudice écologique*' ('an environmental damage') at art. 1246 of Civil Code, which means that there are different kinds of environment damages. In France, a Nomenclature of environmental damages was carried out.³³

Threshold of seriousness of the damage. In any case, in order to give rise to civil liability, the damage caused to the environment must exceed a certain degree.

In Italy, even with the mobilization of the right of ownership, it was necessary that the threshold of tolerance be exceeded; and civil liability presupposes an '*ingiusto*' ('unfair') damage : art. 2043 of the Italian Civil Code.

However, since the Law 349/1986, the legislature has not taken up the criterion of 'unfairness' for environmental damage.

For Lucio Valerio MOSCARINI³⁴, this would have been the corollary of the requirement of the specificity of the violated norm, since the special law whose violation was to be sanctioned had in fact already considered that the prohibited element was unfair. But this analysis no longer holds since the 2006 decree-law, which as we shall see no longer requires the violation of a *special* text.

Some authors³⁵ think that the absence of a requirement that the damage should be unfair would constitute a guarantee of a better protection of the environment. Indeed, the fewer characteristics of damage are required, the easier it is to implement environmental liability.

However, today the damage to the environment must be of a particular intensity, which does not seem likely to encourage its recognizing by the judge: it must in fact consist of a '*deterioramento significativo*' ('significant deterioration') according to the Italian Environment Code criterion (art. 300). In France, environmental damage must likewise result from at least one '*atteinte non négligeable*' ('non-negligible impairment') according to the Civil Code criterion (art. 1247).

The two laws are thus close on this point: the Italian positive criterion of 'significant' is in fact answered by the French negative criterion of 'non-negligible'.

In any event, according to some French authors³⁶, this would be a 'superfluous' clarification which would merely enshrine in the law the well established latin adage *de minimis non curat praetor* (the judge doesn't care about insignificant disputes) according to which judges don't have to solve 'minimal cases'.

Yet, the adage actually refers to the *admissibility* not to the *merits* of the action.

³² A Amato, 'La nozione giuridica di ambiente e di bene ambiente. Danno ambientale e tutela civile dell'ambiente', in A Amato, M Balletta, M Montini and others, *Danno ambientale: quantificazione e aspetti procedurali* (Lexambiente 2004), 4.

³³ L Neyret et GJ Martin, *Nomenclature des préjudices environnementaux* (1st edn, Lextenso 2012).

³⁴ LV Moscarini, 'Responsabilità aquiliana e tutela ambientale' [1990] Riv. Dir. Civ. 499.

³⁵ M Richiedei, *La responsabilità della pubblica amministrazione per danno ambientale* (Univ. Ca'Foscari 2014) 50.

³⁶ L Neyret, 'La consécration du préjudice écologique dans le code civil' (2017) 17 Rec. Dalloz 924.

Therefore, if the precision seems unhelpful it is mainly because in matters of civil liability the 'legally reparable' damage already consists in essence of a *non-negligible* or *significant* damage.

Italian civil liability already includes as recalled the general filter of the requirement of unfair damage (art. 2043 of the Italian Civil Code). This can undoubtedly refer to both a quantitative and qualitative assessment. In short, unfair because *disproportionate* or unfair because *inappropriate*.

Some damages are indeed part of life in society, as for example for a student not to graduate from university despite having made great efforts.

In contrast, the requirement of 'significant' environmental damage seems to refer exclusively to a quantitative assessment.

This appears to be no less than an unnecessary precision in relation to the general requirement of unfair damage by traditional civil liability.

Moreover, all the exceptions expressly provided for by Italian law to the reparability of environmental damage show perfectly that it is simply a matter of taking in consideration only that which is unfair. Article 303 of the Italian Environmental Code, entitled 'exclusions', in fact lays down a series of exceptions to the principle of reparability of environmental damage: environmental damage or imminent threat of such damage caused by acts of armed conflict, sabotage, acts of hostility, civil war, insurrection, or natural phenomena of an exceptional, unavoidable and uncontrollable nature, etc.

Thus, for instance the destruction by missile of an element of the Russian military fleet penetrating Italian air or sea space without authorization would of course have significant consequences for the environment, but no environmental liability could for as much be implemented.

At the most, it can be noted that with regard to these exceptions it is the text which upstream makes the distinction within environmental damage, between unjust and just damage; whereas it is essentially the judges who will have downstream to assess the question of the significant intensity of environmental damage.

Although the French Civil Code on the one hand does not contain such a precision (its art. 1240 refers indeed to any damage), French doctrine on the other hand integrates it perfectly by considering following the judges (that do so in a more implicit manner) that it is indeed socially unjust damage which is reparable. For example, the French Court of Cassation has already ruled that the revelation of trivial facts of private life, such as a celebrity's outing to a restaurant, does not constitute a source of liability.³⁷ The requirement of environmental damage resulting from a non-negligible infringement thus appears once again to be largely unnecessary.

Such legislative clarifications which follow the position of the courts but are not in the European directive of 2004 seem to be explained by the fear aroused by the relatively recent introduction of environmental liability into the law (in France, in 2012 and in 2016; in Italy, since the 1970s, then in 1986 and in 2006). It deals indeed with a new type of potentially frequent damage, the invocation of which could give rise to a fear of a clogging up of the jurisdictions. In a context of insufficient judicial budgets, an overly broad definition of environmental damage

³⁷ Cass., civ. I, 2002/04/3, n 99-19.852.

would also have constituted a potential additional source of slowness of the justice dans then condemnation of the concerned State for violation of Article 6 of the European Convention on Human Rights.

In any event, the significant character or the absence of negligibility seems to constitute an intrinsic element of the damage, and not a specific condition of environmental damage.

However, if it seems unnecessary, this legislative precision concerning environmental damage does not appear to be unconstitutional. Indeed, in France the Constitutional Council has ruled that this limiting precision of the reparability of environmental damage was in conformity with the Constitution.³⁸

In any case, after examination, environmental damage appears to be an unjust damage. Like that required by traditional civil liability. There is thus a solubility, in this respect, of environmental damage in the general category of damage and thus, at least from this point of view, of environmental liability into civil liability.

The real specificity of the environmental damage seems to be its duality of damage either to the environment as such, devoid of legal personality, or, where applicable, through harm to the utilities of the environment, especially for human beings.

Event giving rise to liability. Although it recognized environmental damage earlier than French law, Italian law hesitated on the question of the cause of environmental liability.

Indeed, the 1986 law required fault or fraud (avatars of the culpa and dolus of Roman law and equivalent respectively to French quasi-delicts and delicts) for the implementation of environmental liability for the author of the damage, especially through the disregard of a special text. From this point of view, this law was in a way 'transparent' because it did not establish any fact specifically generating liability: it effectively referred to the classic conditions of civil liability (fault or fraud of art. 2043 of the Italian Civil Code) or to already existing texts.

Special texts such as the Ronchi Decree-Law n 22/1997 on environmental clean-up and the Decree-Law n 224/2003 on the deliberate release of GMOs into the environment had, in these respective fields, retained a strict liability, disconnected from fault or fraud.

While the Act of 86 could be seen on the one hand as *transparent* in that it referred to the fault or the fraud already present specially in the Italian Civil Code, it could also be seen on the contrary as *opaque* in that, in effect, it appeared to hinder strict liability (i.e. without any fault nor fraud and also possible in certain circumstances in the Italian Civil Code) at least if the latter was not provided for in a text specific to environmental liability.

Subsequently, albeit for events occurring before the 1986 law, the Italian Court of Cassation³⁹ also decided to apply strict liability for dangerous activities. Once again, it was thus classical civil liability and its instruments that were mobilized for the protection of the environment.

³⁸ Constitutional Council 2021/02/05, 2020/881 QPC. See also : F Savonitto, 'La question prioritaire de constitutionnalité sur le préjudice écologique. Une « petite » décision du Conseil constitutionnel' (2021) 16 Act. Jur. Dr. Adm. 926.

³⁹ Cass. Civ., n. 9211/95.

The choice of strict liability was also made by the above-mentioned European directive of 2004. It is therefore also the choice which, after further hesitation to which we shall return, was partially endorsed by the Italian environmental code, which retains strict liability for the activities specifically mentioned in it.

At first sight, this appears to be consistent with the principles laid down in the same code, according to which, in article 3 ter on the 'principio dell'azione ambientale' ('environmental action principle') : '1. *La tutela dell'ambiente e degli ecosistemi naturali e del patrimonio culturale deve essere garantita (...)*' ('1. The protection of the environment and natural ecosystems and cultural heritage must be guaranteed (...)'). In fact, the *guarantee* seems to presuppose that protection of the environment, when this is ensured by civil liability, is irrespective of any subjective behaviour and thus fault or fraud on the part of the person responsible.

However, are the facts that give rise to this strict liability under the Italian Environmental Code really specific compared to those that give rise to an equally strict liability under the Italian Civil Code? In fact, if we analyze the activities subject to strict liability listed in Appendix 5 of Part 6 of the Italian Environmental Code, we realize that the vast majority of them could be covered by the liability, without any fault having to be proven, for dangerous activities (art. 2050 of the Italian Civil Code), or even for things custody (art. 2051 of the Italian Civil Code). With regard to things in one's custody, one can indeed mention point 2 about '*Operazioni di gestione dei rifiuti, compresi la raccolta, il trasporto, il recupero e lo smaltimento di rifiuti (...)*' ('Waste management operations, including collection, transportation, recovery, and disposal of waste (...)').

Regarding dangerous activities, we can mention point 1 and think about several activities subject to authorization or registration such as '*Funzionamento di impianti soggetti ad autorizzazione, conformemente alla direttiva 96/61/Ce del Consiglio, del 24 settembre 1996, sulla prevenzione e la riduzione integrate dell'inquinamento*' ('Operation of installations subject to permit in accordance with Council Directive 96/61/EC of September 24, 1996, concerning integrated pollution prevention and control') , point 2 about the '*Operazioni di gestione (...) di rifiuti pericolosi*' ('Management operations (...) of hazardous waste') but also point 3 about '*Tutti gli scarichi nelle acque interne superficiali che siano soggetti ad autorizzazione preventiva conformemente alla direttiva 76/464/Cee del Consiglio, del 4 maggio 1976, concernente l'inquinamento provocato da certe sostanze pericolose scaricate nell'ambiente idrico della Comunità.*' ('All discharges to inland surface waters that are subject to prior authorization in accordance with Council Directive 76/464/EEC of May 4, 1976, on pollution caused by certain dangerous substances discharged into the aquatic environment of the Community', or again to '4. All discharges of substances into groundwater that are subject to prior authorization in accordance with Council Directive 80/68/EC of December 17, 1979, on the protection of groundwater against pollution caused by certain dangerous substances').

Thus the event giving rise to environmental liability appears to be a dangerous event.

The Italian Environmental Code provides for subsidiary liability for fault or fraud for other activities than those specifically listed.

On the one hand, one may wonder about this element : would it not have been enough to refer to the classic civil liability and in particular to article 2050 of the

Italian Civil Code?

On the other hand, this absence of a reference must have the consequence that it is environmental damage as conceived by the Italian Environmental Code, that is to say, a *significant* harm, and not as it might be understood by the Italian Civil Code, an *unfair* damage in a general way, that is to be required.

The specificity in relation to liability under the Civil Code could thus be found not so much in the operative event as in the damage, although the latter appears as we have seen to be truly specific only in its nature as damage caused to a non-personified entity, and not insofar as it requires a threshold of gravity.

In any event, while there may be a fairly specific regime of environmental liability with respect to damage, there is no homogeneous regime in Italy with respect to the event giving rise to liability. From this point of view, French law seems both less hesitant and less heterogeneous, since the provisions resulting from the aforementioned law of 2016 do not require fault in the case of environmental damage for the implementation of civil liability.

In France, it is then a strict liability, and thus more homogeneous as to the generating fact (even if this one can in fact be culpable, the fault and a fortiori its demonstration by the plaintiff is not legally required).

One may also ask whether the Italian civil code can be invoked outside the specific cases provided for in the Italian environmental code.

In any case, while there may be a specific system of environmental civil liability as far as damage is concerned, there is no uniform system in Italy, in this field, if one looks at to the event that gives rise to liability.

This is not exactly the same choice made by the French legislature, which in fact in general unlike Aquilian liability (art. 1240 Civil Code) does not require fault in order to implement environmental liability (art. 1246 et seq. of the Civil Code). It is therefore in France a unique strict liability.

Causal link. Italian Law 349/1986 required proof not only of fault or fraud, but also of the causal link between the fault or fraud, resulting from the violation of a special law, and the damage caused to the environment (even though the latter could be deduced from the violation of the special law).⁴⁰

Contrawise, the Ronchi Decree-Law of February 8, 1997 didn't require any proof of fault or fraud, nor of the causal link between the exceeding of the limits of acceptability of soil contamination set by the Minister of Environment. The Italian Environment Code opts for a strict liability where the causal link is presumed for the only activities listed.

It is very difficult to establish such a causal link. On the one hand, because the environmental damage may appear several years after the event that caused it. On the other hand, and perhaps above all, because environmental damage, except when a person such as a company accidentally pollutes a localized element, may result from a plurality of facts (which may have occurred over several years) and from a plurality of actors. Let's think about the example of the pile of plastic waste in the oceans - the infamous 6th continent - in which we all participated. Who can and should be considered responsible for the disappearance of sea turtles suffocating by plastic? The same is true for lawful

⁴⁰ A. Amato, 'La nozione giuridica di ambiente e di bene ambiente' (n 32) 8.

activities such as driving: can and should each driver be held responsible for the premature deaths caused by air pollution? Beyond the proof of the existence of the causal link, the question of the distribution of responsibility appears quite delicate between: drivers of individual or collective vehicles? users of coal heating? The State itself which authorized and did not regulate enough these activities (all the more so in legal systems which admit the theory of equivalence of conditions, i.e. considering as the cause of the damage any event, whatever its intensity, which has participated in it: both the State and citizens could thus be considered to be different causes of pollution. By the way we can sometimes see a change of course of the legislation, for example in France with a recent decree prohibiting heating on café terraces)?⁴¹

Not to mention the regenerative capacity of nature, which can erase some environmental damage or part of it. The situation is therefore unusual where it is the victim who not only can erase all or part of the injury but also can hide the causal link which appears indeed delicate to establish.

In order to alleviate this difficulty in part, strict liability may appear to be more appropriate since it does not presuppose proof of a causal link, which is in fact presumed. This is how it was implemented by the Court of Cassation in 1995⁴² for acts prior to the 1986 Law.

Strict liability is also a way of focusing on the victim by putting in the background the conduct of the person responsible.

However, in order to avoid conferring too broad a scope of application on a nascent and in this respect potentially suspect environmental civil liability, the Italian Environmental Code has formally excluded (art. 303,1, h) the '*danno ambientale o [la] minaccia imminente di tale danno causati da inquinamento di carattere diffuso, se non sia stato possibile accertare in alcun modo un nesso causale tra il danno e l'attività di singoli operatori*' ('environmental damage or [the] imminent threat of such damage caused by pollution of a diffuse character, if a causal link between the damage and the activity of individual operated could not be established in any way').

In France, the law (art. L. 161-2, paragraph 7 of the Environmental Code, as it results from the aforementioned law of 2008), likewise expressly excludes from the scope of environmental liability damage caused by pollution '*à caractère diffus*' ('of a diffuse nature') such as air pollution, unless a causal link between the damage or its threat and the activities of an operator is established by the prefect. It is therefore up to the administrative authority to establish a causal link between an activity and environmental damage. But the aforementioned French law of 2016 does not lead in the Civil code to such an exclusion of liability in case of pollution of a diffuse nature.

B) Functions

Damage is a *sine qua non* condition of extra-contractual civil liability (art. 1240

⁴¹ Décret n 2022-452 du 30 mars 2022 *relatif à l'interdiction de l'utilisation sur le domaine public en extérieur de systèmes de chauffage ou de climatisation* (prohibiting the use of outdoor heating or air conditioning systems on public property), after Loi n 2021-1104 du 22 août 2021 *portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets* (combating climate change and building resilience to its effects).

⁴² Cass. Civ., N 9211/1995 (n 7).

et seq. of the French Civil Code and art. 2043 et seq. of the Italian Civil Code), unlike other forms of liability, and in particular criminal liability. Extra-contractual civil liability thus traditionally fulfils an essential function of reparation for this damage.

However, with the evolution of the matter, the Italian Court of Cassation⁴³ has now come to identify three functions of civil liability: compensatory, but also preventive and punitive.

Environmental liability seems not only to correspond to these three identified functions but also to participate to the aforementioned evolution.

Compensatory function. First of all, is *reparation* really possible in environmental matters? With regard to the possibility of reparation, the European Directive 2004/35/EC of April 21, 2004 on environmental liability refers in particular to the reparation of environmental damage in its very title. Like the legislature in France: art. 1246 of the French Civil Code states that : '*Toute personne responsable d'un préjudice écologique est tenue de le réparer*' ('Any person responsible for ecological damage is obliged to repair it'), on the model of art. 1240 : '*Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer*' ('Any act that causes damage to another one obliges the person by whose fault it occurred to repair it'), but with the following precision of art. 1249 : '*La réparation du préjudice écologique s'effectue par priorité en nature*' ('The repair of ecological damage is carried out by priority in kind'). Damages can only be envisaged where reparation in kind is impossible or insufficient. This clarification of the mode of reparation of environmental harm appears to be welcome in France in comparison with the traditional provisions of the Civil Code which do not specify the form of reparation of harm in a general way (art. 1240). Otherwise, reparation in kind would certainly appear to be perfectly conceivable but not necessarily constitutive of a principle.

In Italy, the provisions of the Civil Code relating to classic extra-contractual civil liability envisage compensation ('*risarcimento*', art. 2043 et seq.). This is done in principle by way of equivalence, i.e. with an allowance, since reparation in kind must 1° first of all be requested by the victim, 2° then must be possible and, 3° finally, must not be excessively onerous for the debtor (art. 2058).⁴⁴ Reparation in-kind thus appears to be an exception.

Conversely, in environmental matters, it is now essentially and by right a reparation in kind (art. 311 of the Italian Environmental Code). That is to say that reparation in kind has become the principle.

Law 349/1986 had made it a subsidiary method of reparation, envisaging the reparation in kind only in case of *material* but maybe also *economic* (the question was indeed discussed of that form of reparation in case of excessive cost) possibility.

On the contrary, the Ronchi Decree-Law n 22/1997 and the Decree-Law n 224/2003 on GMOs had generalized the compensation in-kind in their respective

⁴³ Cass. Civ., 2017/07/05, n 16601.

⁴⁴ « Il danneggiato può chiedere la reintegrazione in forma specifica, qualora sia in tutto o in parte possibile. Tuttavia, il giudice può disporre che il risarcimento avvenga solo per equivalente, se la reintegrazione in forma specifica risulta eccessivamente onerosa per il debitore » («The aggrieved party may seek reparation in kind if it is possible in whole or in part. However, the court may order that compensation be made only by equivalent, if repairing in kind is excessively burdensome for the debtor»).

fields.

Judges for their part had made reparation in kind a natural way of environmental damage. For example, a decision of the Lombardy Regional Administrative Tribunal stated for facts prior to the adoption of the Environmental Code, with regard to the responsibility of a producer for the contamination of a site: *'è l'articolo 2050 c. c. ad imporre al responsabile di attivarsi al fine di porre in essere atti e comportamenti unitariamente finalizzati al recupero ambientale del sito'*⁴⁵ (*'it is Article 2050 c. c. that requires the responsible party to take action in order to put in place acts and conduct unitarily aimed at the environmental recovery of the site'*).

Despite some controversy, money can be combined with reparation in kind. In fact, Article 311 of the Italian Environmental Code refers to *'il risarcimento del danno ambientale in forma specifica e, se necessario, per equivalente patrimoniale'* (*'the compensation for damage environmental in kind and, if necessary, by pecuniary equivalent'*). For example, when the reparation in kind occurs several years after the damage has been produced and it is therefore necessary to repair the harm caused by the unavailability of the natural resource.⁴⁶

In any event, today the reasons for the priority of this reparation in kind are quite understandable: the environment and its components have also and may be above all, as recalled, an extrapatrimonial value. Therefore, when reparation can in principle be made by monetary equivalent for damage caused in general in an economically liberal society where money constitutes a reference standard, it must on the other hand be made in kind when it is a question of environmental damage caused to a value that is in particular extrapatrimonial and of general and not private interest.

Moreover, it can be very difficult to put a figure on environmental damage, such as the destruction of animal species. Damages that are only symbolic would only devalue the object of the protection, like the request in the *'Affaire du Siècle'* ('Case of the Century') in France where, as we will come back to, the associations that were plaintiffs asked for symbolic damages.

From this point of view, the 'polluter pays' principle resulting from European law (in particular from the Single European Act and the aforementioned European directive of 2004), which is very much imbued with an economic market logic, but which is also taken up by the Italian environmental code - art. 3 ter: *'Principio dell'azione ambientale'* ('Principle of environmental action'- does not therefore appear to be totally adapted to environmental liability. Indeed, a 'polluter repairs' principle would seem to be more relevant.

Furthermore, to ensure the effectiveness of reparation in kind, Italian law provides for a substitution mechanism by the Minister of Environment in case of default by the person responsible, who can then turn against the defaulting party within a period of 5 years.

However, reparation in kind does not always appear to be an appropriate solution. This is particularly true in view of the time that may have elapsed between the production of the damage and the pronouncement of the judicial

⁴⁵ TAR Mil., Sez. I, 2013/10/03, n 2222.

⁴⁶ Cass. 2008/04/17, n 10118 : 180 000 euros to pay in addition to the repair in kind of Piave river damaged 9 years before.

solution. This is particularly evident in the Erika case in France which occurred in 1999, 13 years before the decision of the French Court of Cassation...

The reparation by monetary equivalent provided for as a subsidiary rule in Italian law as in French law thus appears inevitable and even welcome. Except that it may remain delicate to put a figure on extrapatrimonial damage such as that caused to the environment.

Moreover, even if it is fulfilled in a manner adapted to its purpose, is the compensatory function of environmental civil liability sufficient?

Preventing function. For the above-mentioned reasons of extrapatrimonial value, but also because prevention is often less onerous than reparation in kind or by equivalent, environmental liability also seems to have to fulfil a function of preventing from damage. The question of the autonomy of an action in prevention in relation to an action in civil liability has been raised.⁴⁷ However, here again, the aforementioned European directive of 2004 now also expressly refers to *prevention* in matters of environmental *liability*. The preventive action is thus now clearly integrated into the very field of environmental liability. In line with the European text, the Italian Environmental Code, after having established a regime applicable in particular to the imminent threat of environmental damage (art. 298 bis 1, a and b), provides in this respect concretely (art. 3041) that 'the operator concerned' shall bear the costs of prevention of the environmental damage whose imminent threat is verified. This is indeed an aspect of liability since, on the one hand, it is necessary that there is an imminent threat of environmental *damage*, which is the very condition of liability, and, on the other hand, that the person *responsible* bear the costs of prevention.

The French Civil Code, which provides for an action to prevent damage or its aggravation, envisages the question in a similar way but from the opposite angle, no longer of the person responsible but of the victim or in any event the payer, by providing (art. 1251) that '*Les dépenses exposées pour prévenir la réalisation imminente d'un dommage, pour éviter son aggravation ou pour en réduire les conséquences constituent un préjudice réparable*' ('The expenses incurred in preventing the imminent occurrence of damage, in avoiding its aggravation or in reducing its consequences constitute compensable loss'). This function of prevention is understood by the idea that 'an ounce of prevention is worth a pound of cure' - in Italy: '*meglio sudare che tremare*' ('rather sweat than tremble') and in France '*mieux vaut prévenir que guérir*' ('prevention it is better than cure') - especially in the case of environmental damage which unlike the classic damage of civil liability concerns the entire community.

Besides, that is not devoid of economic considerations since the cost of prevention can be much lower than the one of repair.

The technique of solidarity, which had been envisaged for a time in the field of environmental civil liability, as we shall return to, also ensured according to some '*a greater deterrent to behaviours of misconduct and an incentive to take appropriate preventive and precautionary measures in order not to incur environmental damage*'.⁴⁸

In addition to this prevention in the strict sense of the term (of such a nature

⁴⁷ A Amato, La nozione giuridica di ambiente e di bene ambiente' (n 32)

⁴⁸ M Richiardi, La responsabilità della pubblica amministrazione per danno ambientale (n 35) 52.

as to avoid damage or its aggravation), civil liability for the protection of the environment may also in France reveal an *interruptive* function (as in the '*Affaire du siècle*' case). In this case, it is no longer a question of avoiding the production or the aggravation of the damage, but simply its continuation. This is done by the injunction of the judge. The advantage of this is that it may be accompanied by a penalty payment, as provided for in article 1250 of the French Civil Code.

Punitive function. In several respects, the punitive function seems to be little present in Italian and French environmental liability laws.

First of all, no punitive damage known in the Common law is laid down in this matter, either by French law or by Italian law. Whether it is in the form of a specific award or a monetary equivalent, reparation is never greater than the damage actually caused.⁴⁹ In practice, it may even be less, because of the absence of solidarity resulting from the law between co-responsible for the same environmental damage.

Also, because reparation by equivalent, in which there may be a desire to punish, is now the exception: judges cannot therefore punish anti-environmental behavior by fixing punitive damages. Moreover, even when reparation in kind is exceptional, in the law 348/1986, it could only be implemented in the absence of impossibility and also in absence of economic cost according to some.

Secondly, because since the 2006 decree-law, it is a question of a strict liability, thus disconnected from a wrongful or fraudulent behaviour of the person responsible that would be to punish. It's then not really a question of 'punishing' the person responsible by impoverishing him or her in order to repair the environment at all costs, in order to 'enrich' Nature!

Moreover, because reparation in the monetary form of equivalent damages is rarely combined with reparation in kind. The Italian Court of Cassation in fact ruled that '*non residua alcun danno ambientale economicamente quantificabile e quindi risarcibile - né in forma specifica, né a maggior ragione per equivalente - ogniqualevolta, avutasi la riduzione al pristino stato, non persista la necessità di ulteriori misure sul territorio reso oggetto dell'intervento inquinante o danneggiante*'⁵⁰ ('no economically quantifiable environmental damage remains and is therefore compensable - neither in kind, nor a fortiori by equivalent damages - whenever, having had the reduction to the pristine state, the need for further measures on the territory made the object of the polluting or damaging intervention persists'). The possible cumulation of reparation in kind and reparation by monetary equivalent does not correspond to any punishing purpose, but to a compensatory function in case of damage resulting specifically from the unavailability of the resource before its reparation in kind.

In addition, since the aforementioned Italian decree-law of 2006 creating the Environmental Code, it is now the more often a question of strict liability and thus one disconnected from any fault or fraud: the conduct giving rise to liability therefore does not appear any more to require punishment.

Eventually, because, unlike the general law of civil liability under the Italian

⁴⁹ Showing that Italian environmental law does not provide punitive damages at all in spite of appearances: G Spoto, 'I danni punitivi e il risarcimento del danno ambientale', in F Alcaro, C Fenga, E. Moscatti and others, *Valori della persona e modelli di tutela contro i rischi ambientali* (n 23) 349, 363.

⁵⁰ Cass. Civ., Sez. III, 2015/08/13 n 16806.

Civil Code (art. 2055), joint and several liability is excluded in environmental liability in cases where there is more than one person liable. This does not seem likely to punish one of the co-responsible persons for the damage which he has contributed to causing by his participation. One can think that, when it provided for solidarity in this matter, the Italian legislature accentuated compensatory function of the environmental liability extending to the maximum the area of the persons liable for the consequences of the environmental damage ; but it can be added that it is also the punitive function that emerges when a person, whose capacity as joint and several debtor is retained, can be made to pay for the other co-responsible parties.⁵¹ Both in terms of the obligation to pay the debt, but also in terms of the contribution to the debt against the other co-responsible persons. In fact, the Italian Civil Code expressly provides for a distribution according to the seriousness of the respective fault and the consequences thereof.

The absence of joint and several liability may appear to be questionable in the case of liability that is precisely of a collective nature: environmental damage is collective and thus public (as Italian law perfectly shows putting Minister of Environment at the center of the environment liability as we'll see in Part 2) because it is caused at the same time to elements of Nature, humans and other beings, and even the event that gives rise to that liability the most often emanates precisely from a plurality of persons.

For Alessandro AMATO⁵², this absence of solidarity would be similar to the Common law market share liability, in which a person is liable only for his market share. However, on analysis, the two systems of Civil law solidarity, on the one hand, and Common law market share liability, on the other, appear to be likely to be combined for greater efficiency when the parties responsible actually intervene in a same market. For example, automobile manufacturers. In this case, the responsible parties could each be liable for the totality of the environmental damage, with the onus on the person or persons convicted to turn against the co-responsible persons to recover the share that the latter must assume. A share then determined according to the one of each operator on the anti-environmental market, and no longer according to the seriousness of the respective faults or their consequences, since as recalled it deals with a strict liability regardless faults and frauds.

In any case, in 1995 but for facts prior to the adoption of Law 349/1986, which expressly excludes it, the Italian Court of Cassation retained passive solidarity in environmental liability; in this case between, on the one hand, the producer and, on the other hand, the manager, transporter and sorter of polluting products.⁵³

Some decisions of regional administrative Tribunals had also opted for solidarity.⁵⁴

In France, the legislative provisions relating to environmental civil liability are silent on solidarity. Thus, unlike Italian law there is no specificity in relation to traditional French civil liability where the jurisdictional cases retain, in the absence of legal or contractual solidarity, an obligation *in solidum* between the various

⁵¹ G. Spoto, 'I danni punitivi e il risarcimento del danno ambientale' (n 49).

⁵² A Amato, 'La nozione giuridica di ambiente e di bene ambiente' (n 32), 26.

⁵³ Civ. Sez. I, 1995/09/01, n 9211.

⁵⁴ TAR Lombardia, Milano, Sez. I, 2013/07/25, n 195 (in this case between all operators of collection and management of toxic waste).

persons responsible for the same damage. Such obligation is a substitute for passive solidarity, characterised by its principal effects (each of the persons is liable for the whole of the debt to the victim) but without its secondary effects (in particular, an action against one of those persons does not interrupt the running of the statute of limitations in relation to the others). The purpose of this obligation in solidum is to protect the victim against a division of the proceedings against the responsible people; but the latter do not appear to be punished because the person ordered to compensate for the harm can turn against the co-responsible persons to make them pay their share of the debt of responsibility.

However, in several other respects, a punitive function of environmental liability appears.

First, reparation by monetary equivalent is provided for only if reparation in kind is impossible. Thus, such reparation in kind may in practice prove extremely onerous for the responsible: it can be avoided only in case of impossibility, understood like an *absolute* one i.e. for everyone, and not a *relative* impossibility (especially in relation to the financial situation of the responsible person).

Secondly, even if it does not require fault or fraud, strict liability does not necessarily exclude their existence, and thus a punitive dimension of the judicial decision. Better still, strict liability makes it possible to condemn a responsible person more easily than in the case of liability for fault or fraud, and thus to punish more widely unlawful conduct.

The Italian Court of Cassation⁵⁵ has moreover expressly recognized this punitive function of liability for damages caused to the environment as such.

In some respects, even if it excluded solidarity Italian law 349/1986 was more punitive. It provided for environmental liability in the case of fault or fraud, and was thus conducive to the punishment of subjective behaviors. It also referred to the benefit derived by the responsible party and the seriousness of the latter's fault. Profit and seriousness thus reflect a reprehensible subjective behavior to the detriment of the environment, and therefore a punitive function of environmental liability.

In any event, the three functions - compensatory, punitive and preventive - of civil liability clearly identified by the Italian Court of Cassation are still relevant today and more than ever in environmental liability. These functions would then benefit from being expressly mentioned by the legislature itself in France as in Italy.

Anyway, with some adaptations civil liability provided a framework for the environment liability that uses its instruments. However, this environmental liability now seems in turn to need to be adapted more closely to the model of civil liability in order to protect the environment more effectively.

3. Part II: The adaptation of environmental liability to make on the model of civil liability.

There are undoubtedly several avenues for improving environmental civil liability. Two that result from the comparison with classical civil liability appear of

⁵⁵ Cass. Civ. 2008/04/17, n 10118.

particular interest: on the one hand, with regard to the persons who can be plaintiffs (A) and, on the other hand, with regard to the persons who are liable (B).

A) Plaintiffs

Who can act? Historically, Italy considering environmental damage as public harm to the State, has opted from the outset for the competence of the latter: from the first decisions of the Court of Auditors in the 1970s, then with the Environmental Code of 2006, passing through Law 349/1986, the Ronchi Decree and the 'GMO' legislative decree.

Various theories have been put forward in doctrine to explain that.

First, the thesis of a subjective public right of the State, according to which it is the latter that must be considered both the holder and the beneficiary of the right to take legal action in case of environmental damage. Indeed, the State can be considered as having an interest in the preservation of the environment. However, even if only the State is invested with the right to act, of which it is thus the sole *holder*, it is easy to understand that it cannot indisputably be considered as the sole *beneficiary*. Indeed, the environmental damage concerns the entire community: everyone breathes the ambient air, consumes and uses water as well as the fruits and products of the earth...

Thus, several other theses have been put forward: that of a power of the State to act in the interest of the whole community⁵⁶, and that of a sort of representation of the people by the State⁵⁷ or even of a particular class action.⁵⁸

Anyway, the Italian Council of State ruled that '*Il bene tutelato in via diretta dal legislatore del decreto legislativo n. 152 del 2006 è l'interesse alla tutela ambientale posto in capo al Ministero dell'ambiente*'⁵⁹ ('The asset directly protected by the legislature of Legislative Decree n 152 of 2006 is the interest in environmental protection placed on the Ministry of Environment').

In spite of that, the Italian Environmental Code through its art. 299⁶⁰ seems to make the power to sue not a personal right but a function and also a duty of the State through the Ministry of Environment.

As far as other public authorities are concerned, the 1986 law was ambiguous because on the one hand it allowed public authorities to bring legal actions, but on the other hand it reserved the right to monetary compensation to the State. The Italian Court of cassation had adopted a bold solution by considering that the protection of their territory constitutes for Regions '*uno loro diritto della personalità*'⁶¹ ('one personal right of theirs', including in Italy and France the one to be left alone).

The Italian Council of State nevertheless confirmed in its part that under the

⁵⁶ GG Greco, 'Danno ambientale e tutela giurisdizionale', [1988] *Sanità Pubblica* 355.

⁵⁷ P Maddalena, 'Il danno all'ambiente tra il giudice civile e il giudice contabile' (n 29).

⁵⁸ A Amato, 'La nozione giuridica di ambiente e di bene ambiente' (n 32).

⁵⁹ Cons. Stato, 2021/02/08, n 1166 (n 20).

⁶⁰ "*Il Ministro de ll'ambiente e della tutela del territorio e del mare esercita le funzioni e i compiti spettanti allo Stato in materia di tutela, prevenzione e riparazione dei danni all'ambiente*" ("Minister of environment shall exercise the functions and duties incumbent on the State in the field of protection, prevention and repair of environmental damage").

⁶¹ Cass. Pen. Sez. III, 1993/06/15, n 9727.

law in force the State monopoly: *'La responsabilità ex art. 2043 cod. civ. si distingue nettamente dall'azione prevista dagli art. 309 e seguenti del d.lgs n. 152 del 2006, in quanto quest'ultima (...) è finalizzata a tutelare il valore "ambiente", che costituisce l'oggetto di uno specifico interesse pubblico rispetto a casi di danno o anche di semplice minaccia di danno ambientale'*⁶² ('Liability under Article 2043 of the Civil Code is clearly distinguished from the action provided for in Articles 309 et seq. of Legislative Decree n 152 of 2006, in that the latter (...) is aimed at protecting the value 'environment', which is the subject of a specific public interest with respect to cases of damage or even the mere threat of environmental damage').

Thus, Italy which has chosen to place the State in the forefront in this area has reserved a very limited role especially for the environmental associations. In 2000, they were granted a limited power to propose liability action to the Municipalities and Provinces, which the latter two had got in 1986. This was subject to certain conditions of purpose, continuity and interregional or national vocation. The reform of 2006 put the State back as the only holder of the right to act in environmental liability. It was considered as one of the manifestations of the regression of the Italian law regarding the protection of the environment.⁶³ In any case the conformity appears doubtful with the European directive of 2004 which foresees a role for the non-governmental organizations with regard to the collective interests at stake. From this point of view, it is not certain that Italian law is fully compliant with European law.⁶⁴

Moreover, the state of Italian law does not appear to be fully in line with the principle of subsidiarity⁶⁵, which in a liberal system must lead to the competence of the State in non-regalian matters (such as the environmental protection) only in the absence of private initiatives.

In any case, this has not been judged contrary to the Constitution: the Italian Constitutional Court has in fact ruled that *:'La scelta di attribuire all'amministrazione statale le funzioni amministrative trova una non implausibile giustificazione nell'esigenza di assicurare che l'esercizio dei compiti di prevenzione e riparazione del danno ambientale risponda a criteri di uniformità e unitarietà, atteso che il livello di tutela ambientale non può variare da zona a zona e considerato anche il carattere diffusivo e transfrontaliero dei problemi ecologici, in ragione del quale gli effetti del danno ambientale sono difficilmente circoscrivibili entro un preciso e limitato ambito territoriale'*⁶⁶ ('The decision to assign the administrative functions to the state administration finds a not implausible justification in the need to ensure that the exercise of the tasks of preventing and repairing environmental damage meets the criteria of uniformity and unity, given that the level of environmental protection cannot vary from area to area and also considered the diffusive and transboundary nature of ecological problems, due to which the effects of environmental damage are difficult to circumscribe within a precise and limited territorial scope').

⁶² Cons. Stato, 2021/02/08, n 1166 (n 20).

⁶³ U Salanitro, 'Il risarcimento del danno all'ambiente: un confronto tra vecchia e nuova disciplina', in F Alcaro, C Fenga, E Moscatti and others, *Valori della persona e modelli di tutela contro i rischi ambientali e genotossici* (n 23) 331, 342.

⁶⁴ F Caringella, L Buffoni, *Manuale di diritto civile* (Dike giuridica 2018), 434.

⁶⁵ MP. Giracca, *Danno ambientale*, 587.

⁶⁶ Corte Cost., N 235/2009.

It later reiterated the compliance with the Constitution.⁶⁷

However, it is not forbidden to consider that in reality it is mainly up to the judge downstream to make homogeneous the consequences of environmental damage, regardless of the quality upstream of the plaintiff to the action. Indeed, whether it is the State or an association which acts to denounce the damage caused to the ambient air, there is no reason why this same damage should be treated differently by the judge according to the person who has seized the court.

In Italian law, environmental associations can intervene in legal proceedings initiated by the State, and even challenge the legality of administrative acts or constitute themselves civil parties in cases of environmental crimes.⁶⁸

But can associations, not recognized as holders of a right to implement environmental liability by the Environmental Code, nevertheless act on the basis of classic civil liability? Could the special law (the Environmental code) be circumvented by means of the general law (the Civil code)?

In fact, it seems to be a matter of articulation. In this respect, the jurisprudence of the Italian Court of Cassation in particular repeats that environmental damage has a triple dimension, personal, social and public.

The first concerns species the health of the person; the second, the interactions between people; the third, the interest in the protection of the environment considered in itself that is called in France '*préjudice écologique pur*' ('pure environmental damage'). Thus, associations can act for the first dimension, personal, and if anything for the second, social, while the last dimension, public, is in Italian law unquestionably a State monopoly.

Any other person will have to prove a personal harm.

Several decisions can be cited, for instance one ruling that: '*Il risarcimento del danno ambientale, in sé considerato come lesione dell'interesse pubblico alla integrità e salubrità dell'ambiente, è previsto e disciplinato soltanto dal D.Lgs. n. 152/2006, sicché il titolare della pretesa risarcitoria per tale tipo di danno è esclusivamente lo Stato, in persona del Ministro dell'ambiente; tutti gli altri soggetti, singoli o associati, ivi compresi gli Enti pubblici territoriali e le Regioni, possono invece agire, in forza dell'art. 2043 c. c., per ottenere il risarcimento di qualsiasi danno, ulteriore e concreto, che abbiano dato prova di aver subito dalla medesima condotta e conseguente alla lesione di altri loro diritti particolari, diversi dall'interesse pubblico e generale alla tutela dell'ambiente*'⁶⁹ ('Compensation for environmental damage, in itself considered as an injury to the public interest in the integrity and wholesomeness of the environment, is provided for and regulated only by Legislative Decree No. 152/2006, so that the holder of the claim for compensation for this type of damage is exclusively the State, in the person of the Minister of Environment; all other subjects, individual or associated, including territorial public bodies and the Regions, may instead act, under Article.

⁶⁷ Corte Cost. 2016/04/19, n 126/2016.

⁶⁸ Cass. Pen. Sec. III 2018/10/15 n 46699 : « In tema di danno ambientale, le associazioni ambientaliste sono legittimate a costituirsi parti civili nel processo per reati ambientali, sia come titolari di un diritto della personalità connesso al perseguimento delle finalità statutarie, sia come esponenti del diritto alla tutela ambientale » ("On the subject of environmental damage, the environmental associations are legitimated to constitute themselves as civil parties in the trial for environmental crimes, both as holders of a personality right related to the pursuit of the purposes statutory purposes, and as exponents of the right to environmental protection").

⁶⁹ Cass. Pen, 2016/08/29 n 35610.

2043 c. c., to obtain compensation for any damage, further and concrete, that they have proven to have suffered from the same conduct and consequent to the injury of their other particular rights, other than the public and general interest in the protection of the environment'); or another stating that : *'La legittimazione a costituirsi parte civile nei processi per reati ambientali aventi ad oggetto fatti compiuti successivamente al 29 aprile 2006 spetta in via esclusiva allo Stato per il risarcimento del danno ambientale di natura pubblica, inteso come lesione dell'interesse pubblico alla integrità e salubrità dell'ambiente, mentre tutti gli altri soggetti, singoli o associati, comprese le Regioni e gli altri enti pubblici territoriali, possono esercitare l'azione civile in sede penale ai sensi dell'art. 2043 cod. civ. solo per ottenere il risarcimento di un danno, patrimoniale o non patrimoniale, ulteriore, conseguente alla lesione di altri loro diritti particolari diversi dall'interesse pubblico alla tutela dell'ambiente, pur se derivante dalla stessa condotta lesiva'*⁷⁰ ('The legitimacy to file a civil action in trials for environmental crimes having as their object facts committed after April 29, 2006 belongs exclusively to the State for the compensation of environmental damage of a public nature, understood as a lesion of the public interest in the integrity and healthiness of the environment, while all other subjects, individual or associated, including the Regions and other territorial public entities, can exercise civil action in criminal proceedings pursuant to Art. 2043 Civil Code only to obtain compensation for further damage, patrimonial or non-patrimonial, consequent to the injury of their other particular rights other than the public interest in the protection of the environment, even if resulting from the same harmful conduct').

Consequently, in Italian law, environmental associations have a role, but a very limited one, in that they must prove that they have suffered personal injury and act in accordance with the classical civil liability.

Instead, should perhaps be reconsidered the legitimacy of associations and other persons to act even with regard to the public dimension of environmental damage. Indeed, the public interest unquestionably linked to the recognition of environmental damage does not seem to require a monopoly of the State, because the public interest in environmental matters actually concerns not at all sovereignty, but the entire community.

In addition, in a liberal society, the State's monopoly of action must remain very exceptional and be linked to the regalian missions.

In France, contrary to Italian law, historically the associations⁷¹ were the first persons recognized by the judges as legitimate to act in case of environmental damage per se, that is to say what is in Italy considered as the public dimension of environmental damage.

The French legislature then broadened the list of potential claimants, including according to article 1248 of the Civil Code *'toute personne ayant qualité et intérêt à agir, telle que l'Etat, l'Office français de la biodiversité, les collectivités territoriales et leurs groupements dont le territoire est concerné, ainsi que les établissements publics et les associations agréées ou créées depuis au moins cinq ans à la date d'introduction de l'instance qui ont pour objet la protection de*

⁷⁰ Cass. Pen, Sec. III, 2016/05/16 n 20150.

⁷¹ For example: L Dutheil de Lamothe, 'Le contentieux en droit de l'environnement mené par les associations devant le Conseil d'Etat' (2019), spec. num. Rev. Jur. Env 41; T Fossier, 'La réparation du préjudice collectif associatif, prélude à celle du préjudice écologique', ibid 63.

la nature et la défense de l'environnement ('any person with standing and interest to act, such as the State, the French Office of Biodiversity, the local authorities and their groupings whose territory is concerned, as well as public establishments and associations approved or created for at least five years on the date of the institution of the proceedings which have as their object the protection of nature and the defence of the environment').

Furthermore, the principle of subsidiarity seems to be more respected in France since the following article 1249.2 states: '*En cas d'impossibilité de droit ou de fait ou d'insuffisance des mesures de réparation, le juge condamne le responsable à verser des dommages et intérêts, affectés à la réparation de l'environnement, au demandeur ou, si celui-ci ne peut prendre les mesures utiles à cette fin, à l'Etat*' ('In case of impossibility of law or fact or of insufficiency of the measures of repair, the judge condemns the person in charge to pay damages, affected to the repair of the environment, to the applicant or, if this one cannot take the useful measures to this end, to the State'). It is therefore mainly up to the non-State plaintiffs not only to take legal action but also to repair - when the responsible person does not do so himself, as we shall see - the damaged environment.

France has also been quite and maybe too much liberal with associations (as shown in particular by the 'Case of the Century' judged by the administrative Tribunal of Paris, February 3, 2021)⁷² by considering, for example, that 'Oxfam', an association fighting against poverty and for fundamental rights, is eligible to act in case of environmental damage. Even if one can consider that the right to the protection of the environment constitutes a fundamental right, the identity of the person who presides over this association - Mrs. Cécile Duflot, former French Minister of Environment and former president of the ecological political party 'Europe Ecologie Les Verts' - does not appear to have been totally unrelated to the judge's decision to consider the association admissible to act and to invoke the ecological damage. In the same way, another association ('*Notre Affaire à tous*') was judged admissible to act, even though it had not previously demonstrated any struggle for the preservation of the environment.

On the one hand, environmental associations may appear legitimate to act; on the other hand, they do not always have expertise in environmental protection - think about the French associations 'Oxfam' and '*Notre Affaire à tous*'.

This case also helps to show their relative inexperience in this matter: not only did they request monetary compensation without considering reparation in kind, although this latter is the priority method of reparation in the French law since 2016, but they also evaluated the damage at... one euro, which can thus contribute seriously to devaluing the environment.

Inexperience or conversely competence, which brings us to the question of who should be responsible.

B) Persons liable

By making the State, if not the beneficiary, at least the holder of the action in environmental liability, Italian law does not expressly envisage that the State can

⁷² Administrative Tribunal of Paris, February 3, 2021 N 1904967, 1904968, 1904972, 1904976/4-1.

be held liable for environmental damage. This seems questionable.

First of all, this is a break with the first movement of jurisprudential consecration of environmental damage. According to some authors like Leonardo SALVEMINI⁷³, there has been a shift from *State liability* to *liability towards the State*. However, this does not appear to be entirely exact insofar as the liability implemented in the 1970s is not that of the State but that of civil servants. The fact remains that in the 1970s if the Court of Audit did not accept the responsibility of the State as such for environmental damage, at least it recognized the responsibility of the President and then the Commissioner-Governor of the Abruzzo National Park, i.e. the responsibility of a public person. It was thus the responsibility of a public person implemented at the request of another public person: the State. That is to say, relations between public persons.

The logical evolution could therefore have consisted, for the administrative judge, in recognizing in the relations this time between private persons and the State, the responsibility of the latter for the damage caused by the public agents and all the persons under its authority.

Secondly, this failure to take into account the State as responsible for environmental damage means in practice that environmental damage, which objectively corresponds to the definition given by Italian law, cannot be compensated if it is caused at least in part by the State. Yet, the definition of environmental damage does not imply any limitation of its consideration according to the status of the persons who are likely to cause it.

Such a lacuna appears more generally to be an obstacle to emerging environmental civil liability.

Finally, the liability of the State would appear to be welcome in the event of the exclusion of the liability of any other person based on article 303,1, h of the Italian Environmental Code for the '*danno ambientale o (...) minaccia imminente di tale danno causati da inquinamento di carattere diffuso, se non sia stato possibile accertare in alcun modo un nesso causale tra il danno e l'attività di singoli operatori*' ('environmental damage or (...) imminent threat of such a damage caused by pollution of a diffuse nature if a causal link between the damage and the activity of individual operators could not be established in any way'). Indeed, who better than the State itself should be responsible for such pollution of a diffuse nature and resulting from multiple activities for which it did not sufficiently ensure the general regulation?

Some authors consider that, since the 1986 Italian law it could be a question of ensuring immunity for public agents, and in any case of a contradictory system.⁷⁴ Nevertheless, today Italian law could lead to the environmental liability of both private and public persons. The case of the State seems to be special, because it is the only one who holds the power to act.

However, some limited possibilities of responsibility of the Italian State in environmental matters appear through the following prisms:

-The liability of the Italian State towards the European Commission for the non-conformity of Italian law with the European Union's norms. This was the case before the adoption of the Italian Environmental Code. The Commission initiated

⁷³ L. Salvemini, *I principi di diritto dell'ambiente* (1st edn Giappichelli 2019), 270.

⁷⁴ Ibid, 270. See also: U. Salanitro, 'Il risarcimento del danno ambientale: profili introduttivi', in I. Nicoltra e U. Salanitro, *Il danno ambientale tra prevenzione e riparazione* (Giappichelli, 2011) II.

several infringement proceedings against Italy after the latter's reluctance to transpose faithfully the European directive of 2004.⁷⁵

Nevertheless, in such a case it is not a question of direct responsibility of the State for ecological damage, but of a failure on the part of the latter to fulfil its European obligation to transpose a text, in this case relating to liability for this type of damage.

-The liability of the State, like that of any public entity with decision-making powers, also seems likely to be engaged when an administrative act appears to be a source of environmental damage. For example, if the State authorizes a public dump in an area already marked by waste pollution. The case of waste in Campania is a good example. A lawsuit was filed by a municipality (Serre) against a series of measures adopted by the Commissioner delegated to solve the waste emergency in the region, including a measure to build a large landfill on the site of the municipality. The plaintiff municipality deduced that the quantity of waste had caused a degradation of the environment to the detriment of the rights of the citizens, of the environmental health and to the local ecosystem (declared wetland). The Tribunal of Salerno admitted the action.⁷⁶ Such a case could appear likely to be verified if necessary against the State.

-The responsibility of the State towards other persons can also be envisaged in case of delay in the protection of the environment : article 309 of the Italian Environmental Code indeed organizes a right of '*Richiesta di intervento statale*' ('Request to the State intervention') in favor of non-governmental organizations⁷⁷, and article 310 of the same code recognizes for them a right to '*risarcimento del danno subito a causa del ritardo nell'attivazione, da parte del (...) Ministro, delle misure di precauzione, di prevenzione o di contenimento del danno ambientale*' ('compensation for the damage suffered as a result of the delay in the activation, by the (...) minister, of precautionary measures, prevention or containment of environmental damage').

One can thus seem to deduce from this a conceivable liability of the State both for the delay in its reaction and also for the period of deprivation of the availability and enjoyment of the environmental goods.

-The State environmental liability can also be envisaged in the case of ecological damage caused following a failure to respect the principles of precaution, prevention and correction of environmental damage. In fact, since the Legislative Decree of 16/01/2008 n 4, article 3 ter of the aforementioned code,

⁷⁵ Part Six of Legislative Decree 152 of 2006 has been revised following the infringement procedure 2007/4679, raised by the European Union against the Italian State, in which the European Commission highlighted the failure to meet the obligations arising from the European Parliament and Council Directive 2004/35/CE of the of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage. In particular, Italy was challenged for having kept in force, in Legislative Decree 152/2006, rules that: - in case of environmental damage link the liability of operators to the requirement of fault or intent; - allow in case of damage the possibility of replacing remedial measures with monetary compensation; - limit the scope of application of the directive.

⁷⁶ Trib. Salerno, 2007/04/28, n 1189.

⁷⁷ Art. 309.1 referring to "*regioni, (...) province autonome e (...) enti locali, anche associati, nonché (...) persone fisiche o giuridiche che sono o che potrebbero essere colpite dal danno ambientale o che vantano un interesse legittimante la partecipazione al procedimento relativo all'adozione delle misure di precauzione, di prevenzione o di ripristino*" ("regions, autonomous provinces, and local authorities, including associated entities, as well as natural or legal persons who are or may be affected by environmental damage or who have a legitimate interest in participating in the proceedings relating to the adoption of precautionary, preventive, or restoration measures").

on 'Environmental action principles', states: '1. *La tutela dell'ambiente e degli ecosistemi naturali e del patrimonio culturale deve essere garantita da tutti gli enti pubblici e privati e dalle persone fisiche e giuridiche pubbliche o private, mediante una adeguata azione che sia informata ai principi della precauzione, dell'azione preventiva, della correzione, in via prioritaria alla fonte, dei danni causati all'ambiente, nonché al principio "chi inquina paga" che, ai sensi dell'articolo 174, comma 2, del Trattato delle unioni europee, regolano la politica della comunità in materia ambientale*' ('1. The protection of the environment and natural ecosystems and cultural heritage shall be ensured by all public and private entities and public or private natural and legal persons through appropriate action that is informed by the principles of precaution, preventive action, correction, as a priority at the source, of damage caused to the environment, as well as the polluter-pays principle, which, pursuant to Article 174, paragraph 2, of the Treaty of European Unions, govern the community's policy on the environment').

Consequently, failure to comply with these principles of European origin and codified by the Italian legislature would constitute a fault.⁷⁸ Such a fault, which is a subsidiary basis of environmental liability in Italian law (if the strict liability for the specific and listed activities cannot be held), as we have recalled, would thus be the cause of liability of the person who caused it, if necessary the State itself, in the event that one or more environmental damages were to result from it.

- More generally, the liability of the State appears likely to derive from article 299, paragraph 3, which states: '*L'azione ministeriale si svolge nel rispetto della normativa comunitaria vigente in materia di prevenzione e riparazione del danno ambientale (...)*' ('The ministerial action shall be carried out in compliance with existing European legislation on the prevention and remediation of environmental damage (...)').

- Again more generally, the State through the acts and policies of the public administration appears likely to be considered as an author, at least in part, of the environmental damage.

This is the case in at least three respects: because of a State policy, or because of the disregard by the State Administration of the State's international commitments, or even because of the disregard by the State of the State environmental laws.

In the first case, France for example (unlike Italy) adopted a policy favoring the development of diesel.⁷⁹ However, a WHO report of 2012 pointed out its carcinogenic effect.⁸⁰

Today, only in France about 45,000 deaths per year are considered to be directly linked to ambient air pollution⁸¹ and 13 million deaths in the world are considered by the WHO to be directly linked to the pollution.⁸²

It is not only a question of infringement of fundamental human rights, in this case the rights to life and health protected by European Convention and Court of Human Rights, but also clearly an environmental damage in the sense of the Italian and French laws since it is a question of a '*atteinte non négligeable aux*

⁷⁸ In France: H Delzangles, 'Le "contrôle de la trajectoire" et la carence de l'État français à lutter contre les changements climatiques' (2021) 36 Act. Jur. Dr. Adm., 2115, 2127.

⁷⁹ <https://www.leparisien.fr/archives/tout-a-debut-sous-de-gaulle-05-06-2012-2032992.php>

⁸⁰ https://www.iarc.who.int/wp-content/uploads/2018/07/pr213_E.pdf

⁸¹ <https://ec.europa.eu/environment/archives/cafe/general/keydocs.htm#country>

⁸² Environmental health (who.int)

éléments ou aux fonctions des écosystèmes ou aux bénéfices collectifs tirés par l'homme de l'environnement' ('non-negligible infringement of the collective benefits derived by man from the environment') in the sense of article 1247 of the French civil code and a '*deterioramento significativo e misurabile, diretto o indiretto, di una risorsa naturale o dell'utilità assicurata da quest'ultima*' ('significant and measurable deterioration, direct or indirect, of a natural resource or of the utility secured by it') in the sense of article 300 of the Italian Environmental Code.

By opening clearly the way to a possible environmental liability of the State, the Italian environmental code would also appear to be consistent with its own provisions: in addition to the above-mentioned provisions which refer to the duties of the State in this matter, art. 302 on definitions sets out: '*4. Per "operatore" s'intende qualsiasi persona, fisica o giuridica, pubblica o privata, che esercita o controlla un'attività professionale avente rilevanza ambientale oppure chi comunque eserciti potere decisionale sugli aspetti tecnici e finanziari di tale attività, compresi il titolare del permesso o dell'autorizzazione a svolgere detta attività*' ('4. "Operator" means any person, natural or legal, public or private, who engages in or controls a professional activity with environmental significance or who otherwise exercises decision-making power over the technical and financial aspects of that activity, including the holder of the permit or authorization to carry out that activity'). Indeed, the State is a legal person under public law, and it is not impossible to think that it exercises decision-making power on technical aspects (for example, with its regulations on the technical characteristics of motor vehicles) and financial aspects (especially through its fiscal policy).

Furthermore, cannot the fact that the Administration authorized, not prohibited or not sufficiently regulated certain polluting activities, especially the massive use of fossil fuels, entail its environmental responsibility? As Italian law stands, article 303 of the Environmental Code exempts the '*danno causato da un'emissione, un evento o un incidente verificatisi prima della data di entrata in vigore della parte sesta del presente decreto*' ('damage caused by an emission, event or accident that occurred before the date of the entry into force of Part Six of this Decree') and the '*danno in relazione al quale siano trascorsi più di trent'anni dall'emissione, dall'evento o dall'incidente che l'hanno causato*' ('damage in relation to which more than thirty years have elapsed since the emission, event or accident that caused it').

This would largely limit the liability of the State as well as of any person for past activities. On the other hand, article L161-2 of the French Environmental Code that lists the various exemptions does not refer to such a case.

The second case of potential liability of the State in case of environmental damage refers to its disregard of international commitments. The aforementioned example of deaths linked to air pollution can also be understood through the fundamental rights protected by the ECHR, and in particular the rights to life (a. 2) and to a healthy environment that the ECtHR has derived from article 8.⁸³ We can also mention, more recently, the Paris agreements providing for a maximum threshold of warming of the air temperature. Here again, French case law is instructive, having sanctioned the French State for failure to comply with the

⁸³ *López Ostra v. Spain*, n 16798/90/, ECHR 227 (1994).

trajectory set by the international texts.

Regarding the third case, a state public service that would disregard the laws of public protection of the environment should engage the responsibility of the State.

Thus, even if the activities of the latter do not fall within the scope of the strict or 'objective' liability foreseen for operators by the Italian environmental code, the environmental liability of the State could well fall within the scope of 'subjective liability', if not for fraud at least for fault (disregard, by the Italian State Administration, of the law or of Italy's international commitments in the matter...).

The fact that the State is the guarantor of the interests of the community should therefore not only lead to conferring on it standing to act, but should also lead to considering it as equally responsible. This is the choice of French law. First, the Charter of the Environment of 2005 (article 4) that has a constitutional value refers to the number of potential debtors as 'any person' - and the State is obviously a legal person. Then, in spite of the traditional reticence of the French administrative judge criticized by a majority of the French doctrine⁸⁴ the Administrative Tribunal of Paris, seized by associations, finally admitted in January 2021 that the State could be considered as responsible for environmental damage.⁸⁵ Thus, in France in matter of environment the State is both a remedy and an evil, Doctor Jekyll and Mr Hyde.

However, this does not appear incongruous insofar as the law of civil liability taught us that the same person can following to the circumstances be responsible or otherwise a victim.

This duality of apprehension of the State - which can be a claimant (the French Civil Code having integrated environmental liability in 2016 grants the State the right to act in case of environmental damage) but also responsible - would thus benefit from being extended to Italian law, which could on this point also be inspired by French law.

Again, the principles of the Italian environmental code lead to the retention that the guarantee of environment, natural ecosystems and of cultural heritage should be assumed according to art. 3 ter, 1 by *'tutti gli enti pubblici e privati e dalle persone fisiche e giuridiche pubbliche o private'* ('all public and private entities and by public or private legal persons'), and art. 3 quarter, 2 rules that: *'Anche l'attività della pubblica amministrazione deve essere finalizzata a consentire la migliore attuazione possibile del principio dello sviluppo sostenibile'* ('The activities of public administration must also be aimed at enabling the best possible implementation of the principle of sustainable development').

This would therefore logically seem to imply a possibility of environmental liability of the State, which is not however expressly provided for in the adopted measure, nor in past legal measures.

Nevertheless, the various difficulties of the environmental liability action against the State should not be overlooked. They appear in light of French law

⁸⁴Marthe Lucas, 'Préjudice écologique et responsabilité: pour l'introduction légale du préjudice écologique en droit de la responsabilité administrative', (2014) 4 Envir., 11-18; C Huglo, 'L'inéluctable prise en compte du dommage écologique par le juge administratif', (2013) 12 Act. Jur. Dr. Adm., 667-673.

Compare: Maryse Deguerque, 'Les imperfections de la responsabilité administrative environnementale' (2018) 36 Act. Jur. Dr. Adm 2077-2081, advocating a *"solidarité"* (public solidarity) without however clearly precisising if it must be a taxation.

⁸⁵ Administrative Tribunal of Paris, in January 2021, N 1904967, 1904968, 1904972, 1904976/4-1.

which also has its own batch of inconsistencies. In particular, French law strangely provides that, in the event that the plaintiff is unable to take the necessary measures, the damages may be paid to... the State itself. Quite singular situation where the State would pay damages to itself!

The State would not be in reality responsible at all, because such a payment would only be made by the game of accounting entries from a public budget to another public budget.⁸⁶

As can be seen, a whole area of environmental liability appears either blocked upstream (Italian law) or annihilated downstream (French law).

Consequently, French law would benefit from eliminating this weapon of mass self-destruction of the environmental liability. For example, by providing that when it is the State that is judged to be responsible or co-responsible, the damages due by the latter should always be paid to the plaintiff and allocated to the concrete repair and protection of the environment. If necessary under the control of the debtor State itself.

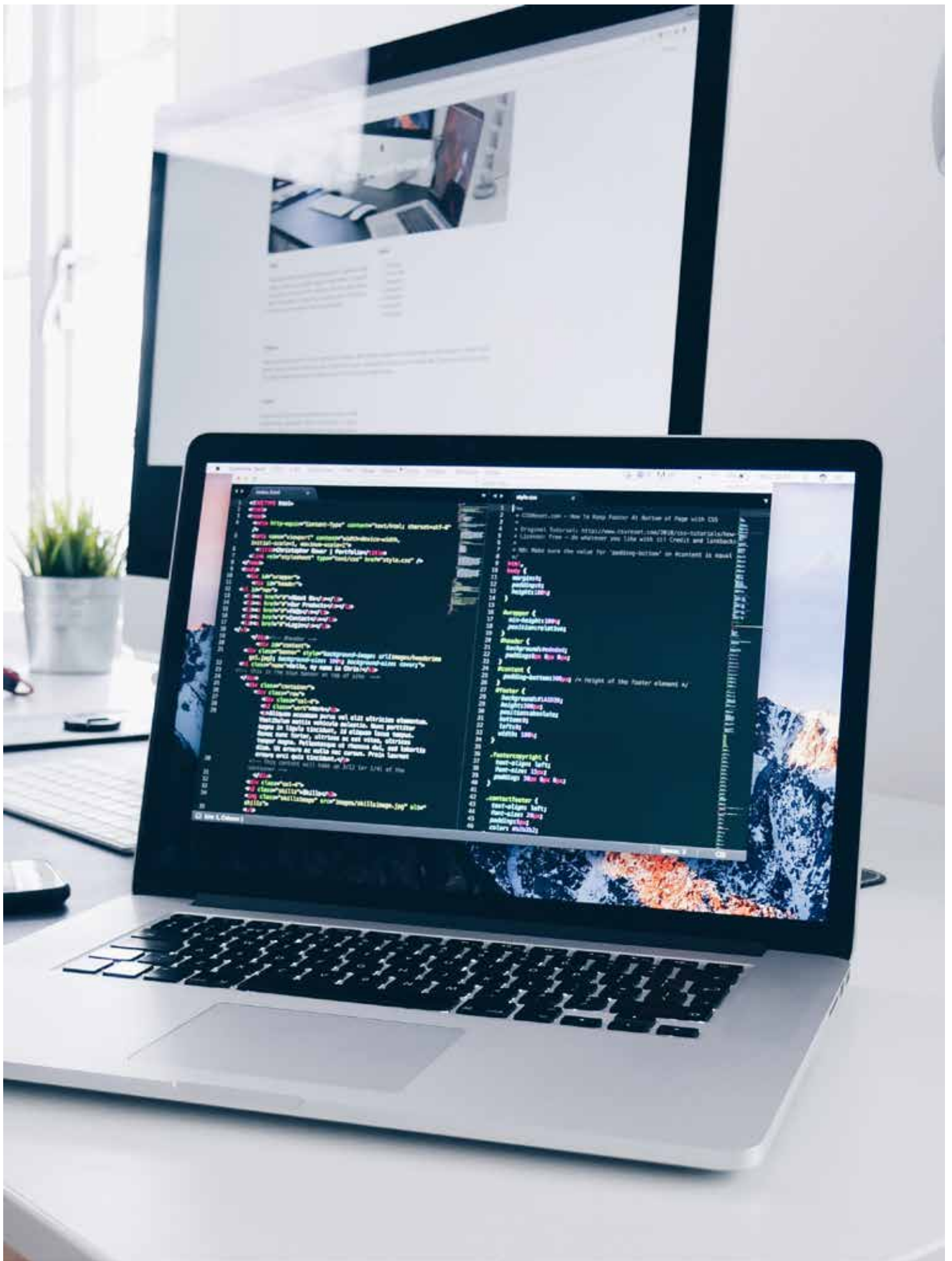
If it were to take up this possibility of holding the State responsible for environmental damage, Italian legislature would have to take care to refrain from providing for the State to pay compensation to itself, even from one State budget to another.

More fundamentally, in all cases where the State is considered as a person potentially responsible for environmental damage, whether the compensation is in kind or in the form of a monetary equivalent, it can only be made at the taxpayer's expense.

More precisely, the present and future taxpayer, for past choices that were essentially public, such as for instance the French policy of favoring diesel.

This contributes definitely to make environmental civil liability a strange legal object between the traditional tools of penalization and taxation, but undoubtedly a necessary evil both before and for a deep ecological transition.

⁸⁶ J Bétaille, 'Le préjudice écologique à l'épreuve de l'affaire du siècle' (2021) 38 Act. Jur. Dr. Adm. 2228-2234.





Artificial Intelligence and Self-determination in Medical Field

CARLOTTA DE MENECH 

Senior Researcher in Private Law, Pavia University

Abstract

The use of artificial intelligence in medicine raises many legal issues. This essay examines how medical AI intersects with the right to informed consent and the principle of self-determination. The author highlights that the complexity and opacity of machine learning could dissuade the patient from consenting AI treatment and, therefore, induce him to give up the benefits that this technology usually brings to his health. Consequently, the author suggests adjusting the content of the information due to the patient, taking into account the limited knowledge that ordinary people have about artificial intelligence, and, more generally, redefining the boundaries of the principle of informed consent.



Keywords: artificial intelligence; machine learning; self-determination; informed consent; data protection.

Summary: [1. Introduction.](#) – [2. Legal issues of informed consent with regards to AI in healthcare.](#) – [3. The regulatory framework.](#) – [4. A realistic approach?](#) – [5. Personal data for health and AI.](#) – [6. Perspective and conclusions.](#)

1. Introduction.

Every generation of legal experts has had to perform the task of investigating the effects that the advent of new technology has had on one or more areas of application of the law. For example: the generation of the early twentieth century investigated the changes brought by the motorization of road traffic on tort law, the generation of the last part of twentieth century had to investigate the impact of digitalization on the format of contracts, as well as the violation of copyright law. The current generation, on the other hand, has had to study the extraordinary changes, both positive and negative, that the development of artificial intelligence (henceforth, AI¹) seems capable of causing within every area of law. One of the areas most affected by the progress of AI is health law, owing to the success that AI devices have had in the medical field. As a matter of fact, synergy between humans and AI systems bring important benefits to the guarantee of the right to health, with respect to the right to obtain high standards of medical care and adequate therapeutic treatments.

As the European Parliament highlighted in two Resolutions on AI and civil law,² and as the EU Commission restated in the “White Paper on Artificial Intelligence”,³ AI medical tools are particularly suitable for carrying out high-precision surgical procedures (such as, for example, analysis of exams, radiographs and CT scans), or even carry out personalized assistance tasks (such as, for example, the so-called continuous glucose monitoring system, which measures the glucose level continuously throughout the day, and also predicts the progress glycemic rate in diabetic patients). The Resolutions and the White Paper also stressed that when AI supports diagnostic decisions of the physicians, diagnostic times, costs and medical errors significantly decrease.

1 It is worthy of being highlighted that, both in common speech and specialistic language, there are many definitions of AI: see A Bertolini, *Artificial Intelligence and Civil Liability. Bruxelles* (European Parliament, 2020, Committee on Legal Affairs) 15 ff. In this essay AI will mainly mean branch of computer science that studies and reproduces mechanisms of human intelligence, using self-learning techniques and their applications. Even the “Proposal of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative act”, which was adopted on 21st April 2021 (henceforth, Artificial Intelligence Act Proposal or, more briefly, Proposal), addresses the issue of how to describe adequately AI technology. Indeed, the 6th recital argues that, ‘The notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments’, and the art. 3, n. 1, of the Proposal states that, ‘artificial intelligence system [...] means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.’

2 European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics and European Parliament Resolution of 12 February 2019 on comprehensive European Industrial Policy on Artificial Intelligence and Robotics.

3 White Paper on Artificial Intelligence. A European approach to excellence and trust (19th February 2020).

Moreover, the recent Artificial Intelligence Act Proposal⁴ explains that, ‘By improving prediction, optimising operations and resource allocation, and personalising service delivery’, the use of AI in the High-Impact Sector (for example, the medical sector), ‘can support socially and environmentally beneficial outcomes and provide key competitive advantages to companies and the European economy.’ In particular, the usage of robotics and AI could bring further advantages in terms of economic savings to health care, thus allowing the allocation of more money for prevention strategies and biomedical research. As it is widely known, biomedical research is becoming more and more efficient because of the support provided by AI techniques.

The benefits in medical treatments and scientific developments, as mentioned in previous paragraphs, are however accompanied by empirical risks, technical complexity, ethical concerns and therefore legal issues. As is sometimes the case, new problems emerging from the use of AI in healthcare require the implementation of new rules by the legislator; this is for cases where intelligent medical devices have caused damage during routine procedures carried out autonomously by these devices, thus creating problems as current liability law doesn’t cover these new aspects of AI. Furthermore, the issues raised by medical AI at the moment only require the adjustment of existing rules or principles; it is not a legal requirement to write new laws for AI at this time. This is likely the case of the several problems that appear when the pitfalls related to development and use of AI in the medical sector intersects with the right of self-determination.

In this article I am going to demonstrate the issue raised in the previous sentence. Specifically, in the next three paragraphs I am going to determine if and to what extent AI’s involvement in treatment should be disclosed to the patient under the current regulation and doctrine of informed consent. In the fourth paragraph I will consider the difficulty in processing the large amount of data necessary for the development of AI medical systems in compliance with the requirements imposed by the General Data Protection Regulation (GDPR) to protect the right of natural persons to control the use of their personal data. In the last paragraph I will consider some scenarios that could arise in the near future and I will present my final considerations.

2. Legal issues of informed consent with regards to AI in healthcare.

As I anticipated in the introduction, the medical applications of AI brings not only many important benefits in terms of efficacy and accuracy of treatment⁵ and in terms of safety and timeliness of diagnosis,⁶ but also raises certain concerns.

First of all, it is necessary to consider the difficulty of humans to understand

4 The Proposal classifies applications of AI in healthcare among the, ‘High-risk AI systems’: see article 6.1 and annex II.

5 See, for example, R Tregunna, ‘Artificial intelligence for intrarenal access’ [2021] *Nat Rev Urol* 18 ff.

6 See, for example, S Goto, K Mahara, L Beussink-Nelson and others, ‘Artificial intelligence-enabled fully automated detection of cardiac amyloidosis using electrocardiograms and echocardiograms’ [2021] *Nat Commun* 2726 ff.; A Rao, H Fishman, ‘Accessible artificial intelligence for ophthalmologists’ [2022] *Eye*.

and explain how AI technology works. The so-called ‘opacity’ of AI⁷ depends on the right of intellectual property, but also on the complexity of the computational language and on the machine learning methods (ML); on which the development and the functioning of the so-called autonomous systems are based on. In particular, ML gives rise to the black box problem. By looking at the source code, programmers and experts are able to understand the logic of the system, the algorithm architecture used and the structure of the data set. However, not even the designers of the intelligent machine fully understand how it works and arrives at individual and concrete outputs.⁸

The lack of transparency or even inscrutability of AI leads to some further questions. Therefore, the doctor could blindly rely on the diagnostic or therapeutic solution suggested by the machine, refraining from making critical assessments and, if necessary, independent choices.⁹ Moreover, because of the opacity of AI technology, the doctor could be prevented from providing the patient with a clear and reliable diagnosis and consequent therapy, by which the patient may be able to rationally come to a self-determined decision about their treatment.¹⁰ There is a serious danger that the patient will know that AI medical technology will be used in the course of treatment but will not understand how the technology works. They therefore will make their decision about treatment based on a lack of understanding of the technology involved, or even more worrying on a preconceived opinion or, sometimes, even fear¹¹ of technology in general.

In the development and practical use of AI there are also some negative factors that could inhibit the success of the treatment. First, there is the risk that AI-based machines could contain cognitive biases that have been trained on a set of data that is not sufficiently representative and, therefore, not fully suitable for carrying out the task for which the system was created.¹² To give a hypothetical example an AI medical device could be used in the diagnosis of breast cancer, which has been developed using a training data set made up only of Caucasian women, although they have a breast density which is different from that of African American women. As a result, the algorithm is likely to give information that is less reliable for the African American population.

Secondly, there is the issue of the ethical lack of AI and, therefore, the inability of intelligent devices to make ethical decisions which frequently occur in the medical field. For example, the decision whether to perform surgery on a young

7 Article 13 of the Artificial Intelligence Act Proposal states that, ‘High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system’s output and use it appropriately.’

8 On the black box problem see: F Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press 2015); W Nicholson Price II, ‘Black-box Medicine’ [2015] Harv. J. L. & Tech. 419 ff.; Id, ‘Regulating Black-box Medicine’ [2017], in Mich. L. Rev. 421 ff.; P Vogel, ‘A “right to explanation” for algorithmic decisions’, in A Santosuosso, G Pinotti, *Data-Driven Decision Making. Law, Ethics, Robotics, Health* (Pavia University Press 2019) 50; C A Tschider, ‘Beyond the “Black Box”’ [2021] Denv. L. Rev. 683 ff.; K Astromske, E Peičius P. Amstromkis, ‘Ethical and Legal Challenges of Informed Consent Applying Artificial Intelligence in Medical Diagnostic Consultations’ [2021] AI Soc. 512.

9 Comitato Nazionale per la Bioetica, Report ‘Intelligenza artificiale e medicina: aspetti etici’ (2020) 11; Astromske, Peičius, Amstromkis, ‘Ethical and Legal Challenges of Informed Consent’ (n 8) 514.

10 D Schiff, J Borenstein, ‘How should clinicians communicate with patients about the roles of artificially intelligent team members?’ [2019] AMA J. Ethics 139 f.

11 P Costa, ‘Cosa ci spaventa dell’intelligenza artificiale?’ (2021) 1 BioLaw J. 303 ff.

12 See article 10, par. 2 and 3, of the Artificial Intelligence Act Proposal. See also S Scalzini, ‘Alcune questioni a proposito di algoritmi, dati, etica e ricerca’ [2019] Riv. it. med. leg. 169 ff.

woman suffering from a malignant neoplasm of the genitalia, either a radical dissection which could save her life, but will prevent her from having children, or to carry out a more standard operation which will not prevent her from having children but that may not save her life.

Finally, it must be considered that the use of AI medical tools decreases but does not eliminate the risk of adverse events that could be harmful for the patient's health; indeed, sometimes, exceptional failures of such devices could damage the patient's health and could lead in some cases to death. This could happen, for example, if a hospital's IT system is hacked causing the sudden arrest of the robot at the most critical moment of an operation in which time is the most important factor.¹³

In the light of the framework outlined above, many questions are raised with regards to medical AI and informed consent.

First of all, if the doctors chose to conceal the use of AI during diagnostic consultation or during treatment, are they violating the patient's right to informed consent? Secondly, to what extent should the patient be informed about their treatment with respect to medical AI? Is it sufficient to give the patient a generic description of AI technology and its benefits, or is it also necessary to fully disclose all the risks? In particular, must the doctor communicate the possibility, however miniscule, of a system malfunction? Is it correct to expect the doctor to explain to the patient fully how AI medical systems work, to the extent that the patient can give a truly 'informed consent'? Finally, if the medical device auto updates its algorithms and is self-learning and is therefore not under the control of the developer, is the doctor obligated to inform this to the patient?

The questions raised in the previous paragraph have so far received surprisingly little attention in the Italian literature and have not given rise to any debate at the time of writing. Indeed, opinions expressed in this regard are few and are all concerned with upholding the doctrine of informed consent in the wake of the advancement of AI technology and, therefore, in support of enclosing every details of medical AI involvement to the patient.¹⁴

The overview is a bit different in the United States where, as it is well known, both the doctrine of informed consent¹⁵ and the science of AI are studied much more widely and have been so much longer than in Italy. In fact, in American literature there are still only a few studies on the intersection between medical AI and informed consent but they do have certain mitigating circumstances in America which relieve the doctor of the onus of explaining to the patient the full details of the treatment; something that we do not have in Italy.

13 To prevent similar accidents the Artificial Intelligence Act Proposal states that high-risk AI should, '... be designed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle': see art. 15, par. 1.

14 R Messinetti, 'La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata' (2019) 3 Contr. impr. 861 ff.; C Casonato, L Violante, 'Forum: AI and Law' (2020) 1 BioLaw J. 463 ff.; E Tozzi, G Cinelli, 'Informed consent and artificial intelligence' [2021] BioLaw J. Special Issue 106 ff.

15 The informed consent doctrine was expressly stated in *Salgo v Leland Stanford Jr University Board of Trustees* [1957] 154 Cal. App. 2d 560, 317 P.2d 170. However, a duty to tell the patient, '... what is about to done to him ...' e duty to obtain the consent was already recognized in *Slater v Baker and Stapleton* [1767] 95 Eng. Rep. 860, 2 Wils. K.B. 359.

In particular, a recent article¹⁶ says that common law exempts the physician from explaining to the patients all the complicated elements, which a doctor has studied in the course of their professional training and in the course of their career; for example: university studies, further academic reading, participation in top up courses etc. These form the basis of decisions, both diagnostic and with respect to treatment, that the doctor must make. Therefore, the article concludes that the doctor could be allowed to conceal the use of AI, all the more so because the opacity of this technology would risk inducing most patients to reject it and, thus, all the benefits it entails.

3. The regulatory framework.

Moving on to the Italian legal system, we need to determine whether to disclose the involvement of AI/ML in medical treatment to the patient and how much to disclose, under Italian informed consent law.

This consists of articles 2, 13 and 32 of the Italian Constitution and article 3, second paragraph, of the EU Charter of Fundamental Rights and articles 1-3 of the Law No. 219/2017 (which is the specific legislation on informed consent and advance directives). In addition to these, there are articles 16 and 33-39 of the Code of Medical Ethics¹⁷ (approved in 2014 and modified later) and in addition, case law. In this matter, legal sources are organized on a basis of sharing rather than on a basis of status.¹⁸ It is well known that the informed consent principle was formerly expressed in international documents,¹⁹ therefore, established by the Codes of Medical Ethics;²⁰ and subsequently was accepted and reinforced by the courts on the basis of the Constitution;²¹ and at the end of this process, was laid down in ordinary legislation which, due to complexity and mutability of the matter involved, still needs to be specified and integrated with other sources.²² This is also true for the questions arising from the use of AI systems in medical diagnosis and treatment.

The article number 1 of Law No. 219/2017, paragraph number 1, presents the principle of free and informed consent and in paragraph number 3 describes what information must be conveyed to the patient and the way in which it should be conveyed. In this description, the legislator simply acknowledged some of requirements that our courts had already previously identified on the basis of

16 G Cohen, 'Informed Consent and Medical Artificial Intelligence: What to Tell the Patient' [2020] Geo. L. J. 1432 ff.

17 On the binding value of the Code, see Cass., sez. un., 20th December 2007, n. 26810, in Foro it., 2009, 3167; and, even previously, E Quadri, 'Il codice deontologico medico nei rapporti tra etica e diritto' (2002) 4-5 Resp. civ. prev. 925 ff.

18 As V Calderai, 'Consensus informato', *Enciclopedia del diritto, Annali VIII* (Giuffrè, 2015) 233, well explains.

19 World Medical Organization, Declaration of Helsinki, Ethical Principles for Medical Research Involving Human Subjects (1964); United Nations, International Covenant on Civil and Political Rights (1976); and Oviedo Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (1997).

20 Firstly by Codes of Medical Ethics (1995).

21 Cass. pen., 21st April 1992, n. 5639, in Cass. pen., 1991, 1333.

22 As A Nicolussi, 'Al limite della vita: rifiuto e rinuncia ai trattamenti sanitari' [2010] Quad. cost. 274 f., clearly explains.

general principles and other legal sources.²³ These rules do not clarify whether it is the duty of the doctor to inform or indeed not to inform the patient or to what extent to inform the patient that the treatment involves these computational methods and related exceptional risks.

The letter of the third paragraph of article number 1 of the Law No. 219/2017, does not indicate clearly if the doctor is obligated at all to communicate to their patient the devices and techniques which will be involved in their treatment. The rule establishes that the doctor must inform the patient about 'diagnosis' and 'prognosis'; terms which are ambiguous in their scope; do they refer only to the results of those particular activities, or do they also refer to the operating methods. Furthermore, the law says that the information must include the, '(...) benefits and the risks (...) related to the medical treatment', without clarifying if the patient must be warned about only the foreseeable risks, or about the unforeseeable risks also. These doubts unfortunately are not reduced by considering the adjectives which the legislator uses in describing the characteristics of the information that must be conveyed to the patient. Indeed, the adjective, 'complete' seems to suggest full disclosure, whereas the adjective, 'comprehensible' seems to suggest selecting the information on the basis of patient's cognitive and rational skills.

The aforementioned confirms the need to refer to other sources, these however do not specifically answer the questions arising from the diffusion of AI in the medical field but do provide ideas on which we can reflect in order to suggest a balanced and reasonable solution.

Firstly, the sources which generated the doctrine of informed consent, in the absence of ordinary legislation, remind us that the patient's self-determination is an essential basis of the medical relationship; yet this does not constitute its sole and exclusive role in the aforementioned relationship.

Therefore, on the one hand, there is no doubt that article number 32, read in conjunction with articles number 2 and 13, of the Italian Constitution represents a cornerstone of the constitutional matrix of informed consent. However, on the other hand, article 32 also requires the medical relationship to be based on the right to individual and collective health and, therefore, on the correlative duty to treat the patient. In spite of this, the majority of Italian jurists perceive the right to health protected by the Constitution as an individual right equal to that of the right to self-determination.²⁴

This theory, which reduces healthcare to the basis of will (i.e. self-determination), has been argued from the spiritual notion of the former given by the World Health Organization. According to them, 'Health is a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity'.²⁵ In addition, the common interpretation of the constitutional right to

23 S Cacace, 'La nuova legge in materia di consenso informato e DAT: a proposito di volontà e di cura e di comunicazione' [2018] Riv. it. med. leg. 935 ff.

24 P Zatti, 'Rapporto medico-paziente e «integrità» della persona' (2008) 12 NGCC 403 ff.; E Rossi, 'Profili giuridici del consenso informato: i fondamenti costituzionali e gli ambiti di applicazione' [2011] Riv. AIC 5 ff.; I Rapisarda, 'Consenso informato e autodeterminazione terapeutica' (2019) 1 NGCC 43 ff.; L Chieffi, *Il diritto all'autodeterminazione terapeutica. Origine ed evoluzione di un valore costituzionale* (Giappichelli, 2019) 99 f.; Corte cost., 22nd June 1990, n. 307, at www.cortecostituzionale.it; Trib. Milano 14 maggio 1998, in NGCC, 2000, 92 ff.

25 See Constitution of World Health Organization (22.7.1946-7.4.1948), 2.

health has been justified by a reasoning which underestimates or even ignores the social relevance of the legal protection of personal rights. Because of the mainstream, the patient's self-determination appears to be an absolute power that has neither limits nor any substance and, therefore, the doctor seems to have a duty to provide them as much information as possible.²⁶

In considering this theory, there are some authors who dissent from the majority and deem that the patient's right to health is broader in sense than that of right to self-determination.²⁷ The opinion of this minority is based on a more complete reading of article number 32 of the Italian Constitution. By reading this article in its entirety and in considering its constitutional context it becomes clear that the right to health is closely related to the values of human dignity (art. 32, 2nd par.) and the duty of solidarity (art. 32, 1st par.; and art. 2) and, consequently, has a scope that goes beyond the patient's personal sphere and also affects public protection of health and social function of medical activity.

In connection with these further aspects, the right to health takes on an autonomous meaning and can serve to limit and shape the right to informed consent. In this way, self-determination regains its substance with regards to mental and physical well-being, as well as the competences of the doctor as a guide, and the patient's weaknesses as a limit. Instead, if (in accordance with the majority) the medical relationship were based only on the patient's will, the medical relationship would become purely "contractual", and therefore the effectiveness of the patient's right to self-determination could be potentially compromised.

This has been demonstrated in other legal contexts (for example labour law, consumer law, banking and financial market law) in which the freedom to choose can be diminished because of the weak negotiating position of a contracting party and consequently some precautions are necessary.²⁸ For example, rules that adjust the quality and the amount of information on the particular condition of the fragile party, who may be confused by an explanation which is too detailed.²⁹

A similar risk has been perceived also by some judges during rulings on self-determination in healthcare. Indeed, Italian courts sometimes consider it necessary to diminish, to a certain extent the amount, of information to be provided to the patient. This is because of their vulnerability and in order to safeguard their health. For instance, several judgments state that doctors must inform the patient about the normal associated risks of treatment but they must not communicate abnormal and / or remote risks, which don't normally occur in the course of standard treatment.³⁰ The rationale of this rule is well explained by

26 As A Carminati, *Libertà di cura e autonomia del medico. Profili costituzionali* (Cacucci, 2018) 26 ff., highlights.

27 Nicolussi, 'Al limite della vita' (n 22) 275 ss.; F D Busnelli, 'Problemi giuridici di fine vita tra natura e artificio' (2011) 1 Riv. dir. civ. 161 ff.; A Nicolussi, 'Testamento biologico e problemi del fine-vita: verso un bilanciamento di valori o un nuovo dogma della volontà?' [2013] Eur. dir. priv. 457 ff.; G Razzano, *La legge n. 219/2017 su consenso informato e DAT fra libertà di cura e rischio di innesti eutanasici* (Giappichelli, 2019) 20 ff.

28 Nicolussi, 'Al limite della vita' (n 22) 294 f.; L Eusebi, 'Note sui disegni di legge concernenti il consenso informato e le dichiarazioni di volontà anticipate nei trattamenti sanitari' [2006] Criminalia 253.

29 See R Costi, *Il mercato mobiliare* (11th edn., Giappichelli 2018) 56, with regards to public offer of financial products.

30 Cass., 20th May 2016, n. 10414; Cass., 11th December 2013, n. 27751; Cass., 30th July 2004, n. 14638, in Resp. civ. prev., 2007, 688; App. Bologna, 2nd February 2006; Trib. Milano, 28th January 2020.

some courts, saying that to communicate in addition to the normal risks, abnormal and/or remote risks could instill in the patient an unjustified amount of fear which could discourage them from giving permission for treatment which is both safe and standard in modern medical practice.³¹ Therefore, in case law we have this idea of quantity versus quality i.e. that the quality of information provided to the patient is more important than the quantity of information. there is the idea of quantity and quality of information.

Thus, the doctor must provide information to the patient, but this should be regulated on the basis of the emotional state and cognitive skills of the patient and, therefore, the quantity of information provided could be reduced based on this principle. Considering the quality of information over the quantity will in fact enable the patient's recovery rather than hindering it. The same idea is expressed by article 33 of the Code of Medical Ethics which states that the doctor must always communicate to the patient whilst being fully aware at all times of their mental competence and emotional sensitivity.

It would be wrong, therefore, to suppose that such a rule and the aforementioned judgments are based on Hippocratic privilege or the paternalistic concept of the medical relationship.³² Indeed, the case law and the Code of Medical Ethics carry out a 'synthesis of concurrent interests';³³ on the one hand there is the patient's informed consent and on the other the doctor's duties and the patient's health. It is better to talk about synthesis instead of balancing because such rules do not intend to restrict the former right of informed consent in order to extend the protection of the patient's health but merely to take into account the inherent limits to the principle of informed consent. Cognitive psychology research shows that the patient's vulnerability and potential lack of comprehension significantly limit their ability to understand the dynamics of the treatment, assess costs and benefits and therefore make rational choices. In such conditions, as Professor Calderai states, 'multiplying the information would be like trying to put out a fire by throwing petrol on it.' Instead, it would be more appropriate to create '(...) communication and decision-making contexts in which it is possible to select information in relation to its relevance and comprehensibility (...)'.³⁴ In short, the patient's weaknesses in this context suggest that a realistic approach to the data aimed at medical consent would be preferable. In particular, the choice of communicating technical details should be at the discretion of the doctor, who should be permitted to make choices based on reasonableness.³⁵ Therefore, the doctor makes a decision that does not adhere ideologically to only one of the contrasting values: self-determination and health. Instead, the doctor makes their decision weighing up the patient's right to self-determination against that of their health requirements in that specific moment. Such an approach is necessary to prevent the outcome of the communication of too much information thus affecting both the patient's self-determination and health.

31 Cass., 30th July 2004, n. 14638, *ibid*; Trib. Bologna, 8th August 2005. See also M Foglia, *Consenso e cura. La solidarietà nel rapporto terapeutico* (Giappichelli, 2018) 69.

32 See G Azzoni, 'Il consenso informato: genesi, evoluzione, fondamenti', in G Viafora, A Gaiani, *A lezione di bioetica. Temi e strumenti* (Franco Angeli, 2015) 172 ff., with regards to the evolution of the relationship between doctors and patients.

33 Corte cost., 23rd December 2008, n. 438, in *Foro it.*, 2009,1328.

34 Calderai, 'Consenso informato' (n 18) 238.

35 G Criscuoli, 'Ragionevolezza e consenso informato del paziente' [1985] *Rass. dir. civ.* 486.

4. A realistic approach?

In answering the questions previously asked in the second paragraph, it is possible to deduce that if the doctor were to conceal the involvement of technology in the treatment, on the basis of a diligent evaluation of their patient, they would not be violating the principle of informed consent. This conclusion has been arrived at using the current regulatory framework and seems to remain valid even in the face of future developments that could affect the legislation on AI applications in healthcare in the future. The first paragraph of article 52 of the Artificial Intelligence Act Proposal establishes some, 'Transparency obligations for certain AI systems,' and, in particular, states that '(...) providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system.' However, this provision seems to impose a duty on the providers to inform the doctor (i.e., the subject who interact with AI system) about the interaction with AI system and therefore it is not a duty of the doctor to inform the patient (i.e., the subject who undergoes the interaction between doctor and AI system).

Instead, the statement made at the beginning must be adjusted to meet specific features that the situation in front of the doctor may present, primarily, to the scenario in which the patient asks specific questions regarding the type of instruments used in the diagnosis or treatment.³⁶ It is well established that the duty to satisfy the patient's curiosity is more restrictive than the duty to inform them because a lie is generally more serious than silence and also because specific questions could be a sign of rationality and competence. For example, it has been argued that the doctor is not obligated to communicate the statistics of the hospital in which they work, the accidents occurred during treatment, and abnormal and/or remote risks of the treatment to be performed. However, such information should be given to the patient only and specifically if they ask for it. In the same way, the doctor is obligated to answer all questions that the patient has with regards to instruments involved in their treatment and therefore potentially any questions regarding the use of robots or AI devices as well. Furthermore, depending on the type of treatment it may be necessary to include the instruments and technology that will be used in the information pack given to the patient. This in particular is true for the field of cosmetic surgery,³⁷ where it is the rule to communicate more comprehensively to the patient the facts of the treatment and the instruments involved. This is because the treatment is aimed at improving the patient's physical appearance or certain functions, rather than safeguarding their life or health.³⁸

The third and final example in which the use and consequences of using

36 See M Graziadei, 'Il consenso informato e i suoi limiti', in S Rodotà, P Zatti, *Trattato di Biodiritto* (Giuffrè 2011) 254 f.; M G Di Pentima, *Il consenso informato e le disposizioni anticipate di trattamento. Commento alla l. n. 219/2017* (Giuffrè 2018) 63.; Foglia, *Consenso e cura* (n 31) 66.

37 Specifically, when the cosmetic surgery is only aimed at improving physical appearance: I Pizzimenti, 'Il diritto di conoscere o non conoscere il proprio stato di salute: modalità e contenuto dell'informazione' (2019) 1 NGCC 75.

38 Cass. 6th October 1997, n. 9705, in Resp. civ. prev., 1998, 667.

medical AI must be communicated to the patient is when they use such devices in their own home. In this case, the information must include simplified explanations of how the instruments work. However, it is necessary to remember that the doctor often does not have the necessary skills to explain how the AI devices work in full detail.³⁹ Moreover, the doctor cannot involve an engineer in the process of informing the patient⁴⁰ because of Article 1, Second paragraph, of the Law No. 219/2017 which states that the duty to inform the patient cannot be delegated to non-medically qualified professionals. To bypass this question, it can be assumed that the patient has a right to be informed of the use of all technology involved in their treatment, however, only in the public health service. This is according to the changes made recently to the Italian rules on telemedicine for all cases in which medical diagnosis and/ or treatment is made online.⁴¹

Firstly, based on what was written in the previous paragraph, it could be possible to deny that the doctor, finding themselves in one of the situations that requires them to communicate to the patient the use of AI in treatment, doesn't have to clarify the technicalities (i.e., algorithms and data mining) on which the development and the operation of such devices is based on.⁴² In fact, the doctor does not have the competence that would be needed for the purpose of an in-depth explanation and indeed the patient cannot have the training and the experience that is necessary for a full comprehension of all that is involved in the procedure. Therefore, the doctor fulfills the obligation to inform their patient about AI, providing a generic but understandable description (given the patient's capacities) of the technology involved in the treatment and presenting the benefits and limits that it normally entails. Instead, in order to avoid refusal of permission caused by unjustified fears on the patient's part, the doctor should conceal the unforeseeable risks; namely, the remote possibility that a breakdown of the device or software could cause injury to the patient's health. With this same rationale as a basis, it could be argued that the doctor should also refrain from explaining to the patient that the devices used in treatment operate using self-learning methods and, therefore, are not fully intelligible to humans, and indeed not infallible. Indeed, as it has been observed, to communicate opaque elements to the patient could compromise the relationship of trust between them and the doctor, and induce the patient to refuse also other therapeutical options.⁴³ Instead, it is always convenient to inform the patient that the AI system involved in the treatment can be effectively overseen by the doctor, who can tackle potential problems which occur in the system in real time.⁴⁴

39 Comitato Nazionale per la Bioetica, Report "Intelligenza artificiale e medicina: aspetti etici" (29th May 2020), 15.

40 As Astromske, Peičius, Amstromkis, 'Ethical and Legal Challenges of Informed Consent' (n 8) 516 suggest.

41 See Italian Ministry of Health, National Guidelines for Telemedicine (27th May 2020), 13.

42 The doctor is not obligated to provide an *ex post* explanation, yet an *ex ante* explanation could be deemed sufficient: U Pagallo, 'Algo-Rhythms and the Beat of the Legal Drum' [2017] *Philos. & Technol.* 515.

43 Astromske, Peičius, Amstromkis, 'Ethical and Legal Challenges of Informed Consent' (n 8) 521.

44 If Artificial Intelligence Act Proposal were approved, human oversight would be juridically binding (see art. 14 of the proposal).

5. Personal data for health and AI.

The field of self-determination with regards to health involves not only the principle of informed consent to treatment but also the consent which should be given for the purpose of processing personal data. The development of AI could cause some issues also with regard to the second area of law.

Firstly, AI technology represents a factor that exposes privacy to new potentially harmful situations. This is because the creation of predictive models is carried out through intensive data research, that is to say, research which requires a large amount of data.⁴⁵ Therefore, Evidence-Based Medicine (EBM) makes use of a volume of data which can be measured in megabytes or gigabytes, whereas the development of AI medical devices requires a size of data which can be quantified in terabytes or petabytes and extrapolated from a very large sample.⁴⁶ Moreover, AI systems make it possible to collect large amounts of data in a short period of time. Therefore, the EBM is an empirical approach based on a few clinical cases, whereas AI allows the analysis of data drawn from a wide range of sources: electronic health records, medical devices that measure biological variables (the so called Internet of Medical Things: IoMT), genomic banks, social networks and internet browsers.⁴⁷ Finally, it should be noted that the logic of Big Data and machine learning techniques facilitate the re-identification of data originally anonymized; and furthermore, they facilitate the creation of derived personal data.⁴⁸ This second problem has given rise to an intense debate in the United States, where Ascension - a healthcare giant that consists of two thousand six hundred medical facilities, including over one hundred and fifty hospitals - sold health data relating to millions of patients to Google, with the aim of allowing the latter to develop a software that enables its healthcare professionals to collaborate in real time and improve the quality and effectiveness of care. This has caused concerns that Google may use its experience in data mining to cross-reference the information obtained with that collected from its users and, thus, obtain new personal data relating to them.

For the reasons explained above AI technology represents an essentially antagonistic element with respect to the protection of the right the collection and processing of people's personal data. However, the Big Data applications seem to bring many advantages with respect to the protection of individual and public health. As we have already highlighted, these applications are involved in medical diagnostics and treatment in a way that is both useful and helpful to the patient. Moreover, as covid-19 pandemic experience has been showing, Big Data and computational methods improve the efficiency of pharmacological research and enable the developing of contact tracing systems.⁴⁹

Therefore, the arrival of AI raises a potential conflict between individual self-determination and other fundamental interests not only in the area of physical

45 G Comandè, 'Ricerca in sanità e data protection: un puzzle ... risolvibile' [2019] Riv. med. leg. 187.

46 N Musacchio, G Guaita, A Ozzello, and others, 'Intelligenza artificiale e Big Data in ambito medico: prospettive, opportunità, criticità' [2018] J AMD 214.

47 Ibid.

48 T Sharon, 'Data-driven Decision Making, AI and the Googlization of Health Research', in Santosuosso, Pinotti, *Data-Driven Decision Making* (n 8) 42; C Colapietro, A Moretti, 'L'intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali' (2020) 3 BioLaw J. 377.

49 A Santosuosso, S Azzini, *La giusta distanza. Le nostre libertà dopo Covid-19* (Mondadori, 2020) 76 ff.

body management but also in the field of controlling the ‘electronic body’.⁵⁰ This conflict cannot always be resolved in favor of individual self-determination when its presumed superiority in the hierarchy of values is taken into consideration in the resolution process.⁵¹ In the field of data protection, the conflict between self-determination and health appears in less direct and final terms than what usually happens in the context of the therapeutic relationship. This is because the refusal by the data subject to give permission for the collecting and processing of their personal data does not immediately harm either their health or that of the collective. Therefore, it seems reasonable to argue that, at least in principle, the data subject should be fully informed of the computational methods involved in the treatment of their personal data.⁵² However, in both areas the actual realization of the self-determination principle faces some empirical difficulties due to specific characteristics of AI technology. Secrecy, complexity and sometimes inscrutability of AI systems are factors which prevent the data subject from fully understanding how their personal data will be used, therefore the consent given to the computational treatment is never true consent and consequently the implementation of the right to self-determination cannot ever be fully effective.

A problem, which occurs only in the field of data protection regulation with regards to AI, concerns the need of identifying the purposes for which the treatment is carried out. The first paragraph of article number 6 of the GDPR states that the consent must be given by the data subject, ‘to the processing of his or her personal data for one or more specific purposes’. In addition, the second paragraph of article n. 9 repeats the same rule with regards to, ‘(...) special categories of personal data (...)’ for example ‘(...) data concerning health.’ However, in the course of the development of AI software the purposes of data processing are not always fully predictable because the system learns and evolves autonomously.⁵³ Moreover, even when the purpose of the data processing is fully known to the designer of the AI system, it could be necessary to use large amounts of personal information which has been collected on the basis of consent given by data subject for purposes other than development of the AI system. An example of this is EyeArt, an AI software capable of detecting serious eye diseases in diabetic patients with a degree of accuracy of approximately 95%. To develop this AI system, it was necessary to analyze and classify a large database of health data which had been collected from people located in different geographical areas of the world for medical diagnosis or treatment purposes; therefore, for purposes other than the implementation of an intelligent screening system. It is clear that a re-use of personal data such as this could not realistically proceed through a new interrogation of all data subjects. Therefore, the re-use of health data should be permitted without requesting a new expression of consent.

In addition, computational methods and, particularly, deep learning methods could obstruct the data subject in exercising the right to withdraw the consent at any time and this right is one of the specific conditions fixed by the third paragraph of article n. 7 GDPR with regards to the treatment legally based on self-

⁵⁰ Expression coined by S Rodotà, *La vita e le regole. Tra diritto e non diritto* (Feltrinelli, 2006) 81.

⁵¹ See: rec. n. 4 GDPR.

⁵² See: Cass., ord. 25th May 2021, n. 14381, at www.leggiditalia.it.

⁵³ See G Olivi, ‘Big data, metadati e intelligenza artificiale’ [2020] *Dir. ind.* 181.

determination.

Most of the critical issues highlighted above do indeed arise whenever the consent of the data subject serves as a legal basis for processing personal information in scientific research, regardless of the methods by which it is carried out.⁵⁴

In consideration of such set of problems, the European legislator has paved the way for the processing of personal data justified by legal grounds other than the consent of the data subject. Specifically, the second paragraph of article number 9, GDPR allows for the processing of sensitive data for, '(...) reasons of public interests in the area of public health (...)', '(...) scientific research purposes (...)' and '(...) statistical purposes (...)' (see Lett. I & J, GDPR), aside from the explicit consent of the data subject.

Nevertheless, even with the reference to the processing of data based on one of the grounds mentioned above, the European legislator has established certain legal requirements which computational techniques cannot adhere to. Consequently, even when Big Data and AI applications are developed for scientific research or public health purposes, these types of technology will not be able to fully comply with privacy legislation.⁵⁵ Therefore, for example, Letter A of the first paragraph of article number 5, GDPR states that, 'Personal data shall be processed [...] in a transparent manner in relation to the data subject (...)' (principle of transparency), whereas a characteristic of AI is its opaque mode of functioning. In addition, Letter B of the same paragraph prescribes that, 'Personal data shall be (...) collected for specified, explicit (...) purposes (...)', whereas computational techniques and self-learning approaches prevent the designer from predicting every potential use of the collected data. Furthermore, Letter C of the first paragraph imposes the principle of, '*Data Minimalization*' which conflicts with the large amount of information which is usually necessary to develop AI systems.

It is clear, then, that computational innovation and related advantages in the medical sector could be curbed by privacy guarantees and, consequently, it is desirable that the legislator should adjust the latter to include new technologies.⁵⁶ In the meantime, current data protection legislation should be interpreted from an evolutionary perspective to achieve a reasonable balancing between data protection and health promotion. In this direction, some jurists have highlighted that lot of rules, laid down by GDPR to govern the processing of personal data, contain general clauses that is to say terms and concepts which are not precisely formulated and, therefore, can be applied in varying degrees depending on

54 G Comandè, 'Ricerca in sanità e data protection' (n 45) 187 ss.; A Bernes, 'La protezione dei dati personali nell'attività di ricerca scientifica' (2020) 1 NLCC 175 ff.

55 G Finocchiaro, 'Intelligenza artificiale e protezione dei dati personali' [2019] GI 1657, explains that GDPR was designed without considering issues which raise from AI technology and Big Data.

With regards to the topic of data protection, Artificial Intelligence Act Proposal states only that, 'To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.'

56 See: Olivi, G Olivi, 'Big data' (n 53) 185; A Cinque, 'Privacy, Big-Data e contact tracing: il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute' [2021] NGCC 957 ff.

contextual circumstances.⁵⁷

Therefore, the principle of '*Data Minimization*' should be interpreted precisely and fully when personal information is transferred to an entrepreneur in a commercial relationship for economic purposes.⁵⁸ However, this should be interpreted in a broader sense when the health data is shared with a doctor in a therapeutical setting for medical research purposes.⁵⁹

6. Perspective and conclusions.

The use of AI in the medical field has already highlighted some of the limits of the logic of self-determination. Further limits could emerge from the expansion of AI applications in the near future, that is unless the legislator intervenes to control them.⁶⁰

First, computational technology could be applied to an even-greater extent to guide people in their personal decisions. Once the numerous traces strewed by the user online have been collected and profiled, the predictive algorithms are able to create and transmit impulses which gradually and imperceptibly induce the user to make choices predetermined by other people. As the President of the Italian Data Protection Authority has been highlighting,⁶¹ 'This is a very strong type of nudging (...) which shows how vulnerable people are in the face of digital power (...) and how the freedom of choice is actually more of an illusion than real.'⁶²

Therefore, when algorithms guide the user on health-related issues, the exercise of right to self-determination will conceal the result of a process of determination which is taken by a third party.⁶³ Which is particularly worrying, when therapeutic decision affects not only the health of subject who makes it but also the collective health. For instance, this is the case when deciding whether or not to get vaccinated against contagious diseases.

This scenario stresses the idea that the voluntaristic logic is becoming more and more precarious in the face of the developments of AI. This technology not only reveal intrinsic limits of individual self-determination, as we have seen in the previous paragraphs, but also threatens individual self-determination as an external agent.

57 A Ottolia, *Big Data e innovazione computazionale* (Giappichelli 2017) 101 ff.

58 Ibid 131.

59 See: D Mastrelia, 'Gestione dei bigdata in una prospettiva orientata alla tutela della privacy degli individui' [2018] *Dir. ind.* 364 ff.; T Sharon, 'Data- driven Decision Making' (n 489 42 f.; McGraw, K. D. Mandl, *Privacy Protection to Encourage Use of Health-relevant Digital Data in a Learning Health System* [2021] *Digit. Med.* 6. See also: Judgement of 22nd June 2021, *Latvijas Republikas Saeima*, C-439/19, EU:C:2021:504, paragraphs 105-106.

60 See n 63 below.

61 P Stanzione, *Annual Report* (2020).

62 A broad explanation of the nudging is in R H Thaler, C R Sustein, *Nudge: Improving Decisions About Health, Wealth and Happiness* (Yale University Press, 2008). On the same topic see also: C R Sunstein, *Human Agency and Behavioral Economics. Nudging Fast and Slow* (Springer 2017); R Viale, *Oltre il nudge* (Il Mulino, 2018).

63 Considering such negative effects, the recent Artificial Intelligence Act Proposal forbids, '... the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm ...'

Another perspective, which is worthy of being considered, concerns the role of AI in the implementation of Human Enhancement.⁶⁴ Human Enhancement consists of technologies and tools which can be used to improve physical and/or mental capacity of an individual overcoming normal human standards. For example, neuronal microchips can be used to increase mnemonic and concentration abilities and in addition, genetic engineering can be used to intensify muscular strength or sensorial capacity. The development of such techniques has possible implications with regards to the principle of self-determination in the medical field. To understand what these implications could be, it is useful to consider that Human Enhancement interventions affect not only the condition of the specific patients but also rights, principles and values which go beyond the individual sphere; for example, the improvement of sensorial capabilities of certain persons might endanger privacy protection.⁶⁵ Moreover, Human Enhancement in the private medical sector could infringe the principle of equality and Human Enhancement in the public sector could aggravate the budget for public healthcare and therefore affect the collective health. Finally, Human Enhancement seems to be in contrast with the principle of human dignity which safeguard the uniqueness of each human being.

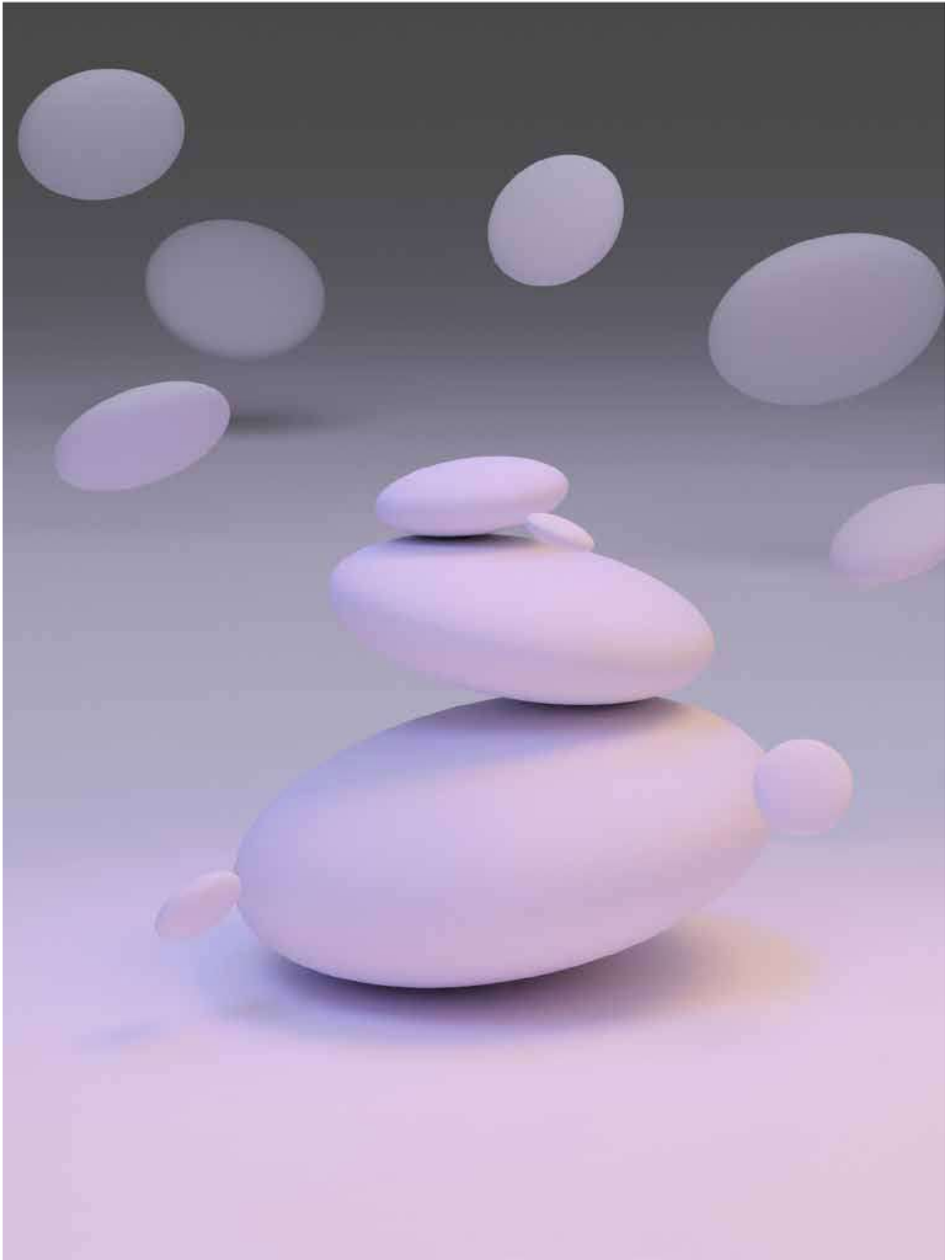
Some authors are of the opinion that the issues mentioned above can be overcome, and that individual self-determination is sufficient to legitimise Human Enhancement practices. This opinion has been argued from the point of view that self-determination in medical field can now even legitimise the patient's death.⁶⁶ However, this latter point is not sufficiently decisive to solve the problem with the lack of legality of Human Enhancement techniques. In fact, the elimination of a human life actually represents something less, not something more than the obliteration of human condition and dignity.

In the first paragraph, we considered the idea that the advent of new technology has often has effects on one or more areas of application of the law. At the end of this paper, it is useful to add that the advent of new technology often implicates the reconsideration of some legal doctrine. For example, the spread of motor vehicles has triggered a process that led to the debunking of the idea that fault is the only possible basis for civil liability. Later, the introduction of digital technology and telematics undermined the real nature of the protection of copyright, sometimes even causing the latter to be degraded to a mere right to compensation. At present, medical applications of AI seem to prompt a critical rethinking of the voluntaristic "dogma", highlighting that the right to self-determination cannot be conceived as an absolute prerogative. On the one hand, it postulates the full capacity of the individual to understand and decide in his own interest and, on the other hand, it is subject to comparison with other rights and principles, which sometimes present an autonomous ultra-singular scope, and, therefore, should be considered prevailing.

64 On the issues related to human enhancement, see: Comitato Nazionale per la Bioetica, Report 'Diritti umani, etica medica e tecnologie di potenziamento (enhancement) in ambito militare' (22nd February 2013).

65 E Palmerini, 'Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea' [2016] Resp. civ. prev. 1820.

66 U Ruffolo, A Amidei, 'Intelligenza artificiale e diritti della persona: le frontiere del "transumanesimo"' [2019] GI 1658 ff.





Automated Decision Making and right to explanation. The right of access as ex post information.

EMILIANO TROISI

Ph.D. (c.) in Humanities and technologies: an integrated research path at Università degli Studi Suor Orsola Benincasa di Napoli

Abstract

The data sets, the processes that determine an algorithmic decision, the rationale of a certain automated decision affecting the legal sphere of a natural person should be traceable, transparent, explained; this is also in order to enable the individual affected to challenge the contents of an unfair decision. Instead, they are rarely so: either by choice - for reasons of competition, of protection of know-how - or because of technological limitations: this is the case of those algorithms that appropriately are referred to as 'black-box'; systems whose inferential mechanisms are not (completely) predictable ex ante or which, in any case, do not always make it possible to explain why an automated decision-making model has generated a particular outcome (and what combination of factors contributed to it). Having affirmed the existence of an ethical duty to transparency of the algorithm and explanation of the (individual) decision reached by automated means, this Paper wonders whether there is a corresponding right on the level of positive law - and what are its limits, of legal but also technological nature. Critically drawing on the most important scholarly opinions on the subject, the right to explanation of the automated decision-making is identified, in the context of the GDPR, in the right of access under Article 15 of the Regulation.



Keywords: Automated Decision Making; algorithm; opacity; explanation; right of access; Gdpr.

Summary: [1. Introduction: Automated Decision Making and the problem of algorithm opacity.](#) – [2. GDPR: 'meaningful information' between 'generic algorithm functionality' and 'right to explanation'.](#) – [3. The right of access as ex post information.](#) – [4. Right to explanation: the functional implication between information and contestation of the automated decision.](#) – [Conclusions.](#)

1. Introduction: Automated Decision Making and the problem of algorithm opacity.

The expression Automated Decision Making (acronym: A.D.M.), refers - broadly - to any process that enables, through the use of technological means, decision making without, or at least with irrelevant, human involvement. Such a definition, therefore, does not imply - being broader - but clearly includes, the use of Artificial Intelligence technologies, as more generally any computer technique that, relying on algorithms - namely, a sequence of operations executable by a processor¹ - enables repetitive tasks to be performed with data without the need for constant human guidance.²

Among these, AI systems - according to one of the most widely accepted definitions - are distinguished as, essentially, rational systems³ capable of '*acting and thinking humanly*';⁴ in other words, capable of solving problems by imitating what human behavior would be under similar circumstances. An intelligent system is capable of collecting data from a certain data base or environment, interpreting it,⁵ and - in light of the goal to be achieved - deciding what the best action or decision is,⁶ then acting accordingly in an almost automatic way.⁷ This decision-making process is conducted by the machine - according to the AI

¹ Treccani online, entry: algoritmo, <https://www.treccani.it/vocabolario/algoritmo/>

² Within the *State-of-the-Art Report on Algorithmic decision-making by Algo:aware*, a December 2018 study commissioned by DG Connect (Directorate General for Communications Networks, Content and Technology), Department of the European Commission, decision making algorithm is more broadly defined as "A software system – including its testing, training and input data, as well as associated governance processes – that, autonomously or with human involvement, takes decisions or applies measures relating to social or physical systems on the basis of personal or non-personal data, with impacts either at the individual or collective level." Consequently, "the definition of algorithmic decision-making is to be interpreted as a decision taken by a decision-making algorithm".

³ S Russell, P Norvig, *Artificial Intelligence: A Modern Approach*, (Prentice Hall, 2009). For further information, as to the more strictly legal sphere, it seems useful to refer also to M Durante, entry *Intelligenza artificiale. Applicazioni giuridiche*, *Digesto Italiano*. (Terza appendice di aggiornamento della IV edizione. *Discipline Privatistiche*, Vol. II, II Agg.), 714.

⁴ M Somalvico, F Amigoni, V Schiaffonati, *Intelligenza Artificiale*, in S Petruccioli (ed.), *Storia della scienza*, (vol. IX, Istituto della Enciclopedia Italiana, Roma, 2003), 615-624; VV. AA., *Artificial Intelligence and life in 2030, One hundred year study on Artificial Intelligence* (Stanford University Press, 2016) 5.

⁵ Reasoning about them or processing the information inferred from the data.

⁶ Possibly changing the environment (natural or virtual) in which it operates or otherwise proposing some output, the solution to a specific problem.

⁷ Cf. the definition developed by the Expert Group established by the European Commission: *A definition of AI: Main capabilities and scientific disciplines*, High-Level Expert Group on Artificial Intelligence (AI HLEG), (Brussels, December 18, 2018).

technique implemented - by applying static reasoning schemes or by resorting to machine learning techniques (e.g. *machine learning*, *deep learning*, *neural networks*, *decision trees* and others). Without going into detail, it suffices to know - for present purposes - that in the latter case the machine, instead of executing pre-defined behavioral patterns, processes 'on its own' and dynamically - in application of self-learning and adaptive algorithms - the decision rule; in some cases resulting, therefore, also in being able to better respond and adapt to changes in the environment or refine, with use experience, the ability to generate an appropriate *output*.⁸

These techniques make AI an incredibly useful tool, capable of making decisions and predictions much earlier and more accurately than humans would, moreover in contexts that require the analysis of huge amounts of data - often unstructured⁹ - that would otherwise be prohibitive for human agents.

AI, however, can make mistakes.¹⁰ The use of Automated Decision Making systems can lead to decisions that are biased, harmful to human beings, discriminatory, and detrimental to fundamental human rights; jeopardizes the human right to free and equal access to goods and services and information; not to be unknowingly manipulated by unfair, aggressive and intrusive forms of marketing; it threatens - as this Paper will show - the legitimate claim to challenge harmful decisions made by the machine or, more importantly, to have them not made in a non-transparent manner and on the basis, perhaps, of incorrect and incomplete data.¹¹

The initial myth of algorithmic neutrality has now been shattered;¹² intelligent machines are created, programmed and trained by human operators and therefore, like humans, are fallible; they can 'reason', or 'learn to reason' in a biased way.¹³ The inferential rules given to the machine by its programmer - by which it then interprets knowledge and operates in its target environment - may

⁸ *Amplius*, s. Y Bathaee, *The Artificial Intelligence Black Box And The Failure of Intent and Causation*, in *Harvard Journal of Law & Technology*, (2018) Vol. 31, n.2, 890.

⁹ This is the case for using self-learning algorithms

¹⁰ So opens the European Commission's *White Paper on Artificial Intelligence* - COM(2020) 65 final, February 19, 2020: "*Artificial Intelligence [...] will change our lives by improving healthcare (e.g. making diagnosis more precise, enabling better prevention of diseases), increasing the efficiency of farming, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the security of Europeans, and in many other ways that we can only begin to imagine. At the same time, Artificial Intelligence (AI) entails a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes.*"

¹¹ Among others, see B Casey, *Title 2.0: Discrimination Law in a Data-Driven Society*, [2019] J. L. & MOB., 36, <https://doi.org/10.36635/jlm.2019.title>; K Crawford, *The Hidden Biases in Big Data*, [2013] HARV. BUS. REV., <https://perma.cc/E95C-TUQU>; see also, E Troisi, *AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla 'intelligibilità' dell'algoritmo*, in *European Journal of Privacy Law & Technologies*, (2019)1, at: <https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1027/276>

¹² See, M Airoidi, D Gambetta, *Sul mito della neutralità algoritmica*, *The Lab's Quarterly*, (2018) XX, 4, 29

¹³ J Burrell, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, *Big Data & Society*, (2016)1, 1-12, for whom the claim that algorithms classify information, and thus make decisions, in a more "objective" way cannot be taken literally given the degree of human judgment involved in the design of the algorithms themselves, particularly from the standpoint of defining clustering criteria, pre-classifying training data, and adjusting thresholds and decision-making parameters.

reflect cultural biases, even well-meaning and unintended ones.¹⁴ In data-driven systems, such as machine learning systems, moreover, biases can also arise from data collection, which may be insufficient, incomplete, or flawed; from training, due to biases induced by human interpretation of the data, in the case of supervised-learning algorithms, or - when un-supervised - as a result of online learning and self-adaptation through user interaction (think of common rank algorithms).

These biases can lead to unfair decisions.¹⁵ And this situation is further aggravated by the opacity that often characterizes these systems, which is reflected in the possibility of contesting the decision made by automatic means.¹⁶

The data sets, the processes that determine the decision of the algorithms, the reason for a certain decision affecting the legal sphere of a natural person should be traceable, transparent, explained; this is also in order to enable the individual affected by it to contest its content. Instead, they are rarely so, at least adequately: either by choice¹⁷ - for reasons of competition, protection of know-how - or because of technological limitations: this is the case of those algorithms that are properly referred to as 'black-box', systems whose inferential mechanisms are not (completely) predictable *ex ante*¹⁸ or which, in any case, do not always make it possible to explain why a model has generated a particular result or decision (and what combination of factors contributed to it).¹⁹

The emergence of these problems and the growing concern, partly due to the fear that mistrust of new technological tools might limit their diffusion in the market, led to the adoption of a series of Ethical Charters - public or even private - at all levels: international, European, national.²⁰

¹⁴ On how classification systems can be and are concretely influenced, even with far-reaching consequences, by the 'point of view' of those who construct them, see the interesting work by GC Bowker, SL Star, *Sorting Things Out: Classification and Its Consequences*, (Cambridge, MA, The MIT Press, 1999).

¹⁵ See, on the point *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on Artificial Intelligence, (8 April 2019); *Statuto Etico e Giuridico dell'IA*, Fondazione Leonardo, (2019).

¹⁶ See, among others, J Burrell, op. cit., for whom "opacity seems to be at the very heart of new concerns about 'algorithms' (operating on data) among legal scholars and social scientists".

¹⁷ The fortunate appellation of 'Black Box Society' is due to Frank Pasquale, who masterfully outlines its features with evocative expressions such as 'the Secret Judgments of Software' and 'the Secrecy of Business and the Business of Secrecy'; cf. F Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, (Harvard University Press, 2015).

¹⁸ But it is sometimes possible - it should be noted - to investigate its behavior by analyzing the responses the system produces in response to the stimuli it receives. So-called 'explanatory tools' [or *post-hoc* explanation techniques, c.f. J Zhong, E Negre, *AI: To interpret or to explain?*, (INFORSID, 2021)] are capable of *ex-post* reconstructing the functioning of certain 'opaque' decision-making models; in particular results of the examined model would be explained by finding the links between input data characteristics and results, or by constructing a simpler model to approximate the original model (*Ibid.*, 6); the accuracy and reliability of these 'explanations' is challenged, for example, by C Rudin, *Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead*, in *Nature Machine Intelligence*, (2019) Vol. 1, No. 5, 206– 215.

¹⁹ J Burrell, op. cit., 3, with whom it is easy to agree, distinguishes 3 types of opacity in decision-making algorithms, which he describes as follows: "Three distinct forms of opacity include: (1) opacity as intentional corporate or institutional self-protection and concealment and, along with it, the possibility for knowing deception; (2) opacity stemming from the current state of affairs where writing (and reading) code is a specialist skill and; (3) an opacity that stems from the mismatch between mathematical optimization in high-dimensionality characteristic of machine learning and the demands of human- scale reasoning and styles of semantic interpretation". S. also, Y Bathaee, op. cit.; D Castelvocchi, *Can We Open the Black Box of AI*, in *Nature*, (2016) Vol. 538, 20.

²⁰ A successful but already incomplete attempt to map the various Ethical Charters, Declarations of Principles, or Guidelines, classified by geo-political context and analyzed by content, is credited to A Jobin,

Based on the idea that - as digital technology becomes an increasingly central part of all aspects of human life - people should be able to trust such technology²¹ and it should be developed to serve humans, be ethical, and respect fundamental rights, a set of principles and requirements have been identified to which intelligent systems, their applications, producers, programmers, and users (i.e., all stakeholders) should adhere. Leverage, or one of the main levers, of this strategy for 'human-centric' and 'trustworthy' AI²² - to use the words of the Expert Group on Artificial Intelligence appointed by the European Commission²³ - is precisely transparency.²⁴ Often, a prerequisite for ensuring that basic human rights and ethical principles are respected, protected, and promoted.²⁵

If Artificial Intelligence is to be developed at the service of human beings, humans must be able to make use of it consciously:²⁶ they have the right to always be aware of the fact that they are interacting with an A.I. system;²⁷ they must be able to understand its purpose, capabilities, and operating mode ('explicability') and the decisions, to the extent possible, must be explainable to those directly or indirectly affected by them²⁸ ('explainability') so that they can

M Ienca, E Vayena, *Artificial Intelligence: the global landscape of ethics guidelines*, [2019] Nat. Mach. Intell. To name a few of the most relevant ones: *First Draft Of The Recommendation On The Ethics Of Artificial Intelligence*, SHS/BIO/AHEG-AI/2020/4 REV.2, Ad Hoc Expert Group (AHEG) for the preparation of a draft text of a recommendation on the ethics of artificial intelligence, United Nations Educational, Scientific and Cultural Organization (UNESCO), (7 September 2020); *Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems*, Council of Europe, CM/Rec(2020)1; more dated and limited to the Justice field: *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, European Commission For The Efficiency Of Justice (CEPEJ), (December 2018); In European Union context: *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on Artificial Intelligence, (8 April 2019); in Italy is to be noted the paper edited by the Task force sull'Intelligenza Artificiale dell'Agenzia per l'Italia Digitale, *Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*, (2018). Famous among the privately authored declarations of principles is the one drafted within the *Future of Life Institute* and signed by some 1,800 researchers and nearly 4,000 other endorsers, some as famous as Stephen Hawking or digital market giants like Elon Musk and Jaan Tallinn: *The Asilomar AI Principles*, 2017, <https://futureoflife.org/ai-principles/>

²¹ In this sense, *White Paper on Artificial Intelligence. A European approach to excellence and trust*, European Commission, COM(2020) 65, (February 19, 2020).

²² See, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, *Building Trust in Human-Centric Artificial Intelligence*, COM(2019) 168 final, 8 april 2019

²³ See the above-mentioned High-Level Expert Group on Artificial Intelligence (AI HLEG), *Ethics Guidelines for Trustworthy AI*, 8 April 2019

²⁴ See, *First Draft of The Recommendation on the Ethics of Artificial Intelligence*, Ad Hoc Expert Group (AHEG) for the preparation of a draft text of a recommendation on the ethics of artificial intelligence, United Nations Educational, Scientific and Cultural Organization (UNESCO), SHS/BIO/AHEG-AI/2020/4 REV.2, (7 September 2020), III (2) §39, according to which "transparency may contribute to trust from humans for AI systems". See also the document compiled by the US National Institute of Standards and Technology (NIST): Vv. Aa., *Four Principles of Explainable Artificial Intelligence*, available online, in draft version, doi: <https://doi.org/10.6028/NIST.IR.8312-draft>

²⁵ Cf., Ad Hoc Expert Group (AHEG) UNESCO, Ibid., III (2) §37. On the relationship between transparency and trust, see, H Felzmann, E Fosch-Villaronga, C Lutz, A Tamó-Larrieux, *Transparency you can trust: transparency requirements for artificial intelligence between legal norms and contextual concerns*, Big Data & Society, (2019)1, 1-14; J Schoeffera, Y Machowska, N Kuehla, *A Study on Fairness and Trust Perceptions in Automated Decision Making*, (2021), online in arXiv: arXiv:2103.04757v1

²⁶ See, Vv. Aa., *Paper sui Principi etici*, in *Statuto Etico e Giuridico dell'IA*, Fondazione Leonardo, (2019)

²⁷ See, *Ethics Guidelines for Trustworthy AI*, High-Level Expert Group on Artificial Intelligence, (8 April 2019), §78.

²⁸ Ibid., §53

challenge its modalities and content ('contestability'²⁹), being able to resort to human intervention to that end.

Therefore, if there exists an undisputed ethical duty of transparency³⁰ of the algorithm and explanation of the (specific) decision reached by automated means (ADM), it need to be addressed the question of whether there is - and to what extent - a corresponding right on the level of positive law, and what are its limits, of legal but also technological nature.

General legal framework of reference (to be investigated)³¹, at least in cases where automated decision-making involves personal data of natural persons is given by Regulation (EU) 2016/679, the General Data Protection Regulation.³²

²⁹ To explainability refers Section III (2) §40 of the *First Draft of The Recommendation on the Ethics of Artificial Intelligence*, Ad Hoc Expert Group (AHEG) – UNESCO, cit., according to which: “*Explainability refers to making intelligible and providing insight into the outcome of AI systems. The explainability of AI systems also refers to the understandability of the input, output and behaviour of each algorithmic building block and how it contributes to the outcome of the systems. Thus, explainability is closely related to transparency, as outcomes and sub-processes leading to outcomes should be understandable and traceable, appropriate to the use context*”.

³⁰ According to the findings of the study conducted in 2019 by A Jobin et al. (s., A Jobin, M Ienca, E Vayena, *Artificial Intelligence: the global landscape of ethics guidelines*, op. cit., 7 ff.) ‘transparency’ is the most prevalent principle in the current literature, present in 73 of the 84 documents analyzed, albeit with different shades of meaning, summarized by the locutions: ‘transparency, explainability, explicability, understandability, interpretability, communication, disclosure, showing’.

³¹ Specific regulations may be found, however, for example, in the area of consumer protection legislation; for an overview of the situation and specific problems, see, among others, M Grochowski, A Jablonowska, F Lagioia, G Sartor, *Algorithmic transparency and explainability for EU Consumer Protection: unwrapping the regulatory premises*, *Critical Analysis of Law*, (2021) Vol. 8, No.1, 43-63.

³² On April 21, 2021, the EU Commission published a proposal for a Regulation for Artificial Intelligence, the so-called *AI Act*, which aims to define the regulatory framework for the development and deployment of artificial intelligence systems. According to a progressive regulatory approach based on risk - which can be unacceptable (whereby the system is banned), high, or low or minimal - AI systems considered to be high risk will be allowed on the European market under certain mandatory requirements and subject to certification of compliance. Among these requirements is transparency. Indeed, Article 13 of the Proposal requires that high-risk systems be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately, and be provided with precise instructions for appropriate use. For other systems, deemed to be of lower risk, only very limited transparency requirements are imposed, e.g., in terms of providing information to signal the use of an AI system in interactions with human beings; moreover, with broad exceptions that have already been met with several criticisms (think, for example, of the non-applicability of the transparency requirement to biometric recognition systems used for crime prevention and detection purposes). This is not the appropriate place to extend the discussion to an analysis of the AI Act's regulatory framework; however, a few brief points cannot be ignored. First, given that Artificial Intelligence requires massive processing of data, very often personal data, it is abundantly clear that the future AI Regulation will have to function in a complementary way to the GDPR, harmonizing with its provisions and obligations, possibly specifying and/or integrating it with reference to the peculiarities of ‘intelligent’ systems; however - precisely on the very point of a clear connection between the two disciplines - the Proposal seems lacking, with the risk of engendering regulatory gaps (even serious) or uncertainties, even with regard to the roles and competences of the Notifying Authorities involved. In addition, however, to the concerns related to the lack of adequate harmonization with the General Data Protection Regulation (for censure see Joint Opinion No. 5 /2021 by EDPB and EDPS on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence; online here: https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en), what is worrying about the proposal under comment is the inadequacy, in terms of the provision of protection mechanisms (including for the many exceptions) and redress-that is, mechanisms that would allow users who suffer detrimental automated decisions to obtain a direct remedy-(absent), to go beyond the discipline of Art. 22 GDPR, which does not cover the full scope of potentially harmful automated decision-making systems and is-as will be seen-in many ways precarious, thus the subject of long-standing criticism in doctrine. Even from the specific point of view of transparency, since it is not always possible - also due to technological limitations we will discuss below - to obtain a prior comprehensible explanation of the results produced by the machine, the

2. GDPR: 'meaningful information' between 'generic algorithm functionality' and 'right to explanation'.

Article 22 GDPR expressly states³³ the right of the data subject 'not to be subject to a decision based solely on automated processing, including profiling³⁴, which produces legal effects concerning him or her or similarly significantly affects him or her.' The prohibition, under paragraph 2 of the same article, does not apply only if, and to the extent that, automated decision-making processing is necessary for the conclusion or performance of a contract between the data subject and a data controller or is based on the data subject's consent.³⁵

Overlooking the scope of this exemption - also, not the only one³⁶ - which

EDPB and the EDPS do not fail to point out (see Joint Opinion No. 5/2021, cit, in particular: §72) how the Artificial Intelligence Regulation should promote new, more proactive, and timely ways of informing users of AI systems about the decision-making status the system is in at any given time, providing early warnings about potentially harmful outcomes so that people whose rights and freedoms might be compromised by the machine's autonomous decisions are able to react to or challenge those decisions.

³³ This is not, however, a legislative innovation, since the problem of automated decision-making was already addressed, with a less extensive prohibitive provision than the current one, by Article 15 and Recital 41 of Directive 95/46/EC. *Amplius*, among others, see LA Bygrave, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, in *Comput. Law Secur. Rev.*, (2001)17, 17-24.

³⁴ The Regulation does not give a precise definition of automated processing; however, Article 22(1) expressly includes profiling in its scope. Under Art. 4, profiling, in the context of the GDPR, means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." Profiling is thus a species of automated processing that consists in the exercise, by a software, of an inferential operation capable of deriving, from a certain amount of data entered in a data-set - analyzed and identified among them, automatically, statistical correlations - other data related to characteristics or behavioral patterns attributable to a given individual or groups of them in order to classify him/her in precise groups or categories and/or predict probable future behavior.

³⁵ It should be emphasized that automated processing and profiling involving sensitive data as referred to in Article 9 of the GDPR are prohibited in any case, unless the data subject has given his or her explicit consent or this is authorised under special legal basis by Union or Member States' laws and provided that, the processing is necessary for reasons of public interest and proportionate to the goal pursued. The data processed then, pursuant to Art. 5 of the Regulation, for (automated) processing to be lawful, must be collected for specified, explicit and legitimate purposes, and subsequently processed in a way that is not incompatible with those purposes. However, as has been aptly noted, the machine learning underlying ML systems involves existing datasets and other real-time data streams in complex dynamic processes with sometimes not entirely predictable outcomes, which are difficult to reconcile with the need for full prior identification of the purposes of the processing to be consented to ex ante, to the point that some go so far as to cast doubt on the very possibility of giving truly informed consent to processing entrusted to black-box systems (see C Kuner, DJB Svantesson et al, *Machine learning with personal data: is data protection law smart enough to meet the challenge?*, *International Data Privacy Law*, (2017) vol. 7, no. 1, 1.

³⁶ the GDPR also admits, in fact, that it may be permissible - pursuant to paragraph 2(b) of the article under consideration - to take decisions on the basis of automated processing in other cases contemplated by Union or Member State law to which the data controller is subject; this, exceptionally, even without the consent of the data subject and provided that appropriate measures are taken to protect the natural persons involved. According to Recital 71 of the Regulation, these hypotheses may include, for example, the use of computerized processing for the purposes of monitoring or preventing fraud or tax evasion, but in any case it must be considered necessary - in the author's opinion - that the use of such mechanisms proves to be justified in the light of the pursuit of purposes of significant public interest and that the related compression of the rights and freedoms of the individuals involved be proportionate. In these cases, the Regulation only requires the Legislator to provide for appropriate measures to protect individuals, but the right to request

allows, in essence, Automated Decision Making under the "consensual" bases for processing³⁷ - considered to be suitable, at least in theory, to ensure a broader awareness of the data subject³⁸ - it is provided that in cases where automated decision-making is permitted, the data controller has a duty - pursuant to Art. 22(3)GDPR - to implement appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, including, in particular, measures that guarantee the data subject's right to obtain human intervention by the data controller, to express their opinion and to contest the decision.

Further requirements for the case of automated decision-making as defined in Article 22 are laid down in Articles 13 (2)(f), 14 (2)(g) and 15 (1)(h) of the Regulation. These provisions, with identical wording, prescribe - respectively in the context of the information (so for Articles 13 and 14), and as an extension of the right of access (Article 15) - that the data subject has the right to be informed about "the existence of automated decision-making, including profiling, as referred to in Article 22(1) and (4), and, at least in such cases, [to receive, *ed.*] meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".

The data controller (of ADM processing) is therefore under a specific duty to provide information, and thus transparency (involving: existence of an automated decision-making process; meaningful information on the logic of the algorithm; significance and envisaged consequences of such processing for the data subject); and if it is true - as has been argued - that in the structure of the GDPR, the objective of the security of the movement of personal data turns out to be entrusted to a strategy focused, first and foremost, on the transparency of data processing³⁹, it is evident that the duty of transparency in question must be interpreted, in any case, more broadly than the 'minimum content' of information already due for any other processing. Any other 'reductive' interpretation, would, in fact, make the specification of the European legislator completely superfluous; not to mention that a more protective regulation - thus a wider notion of

human intervention and to possibly challenge the decision is not ensured by paragraph 3 of Article 22 (as it is in the other cases examined), although nothing, of course, precludes that the rules authorizing such processing, in providing the required safeguards, may provide for even broader forms of protection. *Amplius*, s. G. Malgieri, *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, in *Computer Law & Security Review*, (2019) 35(5). <http://dx.doi.org/10.1016/j.clsr.2019.05.002>

³⁷ See, E Troisi, *AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla 'intelligibilità' dell'algoritmo*, in *European Journal of Privacy Law & Technologies*, (2019)1, online: <https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1027/276>

³⁸ With the consequence that the processing should be considered unlawful in all cases in which the data subject has not expressly consented to it through his or her own conscious manifestation of will, either directly, or as part of a more complex contractual relationship, on the assumption, however, in the latter case, that the automated processing is to be considered necessary for the conclusion or execution of the agreement. For further analysis of the effectiveness of the informed consent mechanism in the digital environment to ensure awareness, and thus protection of the data subject, see IA Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, [2018] *Osservatorio del diritto civile e commerciale*, 67-106; and the recent L Gatt, IA Caggiano, R Montanari (eds.), *Privacy and Consent. A Legal and UX&HMI Approach for Data Protection*, (Suor Orsola University Press, 2021), which address the topic with an empirical approach and statistical dignity, accompanying the legal reading with behavioral analysis.

³⁹ C.f. R. Messinetti, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, *Contratto e Impresa*, (2019) 3, 861.

transparency - would be well justified because of the greater (potential) harmfulness of automated individual decision-making compared to other data processing⁴⁰; this is precisely the reason why the legislator decided to regulate ADM with a prohibition rule (albeit with many exceptions).

Following this guideline, the information referred to in Articles 13(2)(f), 14(2)(g) and 15(1)(h) of the Regulation (i.e., the 'logic' of the algorithm and the 'envisaged consequences') must certainly consist of more than the indication in concise, transparent, intelligible, and easily accessible form⁴¹ of the categories of data processed and the purpose of the processing, as well as its automated mode.⁴² The question is whether such a duty of transparency, however, extends to the point of being able to consider legally enshrined in positive law a right of the natural person subject to the processing to the algorithm's 'disclosure'-that is, at least to something more than the general functional logic implied by the system, a right to 'open the black box'⁴³ and look inside it-and, more than that, a right to the 'explanation' of the specific decision affecting him or her and affecting his or her legal sphere: the reasons, the individual circumstances why a specific decision, with a certain content, was taken by the algorithm with respect to him or her.⁴⁴

As has been acutely observed,⁴⁵ Articles 13(2)(f) and 14(2)(g), which impose a duty of transparency to be performed, precisely, in the context of the privacy information - at a time, therefore, logically preceding the decision-making processing - can only refer to the general functionality of the algorithm and to the pattern of decisions normally expected from its operation through an abstract and *ex ante* evaluation ('envisaged consequences' indeed says the Regulation). The content of the data subject's informational right - referring to these legal bases - is therefore necessarily limited and certainly unsuitable to substantiate a duty to 'explain' the automatic decision. However, the reference to "meaningful

⁴⁰ When automated processing is also likely to produce legal effects or otherwise significantly similarly affect the natural person whose data are being processed, it is no longer just the data-subject's privacy that is at stake but his or her right not to be discriminated against, to have free and equal access to goods and services not to be manipulated without his or her knowledge by unfair, aggressive, and intrusive forms of marketing, but also the legitimate claim to challenge detrimental decisions by a machine or, more importantly, that these are not taken in a non-transparent manner and on the basis, perhaps, of incorrect and incomplete data.

⁴¹ C.f. Recital 39 GDPR.

⁴² According to B Goodman, S Flaxman, *European Union Regulations on algorithmic decision-making and a "right to explanation"*, *AI Magazine*, (2017) vol. 38, n. 3, 50-57 or available online at: <https://arxiv.org/abs/1606.08813v3>, "It is reasonable to suppose that any adequate explanation would, at a minimum, provide an account of how input features relate to predictions, allowing one to answer questions such as: *Is the model more or less likely to recommend a loan if the applicant is a minority? Which features play the largest role in prediction?*"

⁴³ The expression is from R Messinetti, q.v., op. cit.

⁴⁴ It should be noted that Recital 71 of the GDPR expressly mentions the data subject's right to "explanation," in these terms: "[...] such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision." However, as Wachter et al. point out, after a careful analysis of all the preparatory work, this wording, originally included in the proposed Regulation, is later expunged from the text finally submitted for legislative approval; c.f., S Wachter, B Mittelstadt, L Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, *International Data Privacy Law*, (2017) vol. 7, no. 2, (Oxford University Press, 2017), 76–99. It also reconstructs the genesis of the provision in question, C Djeflal, *The normative potential of the European rule on Automated Decisions: a new reading for Art. 22 GDPR*, *ZaöRV* (2020) 80, 847-879.

⁴⁵ C.f., S Wachter, B Mittelstadt, L Floridi, op.cit.

information," "significance," and "envisaged consequences" for the data subject requires the data controller, if not certain a disclosure of the algorithm functioning⁴⁶, at least to illustrate, in an easily accessible form, the main criteria for its operation⁴⁷, while also providing "information about the intended or future processing, and how the automated decision-making might affect the data subject."⁴⁸ The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision⁴⁹ and express valid consent under Article 4 GDPR.⁵⁰ For example, consider a loan file that is fully processed online whereby a bank relies on profiling algorithms to identify the applicant's creditworthiness score (credit scoring) and then decide whether to grant or reject the loan and what interest rate to propose.⁵¹ Where the decision is based solely (c.f. Art. 22 GDPR) or otherwise substantially on such a score, the data controller will have to explain to the data subject that he or she will be evaluated by an algorithm and how this works - not the mathematical formula, but rather how the system actually 'reasons' - thus, what information is taken into account (e.g., employment and income situation; degree of indebtedness; credit history; etc.); what are the sources (e.g., what are the data provided by the data subject in the application form or obtained from third parties; data already collected from previous reports; information from public records; etc.); what circumstances mainly affect the decision and how (e.g., by identifying a possible case history; by resorting to simulations); how users are ranked (how

⁴⁶ In the sense of the non-necessity of disclosure of the algorithm, in order to comply with the minimum level of transparency required by the Regulation, see Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, No. 251, (Oct. 3, 2017), for which "The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm".

⁴⁷ Complexity is not an excuse for failing to provide information to the data subject. Recital 58 states that the principle of transparency is "of particular relevance in situations where the proliferation of actors and the technological complexity of practice makes it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him are being collected, such as in the case of online advertising". In the light of an interpretation that looks at the context of the regulatory provisions - in particular the requirements of clarity, intelligibility, accessibility, and plain language that preside over the information the data subject is generally entitled to under Art. 12 (1) GDPR - it must be excluded that the European legislator wants to refer to a duty of mere 'disclosure' of the algorithm, especially if intended in its mathematical guise as i.e. system architecture, having rather to consider that what is pertinent here, and it is up to the data controller to explicate - perhaps in addition to the mathematical function that substantiates the algorithm in question - is its concrete performance: the context in which it is applied, the purposes pursued, the techniques applied and perhaps even examples about its concrete functioning. Only by including such circumstances in the content of the disclosure should the "explanatory" duty that the regulation requires be considered fulfilled.

⁴⁸ In this sense Article 29 Working Party, op. cit., p. 26, also adding that "in order to make this information meaningful and understandable, real, tangible examples of the type of possible effects should be given."

⁴⁹ Thus, verbatim, Article 29 Working Party, op. cit., p. 25.

⁵⁰ On this point, see, for example, the recent ruling of the Italian Supreme Court (Cass., sez. 1 Civ, 25/05/2021 no. 14381, Ord.) on the validity of the consent given by the user who did not have prior knowledge of the performing scheme of an algorithm (in this case a rating algorithm, used by the defendant to process users' reputational profiles); speaking precisely of "lack of transparency of the algorithm," the Court in fact affirmed that for the processing of personal data, consent is validly given only if it is freely and specifically expressed with reference to a clearly identified processing, with the consequence that "in the case of a web platform (with associated computer archive) designed to process the reputational profiles of individuals, based on a computational system with at its base an algorithm aimed at establishing reputational scores, the requirement of awareness of the data subject cannot be considered met where the algorithm's concrete functioning scheme and the elements of which it is composed remain unknown or not knowable by the data subjects.

⁵¹ The case is evoked in Recital 71 of the Regulation.

many and what ranks are considered, based on score); how and how much the score affects the credit application outcome. To make this information (cf. *significance* and *envisaged consequences* of such processing) *meaningful* and understandable, real and concrete examples should be given of the kind of possible decisions and effects for the data subject.⁵² The data controller should also briefly explain to the data subject what measures are taken to avoid, for example, algorithm malfunctions and biases, and inform him or her that he or she has the right to request the review of the decision by invoking human intervention (cf. Art. 22(3) GDPR). In addition to this,⁵³ the controller should also make it clear

⁵² Italics refer to Articles 13(2)(f) and 14(2)(g) GDPR.

⁵³ When it comes to algorithmic procedural activity of the public administration, that is, when automated decision-making systems are used in public decision-making, the minimum content of the duty of transparency imposed on the data controller (in this case, a public entity in the exercise of an authoritative power) is much more defined, thanks to the already intense interpretative contribution of case law. The Council of State (Consiglio di Stato, the Italian administrative judge), in particular, in ruling no. 8472/2019 [see comments by A Mascolo, *Gli algoritmi amministrativi: la sfida della comprensibilità*, *Giornale di diritto amministrativo*, (2020) 3, 366 ff; M Timo, *Algoritmo. Il Procedimento di assunzione del personale scolastico al vaglio del Consiglio Di Stato*, *Giur. It.*, (2020) 5, 1190] - in part recalling but overruling precedent No. 2270/2019 - affirming a general principle, states (para 15.1), in interpreting what it calls the principle of knowability, i.e., the principle - introduced by the GDPR - whereby everyone has the right to know about the existence of automated decision-making processes concerning him or her and, in this case, to receive meaningful information about the logic involved, that "*such a right [...] must be accompanied by mechanisms capable of deciphering its logic. In this view, the principle of knowability is complemented by the principle of comprehensibility [...].*" More specifically, it clarifies how (para 13.1) "*the mechanism through which the automated decision (i.e., the algorithm) is implemented must be 'knowable,' according to a strengthened declination of the principle of transparency, which also implies that of the full knowability of a rule expressed in a language different from the legal language. Such knowability of the algorithm must be ensured in all aspects: from its authors to the procedure used for its elaboration, to the decision mechanism, including the priorities assigned in the evaluation and decision-making procedure and the data selected as relevant*"; so, the "*technical formula*" must be accompanied "*by explanations that translate it into the 'legal rule' underlying it and make it readable and understandable.*" This is "*in order to be able to verify that the criteria, prerequisites and outcomes of the robotized procedure comply with the requirements and purposes established by the law or by the administration itself upstream of that procedure, and so that the methods and rules under which it was set are clear - and consequently open to review.*" [author's translation]. The absence of such a minimum level of comprehensibility (could be said, explanation) of the algorithm constitutes, in the opinion of the Council of State, such a vice as to invalidate the entire procedure (and consequent measures) for being its entire method censurable for lack of transparency. It is clear, however, and the writer of the cited ruling makes this explicit, that such an interpretation of the rules of the Data Protection Regulation, which are general in nature and therefore applicable both to decisions taken by private parties and, as in this case, by public bodies, is affected, however, in the latter case, by the concurrent effectiveness of the principles already governing public action: in particular, the principle of knowability set forth in the GDPR, interpreted in the aforementioned terms, constitutes in this specific case, more than anything else, "*direct specific application of Art. 42 of the European Charter of Fundamental Rights ('Right to a good administration')*", where it states that when the Public Administration intends to take a decision that may have adverse effects on a person, it has an obligation to hear the individual before acting, to allow him or her access to its archives and documents, and, finally, [...] to 'give the reasons for its decision.'" More extensively, on transparency and the necessary 'comprehensibility of the decision-making algorithm used in the exercise of administrative activity, see G Fasano, *L'intelligenza artificiale nella cura dell'interesse generale*, *Giornale di diritto amministrativo*, (2020) 6, 715.

In France, it is the legislator who by LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (<https://www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo/texte>) amended the Code des relations entre le public et l'administration providing for the introduction of Art. L. 311-3-1 for which "*Sous réserve de l'application du 2° de l'article L. 311-5, une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande*". Rule further specified with the Décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique (<https://www.legifrance.gouv.fr/eli/decret/2017/3/14/PRMJ1632786D/jo/texte>) providing for the introduction of Art. R. 311-3-1-1 ("*La mention explicite prévue à l'article L. 311-3-1 indique la finalité*

that the user has the right to know (have access to) the score assigned to him by the algorithm and the rationale - i.e., the logical premises - for this ranking; this point will be addressed in the next section, after a necessary introduction.

3. The right of access as *ex post* information.

As mentioned above, it can be easily agreed that the transparency obligations in Articles 13(2)(f) and 14(2)(g) GDPR do not seem suitable to ground an actual right of the data subject to an *ex post* explanation of the automated decision; nevertheless, an equally restrictive interpretation of Art. 15(1)(h) of the Regulation, variously justified, in the scholarly literature, on the wording of the regulatory provision⁵⁴ - identical to that of the above articles⁵⁵ - or on the assumption that the right of access has the same scope and purpose as the right to information.⁵⁶

Within the framework of the analyzed rules - which the GDPR provides for the protection of the natural person in the case of Automated Decision Making - the oversight power attributed to the data subject is embodied not only in the right to information, but also in the right to obtain human intervention and especially to challenge the decision generated by the algorithm.⁵⁷ In this system of safeguards for the data subject, which bases the lawfulness of automated decision-making processing on his or her consent (in a broad sense), the information required by Articles 13 and 14 GDPR - as it has been here outlined - fulfills the important function of enabling the data subject to exercise, with awareness, his or her right

poursuivie par le traitement algorithmique. Elle rappelle le droit, garanti par cet article, d'obtenir la communication des règles définissant ce traitement et des principales caractéristiques de sa mise en œuvre, ainsi que les modalités d'exercice de ce droit à communication et de saisine, le cas échéant, de la commission d'accès aux documents administratifs, définies par le présent livre") and Art. R. 311-3-1-2 ("L'administration communique à la personne faisant l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, à la demande de celle-ci, sous une forme intelligible et sous réserve de ne pas porter atteinte à des secrets protégés par la loi, les informations suivantes : 1°) Le degré et le mode de contribution du traitement algorithmique à la prise de décision ; 2°) Les données traitées et leurs sources; 3°) Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé; 4°) Les opérations effectuées par le traitement). Moreover, the principles are the object of Décision n° 2018-765 DC du 12 juin 2018 del Conseil Constitutionnel which appears to give them a narrow reading. Available at the link: <https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.htm>.

On algorithmic decision-making in the French legal system, s., G Malgieri, *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, Computer Law & Security Review, (2019) 35(5), 13. <http://dx.doi.org/10.1016/j.clsr.2019.05.002>.

⁵⁴ See, S Wachter, B Mittelstadt, L Floridi, op. cit.; G Finocchiaro, *Intelligenza artificiale e diritto. Intelligenza artificiale e protezione dei dati personali*, Giur. It., (2019) 7, 1657, according to which there would not be granted a full right to explanation under Art. 15 GDPR, the wording of the provision precluding it, assuming a "lack of harmony" between it and Recital 71 of the Regulation.

⁵⁵ For S Wachter, B Mittelstadt, L Floridi, op. cit., this provision, mentioning the "envisaged consequences" of the decision-making processing would unequivocally refer, in this case as in Articles 13 and 14, to a necessarily *ex ante*, and therefore limited, 'explanation': in essence, no explanation at all.

⁵⁶ Along these lines, Article 29 Working Party, Op. cit., p. 27, concludes as follows: "Article 15(1)(h) says that the controller should provide the data subject with information about the envisaged consequences of the processing, rather than an explanation of a particular decision".

⁵⁷ See, R Messinetti, op. cit.; C Malgieri, G Comandè, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, International Data Privacy Law, (2017) Vol. 7, No. 4; ME Kaminski, *The Right to Explanation, Explained*, Berkeley Technology Law Journal, (2019) 34, 189–218.

to manage (i.e., give, withdraw, restrict, etc.) consents⁵⁸, while the right of access would add to this same function the additional one (in this specific context) of enabling him or her to effectively challenge - because duly informed - the harmful decision.

In spite of the almost identical wording of Articles 13 (2)(f) and 14 (2)(g), on one side, and Art. 15 (1)(h), on the other, it is not possible to make a symmetrical interpretation: while in the context of the information notice the information due can only refer to the generic functionality of the algorithm and to the sorts of decisions normally expected from its operation, in the case of the right of access it is more appropriate to interpret the rule extensively, deriving from it a duty of information, for the data controller, that is more significant and detailed and that pertains to the specific decision - possibly already taken by the system towards the data subject - and to the inferential stages that led (the machine) to that given output⁵⁹: an *ex post* explanation.

Going back to the example of the online loan, it is reasonable to think - given these premises - that the right of access accorded by the GDPR to the data subject - the applicant, in the example - extends to the score, i.e., the profile, assigned to him by the rating algorithm that would define his creditworthiness; this is in fact - on closer inspection - an applicant's personal data, while also, at the same time, the product of a profiling process, thus decisive for the purposes of the automatic decision of the loan application in which he is interested. Knowing this data, in addition to being a right of the data subject (Art. 15 GDPR), is also essential so that he or she can, for example, assess its accuracy, perhaps request its rectification (or in general exercise the further rights over his or her own data set forth in Art. 16 to 20 of the Regulation);⁶⁰ properly challenge the

⁵⁸ Of a role of the Information Notice as a tool meant to enable the data subject to exercise control over data processing, speaks IA Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, op. cit.; S Mazzamuto, *Il principio del consenso e il potere della revoca* in R Panetta (ed.) *Libera circolazione e protezione dei dati personali*, (Milano, Giuffrè, 2006), 1004.

⁵⁹ Of this opinion, among others: C Malgieri, G Comandè, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, op. cit.; TW Kim, BR Routledge, *Why a Right to an Explanation of Algorithmic Decision-Making Should Exist: A Trust-Based Approach*, in *Business Ethics Quarterly*, (2022) Vol. 32, Issue 1, 75 – 102. <https://doi.org/10.1017/beq.2021.3>.

⁶⁰ If this were not the case, the rights of rectification, erasure and restriction of processing (recognized under Articles 16, 17 and 18 GDPR, respectively) would, paradoxically, inevitably be undermined precisely in those cases where they would be most needed: profiling and, more generally, data analytics techniques, involving elements of 'prediction' and 'extrapolation', greatly increase the inherent risk of data inaccuracy (output) and expand the range of data processed, making it more difficult for the data subject to control them. In the interpretation aimed at here, the information referred to in Article 15 GDPR, would be considered to be functional to the exercise of these rights (as well as that of challenging the decision based solely on automated data processing, in the case of ADM). Cf. on the point, with reference to profiling, Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, No. 251 of October 3, 2017, WP 251 rev01, English version, p.18, according to which, verbatim, 'The rights to rectification and erasure apply to both the 'input personal data' (the personal data used to create the profile) and the 'output data' (the profile itself or 'score' assigned to the person)'. On the (broad) content of the right of access in the case of inference, s. C Malgieri, G Comandè., Op. ult. cit., p. 246, who also enhances in this sense the scope of Article 20 GDPR, which recognizes the data subject's right to data portability in a readable format. Article 20, on this point, however, is recognized as having a far lesser scope by Article 29 Working Party, which excludes data produced by algorithmic activity of the data controller from the scope of the obligation: see in particular, *Guidelines on the right to data portability*, Article 29 Working Party, No. 242, (December 13, 2016), WP 242 rev.01, p.10 ff. [recently referred to and confirmed by *Guidelines on the targeting of social media users*, EDPB, No. 8, (September 2, 2020)].

automatic decision (e.g., the non-granting of the loan or its undesirable conditions). Admittedly, the profile - the rank assigned to the score determined by the algorithm - expresses behaviors or characteristics that are probable, expected, but which as legally relevant (to the granting or terms of the loan) must nonetheless be reasonably inferred from the data of the data subject, who must therefore be enabled to assess such reasonableness and "express his or her point of view" (cf. Art. 22(3)). In order for this to happen, the information the data controller is required to provide (as per Art. 15) cannot have the same content as the *ex-ante* Information; it cannot simply explain in an understandable way how the algorithm supposedly works, rather it should -sticking to the example above - indicate the score assigned; identify the concrete reasons for it (i.e., at least the specific circumstances that weighed in the judgment); explain (or at least report in an 'intelligible' way) why that score resulted in the rejection of the application and perhaps what different score or characteristic would have led to a different outcome.⁶¹

4. Right to explanation: the functional implication between information and contestation of the automated decision.

The interpretation of the right of access as a right to an *ex post* information (or rather, at this point, it should be said, explanation) of the ADM-decision is, in this writer's opinion, the natural consequence of a systematic and consistent reading of paragraph 1(h) of Article 15 of the General Data Protection Regulation. As seen, in fact, Article 22 GDPR, in paragraph 3, expressly provides for the right of the data subject affected by an ADM process to question the decision based solely on automated processing through the possibility of obtaining human intervention, namely, to interact in a 'dialectical' way to the data controller, expressing his or her opinion, requesting a verification of the decision and also being able, subsequently, to contest its assumptions. This is a right, on closer inspection, which, unless its scope being frustrated, must necessarily imply, for the data subject (and therefore owed by the data controller), a specific information on the functioning of the decision-making algorithm; an information that is not abstract and prognostic, but concrete and *ex-post*,⁶² referring to the specific application that concerns him/her; only in this way, in fact, would the data subject be put in a position to fully exercise his/her oppositional right, having the appropriate instruments to formulate a specific and reasoned contestation.⁶³ It is

⁶¹ The last reference is to the so-called counterfactual explanations technique; see, S Wachter, B Mittelstadt, C Russell, *Counterfactual explanations without opening the Black box: automated decisions and the GDPR*, *Harvard Journal of Law & Technology*, (2018) Vol. 31, No. 2.

⁶² In the sense intended by S Wachter, B Mittelstadt, L Floridi, *op.cit.*, p. 6, according to which "an *ex post* explanation occurs after an automated decision has taken place" and "[...] can address both system functionality and the rationale of a specific decision". See also, TW Kim, BR Routledge, *op. cit.*

⁶³ Among others, s. AD Selbst, J Powles, *Meaningful information and the right to explanation*, *International Data Privacy Law*, (2017) Vol. 7, Issue 4, 233-242. <https://doi.org/10.1093/idpl/ix022>. Kaminski speaks of a 'qualified' transparency, to be defined precisely because of its functional nexus with the exercise of the other rights accorded to the data subject, not least the right to contest the automatic decision: ME Kaminski, *op. cit.*, according to which "there is a clear relationship between the other individual rights the GDPR establishes—contestation, correction, and erasure—and the kind of individualized transparency it requires."

arguably not coincidental that Recital 71 of the Regulation⁶⁴ - which, unlike the regulatory text, expressly mentions the right of the data subject to "obtain an explanation" - explicitly relates this safeguard to the right to "obtain human intervention" and to be able to "express his or her opinion" about the automatic decision. The functional implication link between information and contestation is, it would seem, also reinforced by the Explanatory Report accompanying the so-called Convention 108+ of the Council of Europe - i.e., the Protocol of Amendment, signed by Italy, which, in updating the 1981 Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data to the new technological context, expressly adds in the new Article 9 (titled: Rights of the Data Subject), subpar. a, the right of every individual "*not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration*" - where, in § 75a, it emphasizes how the right of access is actually functional to the possibility of effective review of the automatic decision: "*It is essential that an individual who may be subject to a purely automated decision has the right to challenge such a decision by putting forward, in a meaningful manner, his or her point of view and arguments. [...]*".⁶⁵

The right of access, furthermore, as can also be seen from Recital 63 GDPR, gives the data subject the right to obtain all the information referred to in Art. 15 of the Regulation, not only at a time prior to or coinciding with the beginning of the processing, but also during the course of the processing, and necessarily extends even to those data (and processes) in the meantime 'produced' by the processing, i.e., to the data inferred from the processed data (input) as a result

This suggests something interesting about transparency: the substance of other underlying legal rights often determines transparency's substance. If one has a right of correction, one needs to see errors. If one has a right against discrimination, one needs to see what factors are used in a decision. Otherwise, information asymmetries render underlying rights effectively void." (Ibid. p. 213). It should be noted how also in the ruling no. 8472/2019 of the Council of State (Consiglio di Stato, the Italian administrative judge) – see *supra* footnote 53 - in justifying a stronger concept of transparency, functional to the judicial review of the algorithmic decision in the administrative field, it is pointed out that (para 13. 3) Article 15 GDPR, unlike Articles 13 and 14, has the merit of providing for a right enforceable by the data subject and not an obligation to the data controller, and also allows to overcome the time limits set by Articles 13 and 14, allowing the subject to acquire information even if the processing [...] has even already generated a decision. Also recognizing the existence of a right to ex post explanation of the individual automatic decision are Kim T.W. and ROUTLEDGE B. R., op. cit., who, however, motivate by valuing the informed consent in cases of algorithmic decision-making processing, which they consider based on a duty of information that is not instantaneous (and ex ante) but continuous and pivotal, a "right to an updating explanation."

⁶⁴ It should be noted that although not binding, the Recitals are a guide to the interpretation of norms. See, in the case law, CJEU, Judgment of the Court (Third Chamber) of 13 July 1989, *Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung*, c. 215/88. ECLI:EU:C:1989:331. See also, European Commission, *Guide to the Approximation of EU Environmental Legislation ANNEX* (Environment, 2015), according to which: "*Recitals explain the background to the legislation and the aims and objectives of the legislation. They are, therefore, important to an understanding of the legislation which follows.*"

⁶⁵ May it be useful to also refer here to the High Level Expert Group on Artificial Intelligence (AI HLEG), which in the paper published on April 8, 2019, and significantly titled *Ethics Guidelines for Trustworthy AI*, after identifying a number of fundamental principles, including fairness, which the new technological framework should be inspired by to be "trustworthy," significantly states significantly states that the procedural dimension of fairness implies the ability to challenge decisions developed by AI systems and the possibility of effective contestation against them. To this end, decision-making processes must be explainable. Furthermore, specifically on explicability, it is added (p.13): "*This means that processes need to be transparent, the capabilities and purpose of AI systems openly communicated, and decisions – to the extent possible – explainable to those directly and indirectly affected. Without such information, a decision cannot be duly contested.*"

(even if only intermediate) of the automated process (of extrapolation, clustering, etc.),⁶⁶ which, if referable to the data subject in the terms of Art. 4 (1), fall within the objective scope of the GDPR.⁶⁷ These inferred data, in fact, in addition to being the 'basis' of a possible (successive) automated decision able to affect the legal sphere of the data subject, are themselves already the 'output' of an automated processing (e.g. data analytics, profiling etc.)⁶⁸ with respect to which the right of access stands out, therefore, as a legitimate request for *ex post* information. At least in this circumstance - moreover, not necessarily coinciding with the scope of Art. 22 GDPR, but referable to a much broader number of cases contemplating profiling or in any case a data processing (including non-automated) that involves predictive or, broadly speaking, inferential elements⁶⁹ - the right of access must be considered, in fact, certainly referring to a much broader information content than that covered by Articles 13 and 14 of the Regulation, embracing not only detailed information on the personal data used as input to the processing⁷⁰ (i.e., in the case of profiling, the data used to create the profile) but also all possible information on the output data (e. g. the profile or score assigned to the data subject; all data 'derived' from the analysis of his or her personal data and the circumstances inferred).⁷¹ When, furthermore, the

⁶⁶ Recital 63's reference to data such as "diagnoses, examination results, assessments by treating physicians..." are in fact *ante-litteram* examples of inferred data; technological innovation and artificial intelligence applied to data analytics models make far greater and more invasive 'inferences' possible. See, B Mittelstadt, S Wachter, *A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI*, Columbia Business Law Review, (2019)1.

⁶⁷ Cf. Article 29 Working Party's *Opinion 4/2007 on the concept of personal data*, available online here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm; on the personal data nature of inferences, s. also, B Mittelstadt, S Wachter, *Op. ult. cit.*, p. 25 ff.

⁶⁸ Data mining and profiling activities, even if not preordained to a decision-making moment, are in themselves already potentially detrimental to individual interests deserving of protection, as the European Court of Human Rights has noted on several occasions (see, ECHR, Guide to the Case-Law of the of the European Court of Human Rights. Data protection., 30 April 2021, online at: https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf), in addition to raising specific problems regarding the protection of 'produced' data, particularly when they have the nature of sensitive data. See, B Mittelstadt, S Wachter, *Op. ult. cit.* The problem has been particularly prominent regarding health data; *amplius*, W Schäfke-Zell, *Revisiting the definition of health data in the age of digitalized health care*, [2021] International Data Privacy Law; G Malgieri, G Comandè, *Sensitive-by-distance: quasi-health data in the algorithmic era*, Information & Communication Technology Law, (2017) Vol. 26, No. 3, 229-249.

⁶⁹ *Amplius*, B Mittelstadt, S Wachter, *Op. ult. cit.*

⁷⁰ their origin, the purpose for which they are processed, and any other information required under Article 15 GDPR.

⁷¹ If this were not the case, the rights of rectification, erasure and restriction of processing (recognized under Articles 16, 17 and 18 GDPR, respectively) would, paradoxically, inevitably be undermined precisely in those cases where they would be most needed: profiling and, more generally, data analytics techniques, involving elements of 'prediction' and 'extrapolation', greatly increase the inherent risk of data inaccuracy (output) and expand the range of data processed, making it more difficult for the data subject to control them. In the interpretation aimed at here, the information referred to in Article 15 GDPR, would be considered to be functional to the exercise of these rights (as well as that of challenging the decision based solely on automated data processing, in the case of ADM). Cf. on the point, with reference to profiling, Article 29 Working Party's *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, No. 251 of October 3, 2017, WP 251 rev01, English version, p.18, according to which, verbatim, '*The rights to rectification and erasure apply to both the 'input personal data' (the personal data used to create the profile) and the 'output data' (the profile itself or 'score' assigned to the person)*'. On the (broad) content of the right of access in the case of inference, s. G Malgieri, G Comandè., *Op. ult. cit.*, p. 246, who also enhances in this sense the scope of Article 20 GDPR, which recognizes the data subject's right to data portability in a readable format. Article 20, on this point, however, is recognized as having a far lesser scope by Article 29 Working Party, which excludes data produced by algorithmic activity of the data controller from the scope of the obligation: see in particular, *Guidelines on the right to data portability*, No.

processing (i.e., the inference) is automated and is functional to the adoption of a decision having legal effects for the data subject (based solely on the quality of that inference) - and at least in this case⁷² - all (further) 'meaningful information about the logic used' by the algorithm that such output has (already) generated must also be considered to be included in the information due; and this is not, evidently, prognostic and abstract information about the functioning of the algorithm in general, but more realistically the reasons for the decision (the output produced) in concrete terms; the logic used in that specific case, the how and why.⁷³ an explanation. The only limit, as to the contents of this explanation, is given by the protection of the trade secret and intellectual property of the data controller and pertains to the (*full disclosure* of the) formula of the decision-making algorithm, which Recital 63 GDPR significantly contemplates precisely with reference to the right of access; moreover, explicitly underlining its nature of not an absolute limitation, but rather subject to judicious balancing, case-by-case, with the opposing interest (to the explanation and contestability of the decision) of those subject to the automated process (and never suitable, in any case, to justify the refusal to provide information to the data subject).⁷⁴

It is the essential need for effective protection of the human person against digital power⁷⁵ that demands for the meaning of Art. 15(1)(h) GDPR to be reconstructed in such a way as to ensure that the data subject has communication of all data concerning him or her: including those 'inferred'; can assess its accuracy, completeness, relevance (to the extent that the Regulation and the purposes of processing allow); and, where that data forms the basis of an (automated) decision that affects (or is likely to affect) his or her legal interests, has access to at least all the information necessary to assess, and possibly sustain an effective contestation of it (by recourse to a human interlocutor or a courtroom).⁷⁶

If the digital world has become a 'social', living space, within which a person's

242, Article 29 Working Party, (December 13, 2016), WP 242 rev.01, p.10 ff. (recently referred to and confirmed by EDPB's *Guidelines on the targeting of social media users*, No. 8, September 2, 2020).

⁷² The reference is to the wording of Art. 15(1)(h) GDPR, intended as alluding to something more than the minimum content of transparency and safeguard that is generally required under Articles 13 and 14, and that is in this case, since in an *ex-post* scenario, possible.

⁷³ Thus the expression 'significance [...] of such processing' in Art. 15(1)(h) GDPR is intended to be interpreted in this perspective and context (i.e., of information intended to reach the data subject after the decision).

⁷⁴ See, G Noto La Diega, *Against the Dehumanisation of Decision-Making. Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (JIPITEC), (2018)9, Vol. 3, No.1, Available at SSRN: <https://ssrn.com/abstract=3188080> (s. in particular p. 23, para 69).

⁷⁵ In addition to the general principle of fair processing, to which certainly can be said to be contrary the refusal, when unjustified, to provide information about the derived data referable to the data subject or about the rationale for a certain automatic decision.

⁷⁶ For R Messinetti, *op. cit.*, p. 867, the legal-technological system must enable the person to understand the machine's understanding of that person in the context of decision-making processes directed to affect his or her legal and vital sphere; it would therefore be the need to retain control over one's personal identity (and its formation) that would justify an interpretation of the right of access as a right to understand the logic and justifying reasons for the automated decision (having as its object precisely that identity) and one's personal data "derived" from the original inputs, which constitute the intermediate and/or conclusive outputs of the processing.

'onlife'⁷⁷ existence takes place and is delineated, i.e., his or her identity is determined, in a way that is (also) legally relevant (and otherwise uncontrolled), then the protection of human dignity - anchor of all data protection legislation - individual freedom, and the fundamental right of each person to affect his or her individual and collective dimension, goes first and foremost through awareness, i.e. transparency meant as the justification of digital power – namely, its explanation -and, only then, through an active power of control over one's own data - particularly automatically inferred data - and the possibility of contain (and contesting) the impact of technologies on and from them, which without a (prior) right to explanation would be voided. Denying *this* transparency, which ultimately means not only the right to know the rationale for a certain automatic decision affecting a natural person but also the relevant (inferred) data behind it (i.e., who that person *is* online) is to somehow dehumanize the individual.⁷⁸

Conclusions.

Having postulated the possible legal basis of a right to an explanation of the algorithmic decision, it is necessary, in conclusion, to dedicate at least a mention to its limitations, although this is neither the object nor the goal of this Paper.⁷⁹

On a legal level, a first limitation would derive from the rather limited scope of Art. 22 GDPR,⁸⁰ at least basing on the literal wording of the article. Automated processing to which Article 15(1)(h) of the GDPR is applicable are in fact only those defined by Article 22 of the regulation, i.e., expressly, only processing that are “*decision-making*”,⁸¹ in other words, lead to decisions affecting the data subject, and are “*based solely on automated processing*”.⁸² These decisions (of

⁷⁷ The evocative term is from Luciano Floridi, who chose it to represent man's experience in hyper-historical societies in which he “no longer distinguishes between online or offline” and even becomes increasingly “unreasonable to ask whether one is online or offline.” Cf. L Floridi, *The Fourth Revolution. How the Infosphere is reshaping human reality*, (Oxford University Press, 2014); Id. (ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, (Springer, 2015).

⁷⁸ Such an understanding of transparency can be found, for example, in R Waelen, *Why AI Ethics Is a Critical Theory*, *Philosophy & Technology*, (2022) 35:9. <https://doi.org/10.1007/s13347-022-00507-5>

⁷⁹ Please refer for further to the larger work of this same author, E Troisi, *Decisione algoritmica, Black-box e AI etica: il diritto di accesso come diritto a ottenere una spiegazione*, *Jus Civ.*, (2022)4, 953 – 975.

⁸⁰ In this sense, see, among others, S Wachter, B Mittelstadt, L Floridi, op. cit.

⁸¹ This implies that all those data processing that is not typically 'inferential,' i.e., where the use of computer techniques is limited, perhaps, to the storage and/or organization of personal data without involving any analytical and/or evaluative passage of them through the application to the data-set of deductive rules algorithmically defined in the model, are excluded from the scope of the Article.

⁸² The literal interpretation of the provision would therefore require that only fully automated decisions fall within the scope of application of the discipline under examination, while excluding all those in which it is possible to detect even the slightest human involvement that can variously 'interfere' with the automated decision-making process, being able to verify or modify the decision but also, for example, merely ratify it. Such an interpretation would risk excluding from the scope of application of the strict protection regulation under consideration a good portion of decisions that are in essence the outcome of automated processing and only formally applied by human, merely passive, intervention. Therefore, a broad interpretation of Article 22 GDPR should be more appropriately preferred, considering included in the scope all decisions that are 'automated in substance,' even those, then, that involve some human intervention in the decision-making process, but this intervention is irrelevant to the content of the decision: in this sense, see, for example, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, No. 251, Article 29 Working Party, (October 3, 2017), 21, where, verbatim: “*The controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies*

which the individual affected would be entitled to an explanation), according to Article 22 (1) of the Regulation, in addition to this, must also "*produce legal effects [concerning the data subject] or [at least] similarly significantly affect him or her.*" The effect of such decisions should therefore affect, by denying or limiting it, the free exercise of a right of the individual recognized by the legal system.

However, of this last clause,⁸³ as of the entire §1 of Article 22 GDPR, it is also possible to make a broad interpretation, as many scholarly opinions have already convincingly argued; this first limitation on the right to explanation therefore seems to have most likely negligible impact.⁸⁴

A more important limitation on the right to explanation of automated decision-making outcome, on the other hand, lies in the need to balance the right of the individual subject to ADM to be adequately informed about how the algorithm works and the right - opposed - of those who developed and use the algorithm for economic purposes to keep its design secret in order to avoid dispersing its commercial value to the benefit of competitors. According to Recital 4 of the GDPR, "*the right to the protection of personal data is not an absolute right; it must be [...] balanced against other fundamental rights, in accordance with the principle of proportionality*" and the Regulation "*respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties [...]*" including "*[...] freedom to conduct a business [...]*". More specifically, Recital 63, on the right of access, textually states that "*that right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the*

automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data". And before that, the British Data Protection Authority, the Information Commissioner's Office (ICO), also observed a similar orientation, for which: "*the interpretation of the word 'solely' in the context of Article 22(1) [...] is intended to cover those automated decision-making processes in which humans exercise no real influence on the outcome of the decision, for example where the result of the profiling or process is not assessed by a person before being formalized as a decision*" C.f.r., *Feedback request – Profiling and automated decision-making*, Information Commissioner's Office, (2017), 19, also referenced in G Malgieri, G Comandè, *Right to legibility of automated decision-making*, op. cit.

⁸³ In fact, the catalog of rights potentially affected by automated decision processing widens considerably where all those fundamental personal rights of constitutional rank are also taken into account; these are expressed in a broad form, such as freedom of expression, freedom and secrecy of correspondence, freedom of movement, freedom of worship, the right of defense and, most of all, the principle of non-discrimination: naturally 'elastic' rights and freedoms, which lend themselves to covering a whole open range of individual legal situations that may be exposed to concrete risk, for those who hold them, in the event of conflicting, and unjust, decisions by an Artificial Intelligence. This broad protection of individual rights, is then further expanded by the very following of the provision; §1 of Art. 22 in fact extends its scope also to those ADM cases which, while not affecting legal situations overtly qualified as rights, "affect [however, ed.] in a similar and significant way the person," i.e. - in the interpretation that seems preferable - affect, and seriously impact (this is the meaning to be attributed to the expression 'significantly') legitimate interests or otherwise legitimate claims of the human person as long as they are not merely factual, i.e., legal situations that the legal system, although it does not recognize as rights immediately enforceable by the individual, considers equally worthy of protection either by granting them some measure of safeguards or at least by demonstrating an overall judgment of reprehensibility toward practices and behaviors that threaten their free and full individual fruition. See, on this point, among others, G Malgieri, G Comandè., *Right to legibility of automated decision-making*, op. cit.; see also E Troisi, *AI e GDPR: l'Automated Decision Making, la protezione dei dati e il diritto alla 'intelligibilità' dell'algoritmo*, op. cit.

⁸⁴ See E Troisi, *Decisione algoritmica, Black-box e AI etica: il diritto di accesso come diritto a ottenere una spiegazione*, Jus Civ., (2022)4, 953 – 975, and footnotes no. 81, 82, 83.

software”, with the clarification that “however, the result of those considerations should not be a refusal to provide all information to the data subject”. In this, echoing, among other things, the recent Council of Europe Recommendation⁸⁵ according to which “States should establish appropriate levels of transparency with regard to [...] use, design and basic processing criteria and methods of algorithmic systems [...]” and “the legislative frameworks for intellectual property or trade secrets should not preclude such transparency, nor should States or private parties seek to exploit them for this purpose”⁸⁶, which, moreover, undoubtedly gives priority, among the protected situations, to the right of individuals to be properly informed.

The issue is far from irrelevant, considering that most of the automatic decision-making algorithms, even very invasive and used - including those of Google and Facebook, to be clear - are proprietary and kept confidential as to their mechanism. In general, it can be said - but this is especially with regard to the area of Competition, for which more case law is given - that the case law of the Court of Justice⁸⁷ allows limitations or exceptions to copyright and trade secret⁸⁸ in “exceptional circumstances”,⁸⁹ that is, when conflicting and equally important general interests or fundamental rights are at stake (within the limits of what is proportionate to the purpose).⁹⁰

In any case, an assessment among all the interests at stake should be required on a case-by-case basis, bearing in mind that when decision-making processes affect individuals, the degree of necessary ‘explainability’ of the algorithm (and its decision), based on the context, should increase as the severity of the consequences (on human rights and the interests at stake) increases if such output is incorrect or otherwise inaccurate. And that anyway, in the author’s opinion, when serious human rights impacts are to be expected, transparency may also require the sharing of specific algorithms or data sets.⁹¹

The last limitation to be addressed is the technological one: the question is whether the data subject’s right to explanation of the algorithmic decision that affects him or her - namely, to receive, ex post, ‘meaningful information’ about the logic concretely used in that specific automated decision-making process that concerns him or her - does not encounter, once overcome the legal limits, a technological limitation capable of hindering its actual enforcement.

⁸⁵ The reference is to Council of Europe, Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.

⁸⁶ Article 4.1

⁸⁷ See: CJEU, Judgment of the Court of April 6, 1995, Joined Cases C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98 (so-called Magill); CJEU, Judgment of the Court (Fifth Chamber) of April 29, 2004, C-418/01, ECLI:EU:C:2004:257 (so-called IMS Health); CJEU, Judgment of the Court of First Instance (Grand Chamber) of September 17, 2007, T-201/04, ECLI:EU:T:2007:289 (Microsoft v. Commission).

⁸⁸ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

⁸⁹ See the just-mentioned Court of Justice of the European Union rulings Magill, IMS Health and Microsoft v. Commission.

⁹⁰ For a more detailed analysis, please refer to E Troisi, *Decisione algoritmica, Black-box e AI etica: il diritto di accesso come diritto a ottenere una spiegazione*, Jus Civ., (2022)4, 953 – 975

⁹¹ For more on this issue, see among others, G Malgieri, *Trade Secrets v Personal Data: a possible solution for balancing rights*, International Data Privacy Law, (2016), 6(2):ipv030. Available online at: <http://dx.doi.org/10.1093/idpl/ipv030>; G Noto La Diega, Op. cit.; ME Kaminski, Op. cit.

According to what has been widely argued in the literature,⁹² the inferential rule that animates the automated processes of Machine Learning systems would not (always) be knowable,⁹³ at least with respect to the reconstruction of the logic that is actually behind the processing of a specific output.⁹⁴

While this is not always the case⁹⁵ - and while awaiting promising new elaborations of technology⁹⁶ - this would nevertheless - as things stand - represent a limitation, of technological nature, capable of making, in these scenarios, the right to explanation 'useless'; and this is because it would be impossible for the data controller who relies on the use of self-learning "black box" systems to retrace (and thus share) the decision-making logic followed by the machine. Certainly, *ex ante*; in many cases *ex post*.⁹⁷

Given this, it is necessary to wonder how the assumption of the practical unfeasibility of the right to explanation reacts in the system of the GDPR. As correctly noted,⁹⁸ from this perspective, in the hypotheses in which the type of

⁹² See among others, Y Bathaee, Op. cit.; D Castelvechi, Op. cit.

⁹³ Among others, s., PJ Lisboa, *Interpretability in Machine Learning. Principles and Practice*, (Springer, 2013). On the difference between explainability and interpretability of decision-making models and the relationship between them, see J Zhong, E Negre, op. cit.; see also DA Broniatowski, *Psychological Foundations of Explainability and Interpretability in Artificial Intelligence*, NISTIR 8367, (2021). Online: <https://doi.org/10.6028/NIST.IR.8367>.

⁹⁴ It seems appropriate to note, however, how there is no shortage of different approaches in the literature to solving the mediated problem of the decision-making 'fairness' of automated systems, which, having abandoned the perspective of the necessary (reconstructability of an) 'explanation' of the machine's 'opaque' decision, provide, for the protection of individuals, for the implementation of systems suitable for detecting and preventing treatment the discriminatory within the automated decision-making process. See in this sense, C Dwork, M Hardt, et al., *Fairness Through Awareness*, ITCS 2012, (Cambridge, MA, USA, 2012). Also online at <https://arxiv.org/abs/1104.3913v2>.

⁹⁵ Explanatory tools make it possible in some cases, and only *ex post*, to analyze the reasoning steps of the system by reconstructing its essential decision-making moments so as to return, upon request, the decision logic concretely used by the algorithm in the analyzed case; see *supra*, note 18. Moreover, research has long been active in this area, with the goal of making ML algorithms increasingly amenable to *ex ante* and *ex post* control; see among others, A Datta, S Sen, Y Zick, *Algorithmic transparency via quantitative input influence*, in *37th IEEE Symposium on Security and Privacy*, (2016), online at: <https://ieeexplore.ieee.org/document/7546525>; S Galhotra, R Pradhan, B Salimi, *Explaining black-box algorithms using probabilistic contrastive counterfactuals*, 2021, online on arXiv:2103.11972v1; S Wachter, B Mittelstadt, C Russell, *Counterfactual explanations without opening the Black Box: automated decisions and the GDPR*, *Harvard Journal of Law & Technology*, (2018) Vol. 31, No. 2, 843-887; M Loi, A Ferrario, E Viganò, *Transparency as design publicity: explaining and justifying inscrutable algorithms*, [October 2020] Ethics and Information Technology, doi: <https://doi.org/10.1007/s10676-020-09564-w>; on the concept of Algorithmic accountability, and the possible role, as an external audit to the automated decision-making system, of reverse-engineering algorithms, see also N Diakopoulos, *Algorithmic Accountability Reporting: On the Investigation of Black Boxes*, [2014] Tow Center for Digital Journalism, Columbia University, online: <https://doi.org/10.7916/D8ZK5TW2>.

⁹⁶ The reference is to that strand of research that goes by the name of XAI, Explanatory Artificial Intelligence, aimed at defining methods and tools of "deep explanation," that is, capable of shedding light on the workings of algorithms with 'opaque' functioning, i.e., the construction of intelligent systems that are more transparent and interpretable; see HJ Watson, *The Need for Explainable Processes and Algorithms*, in *Business Intelligence Journal*, Vol. 25, No. 2, p. 5; AB Arrieta, N Díaz-Rodríguez, et al., *Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI*, (2020), online in ArXiv, [abs/1910.10045](https://arxiv.org/abs/1910.10045).

⁹⁷ Skeptical that technological solutions truly capable of ensuring high standards of transparency of decision-making processes animated by complex ML algorithms may be found, even in the future, and therefore critical of the possibility and desirability of affecting technological design through regulatory tools, is, for example, Y Bathaee, op. cit., p. 929; on the possibility of different approaches to that of *ex ante* or *ex post* (audit) transparency of the algorithm, see, among others, C Dwork, M Hardt, et al., op. cit.; on the advantages of a scalar case-by-case approach, see again Y Bathaee, op. cit., p. 889.

⁹⁸ R Messinetti, op. cit., p. 889.

explanation requested is assumed to be precluded, making it impossible to verify the lawfulness and fairness of the processing, the consequence produced on the logical level would not be the inapplicability of the rule - thus its uselessness - but the reinstatement of the prohibition - absolute, lacking the minimum conditions for its derogation⁹⁹ - of subjecting the data subject to automated decision-making processing under Article 22 (1) GDPR. Unless the data controller, therefore, can guarantee, including on a technological level, that the decision, having legal effects, based solely on automated processing of the data subject's personal data, is also explainable (i.e., its concrete decision-making logic can be traced), the data controller is obliged to refrain from implementing automated decision-making processing.

⁹⁹ That is, the suitable measures referred to in the Article 22(3) GDPR



Riflessioni sul diritto d'accesso agli atti tributari: la dialettica fra la tutela della *privacy* del contribuente ed il perseguimento dell'interesse fiscale dell'amministrazione finanziaria

Considerations on the right of access to tax documents: the relationship between the protection of taxpayer's privacy and the pursuit of the tax administration's fiscal interests

FEDERICO SERGIO

Ph.D. (c) at Università degli studi Suor Orsola Benincasa

Abstract

Il rapporto fra la riservatezza dei dati personali del contribuente e l'interesse erariale alla riscossione dei tributi ed alla lotta all'evasione fiscale si muove lungo il confine segnato dall'espansione del diritto d'accesso anche in ambito tributario. Il difficile contemperamento degli interessi in gioco richiede di adottare scelte mai aprioristiche e sempre illuminate dai principi regolatori dell'ordinamento giuridico interno e di quello sovranazionale.

The relationship between the taxpayer's privacy and the interest of the Treasury in the collection of taxes and the fight against tax evasion moves along the borderline marked by the expansion of the right of access also in tax law. The difficult balancing act between the interests at stake requires the adoption of choices which are never a priori and always enlightened by the regulatory principles of the domestic and supranational legal system.



Keywords: diritto d'accesso; diritto alla riservatezza dei dati; *privacy*; interesse fiscale; evasione fiscale

Summary: [1. Introduzione](#) - [2. I nuovi confini dell'accesso nell'attuale ordinamento giuridico interno](#) - [3. Il generale divieto di accesso agli atti tributari procedurali: contraddizioni normative](#) - [3.1. Segue: il riserbo "relativo" sull'attività istruttoria dell'amministrazione finanziaria. Primi passi in direzione di un'apertura verso l'accessibilità agli atti tributari nonostante le ancora numerose limitazioni "settoriali"](#) - [4. L'orientamento pretorio eurounitario a favore dell'ostensibilità dei documenti tributari in un'ottica di maggiore garanzia dei diritti del contribuente](#) - [5. Il pericolo di un'ipertutela del contribuente a discapito di un'ingiusta menomazione dell'interesse fiscale: il tema della lotta all'evasione nel rapporto con la riservatezza del contribuente affrontato dalla Corte europea dei diritti dell'uomo](#) - [6. Riflessioni conclusive](#)

1. Introduzione.

Il presente lavoro mira ad analizzare l'eterna, e mai sopita, dialettica fra contrapposti interessi tutelati sia a livello costituzionale che sovranazionale. Il riferimento è, da un lato, alla riservatezza dei dati personali e privati del contribuente e, dall'altro lato, all'interesse fiscale alla pronta riscossione dei tributi nonché alla lotta all'evasione fiscale.

Nell'ordinamento giuridico non vi è una scala di valori assiologicamente predefinita e perciò il relativo bilanciamento deve avvenire in base al caso concreto ed alla luce delle specifiche ed irripetibili contingenze che lo caratterizzano.

Una tale operazione deve essere sempre illuminata dai principi di proporzionalità e ragionevolezza e non deve essere mai il risultato di scelte aprioristiche avutesi tramite automatismi.

Nella disamina che verrà svolta nei seguenti paragrafi l'attenzione si focalizzerà, preliminarmente, sul perimetro del diritto d'accesso, in continua espansione nel sistema giusamministrativistico e, invece, caratterizzato ancora da significative preclusioni in ambito tributario.

La disamina ripercorrerà, poi, i più salienti orientamenti normativi e giurisprudenziali, in particolare di matrice eurounitaria, da cui si desume una sostanziale apertura verso un'accessibilità pressoché totale delle informazioni anche nel settore fiscale, nonostante talune contraddizioni normative che, in una prospettiva *de iure condendo*, sarebbe utile dirimere definitivamente.

La volontà di fornire un'accessibilità più ampia ai documenti tributari non può, in ogni caso, prevalere sull'interesse erariale. Allo stesso modo nemmeno la *privacy* del contribuente può farlo.

In ciò consiste la problematica del presente scritto il quale si propone di fornire, senza alcuna pretesa di esaustività, delle coordinate ermeneutiche per comprendere, apoditticamente, le ipotesi in cui un valore può prevalere sull'altro. Ciò tenendo presente che l'orientamento sovranazionale tende verso

un'accessibilità ampia anche nei confronti degli atti tributari endoprocedimentali il che, però, non deve sfociare in un'ipertutela del contribuente a discapito, giocoforza, dell'interesse erariale.

Il bilanciamento dei valori a confronto è un'operazione molto delicata. Sul punto verranno scrutinate argomentazioni interessanti della Corte di Giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo.

2. I nuovi confini dell'accesso nell'attuale ordinamento giuridico interno.

L'odierno sistema di diritto italiano tende oramai verso un'accessibilità pressoché totale delle informazioni e ciò, in particolare, alla luce dell'entrata in vigore dell'accesso civico generalizzato con il d.lgs. 97/2016 che, di fatto, introduce il c.d. FOIA¹ (*"Freedom of information act"*)².

Tale istituto non subordina l'ostensione di un atto al possesso di un interesse difensivo collegato ad esso³. Per la prima volta si contempla un vero e proprio diritto alla richiesta di accesso ad atti inerenti all'attività della pubblica amministrazione per qualunque fine e senza necessità di motivazioni⁴.

Si passa, quindi, dal "bisogno" di conoscere al "diritto" di conoscere (*from need to know to right to know*)⁵, così realizzando un regime del potere visibile di tipo "reattivo", cioè in risposta alle istanze di conoscenza avanzate dagli interessati⁶. Dunque, si assiste ad una "rivoluzione copernicana" che permette di evocare la celebre immagine, cara al noto statista Filippo Turati, della pubblica amministrazione trasparente come una "casa di vetro"⁷.

D'altronde, il principio di trasparenza, sotteso alla disciplina dell'ostensione degli atti, si colloca all'interno del processo di trasformazione della pubblica amministrazione caratterizzato dall'apertura all'esterno di quest'ultima⁸; in concreto, l'attività pubblica non è più autosufficiente, ma cede il passo alla gestione della fase istruttoria e di quella decisoria di concerto con i cittadini

¹ "Il *Freedom of Information Act*, diffuso in oltre 100 paesi al mondo, è una normativa che garantisce a chiunque il diritto di accesso alle informazioni detenute dalle pubbliche amministrazioni, salvo i limiti a tutela degli interessi pubblici e privati stabiliti dalla legge. In Italia tale diritto è previsto dal decreto legislativo n. 97 del 2016 che ha modificato il decreto legislativo n. 33 del 2013 (c.d. decreto trasparenza) con la finalità di promuovere una maggiore trasparenza nel rapporto tra le istituzioni e la società civile e incoraggiare un dibattito pubblico informato su temi di interesse collettivo.

² C. COLAPIETRO, *La terza generazione della trasparenza amministrativa*, Napoli, 2018, 113 ss.

³ M. MENDILLO, *La "funzionalizzazione" del principio di trasparenza. Il diritto di accesso agli atti ed ai documenti amministrativi come evoluzione funzionale del concetto di partecipazione: linee evolutive e profili applicativi nella disciplina interna e sovranazionale*, in *Riv. sem. dir.*, 2020, 1, 100; M. Savino, *La nuova disciplina della trasparenza amministrativa*, in *Giornale dir. amm.*, 2013, 9, 795.

⁴ S. BACCARINI, *Posizione giuridico-soggettiva dell'aspirante all'accesso amministrativo: natura giuridica ed implicazioni applicative*, in M. A. SANDULLI (a cura di), *Codice dell'azione amministrativa*, Milano, 2001, 215.

⁵ M.A. SANDULLI, *La trasparenza amministrativa nel FOIA italiano. Il principio della conoscibilità generalizzata e la sua difficile attuazione*, in www.federalismi.it, 2020.

⁶ C. TOMMASI, *Criteri di bilanciamento e discrezionalità amministrativa nell'accesso civico generalizzato, in Foia Italia: vincitori e vinti. Un bilancio a due anni dalla riforma*, a cura di G. GARDINI - M. MAGRI, Rimini, 2019, 73.

⁷ A. BOHUNNY, *Accesso ai documenti amministrativi nella legge n. 241/90 riformata*, in R. TOMEI, (a cura di), *La nuova disciplina dell'accesso ai documenti amministrativi. Commento alla legge n. 241 del 1990 ed al DPR 184/2006*, Padova, 2007, 89 ss.

⁸ B. CAROTTI, *La riforma della pubblica amministrazione - L'amministrazione digitale e la trasparenza amministrativa*, in *Giornale dir. amm.*, fasc. 5, 2015, 11 ss.

interessati⁹. L'esigenza di implementare la trasparenza nasce anche dalla necessità di controllare la spesa pubblica e ha carattere di moralizzazione della vita sociale, oltre ad essere uno strumento efficace di prevenzione e di lotta alla corruzione¹⁰.

La trasparenza è, quindi, considerata come la preconditione per ricostruire e rafforzare il rapporto di fiducia fra cittadini e poteri pubblici¹¹. Un valore-chiave, immanente nell'ordinamento, modo d'essere tendenziale dell'organizzazione dei pubblici poteri, parametro cui commisurare l'azione delle figure soggettive pubbliche, al fine di trovare il giusto punto di raccordo fra esigenze di garanzia e di efficienza nello svolgimento dell'azione pubblica¹². Tuttavia, nonostante l'indubbia *vis expansiva* dell'accessibilità delle informazioni in un'ottica di massima garanzia per il consociato, permane in maniera pervicace l'esigenza di tutelare interessi contrapposti all'ostensione¹³. In questi termini si sviluppa la dialettica intercorrente fra l'attenzione alla tutela della riservatezza dei dati personali di un individuo ed altri interessi pubblici che vengono in rilievo¹⁴.

Ciò pur sempre nell'ottica di non sconfinare in un'ipertutela del cittadino che si ponga a discapito dell'interesse pubblico di cui, nel caso di specie, l'amministrazione statale è portatrice¹⁵. Al riguardo si pensi alle regole dettate in combinato disposto dalla legge sul procedimento amministrativo (artt. 22 ss. l. 241/90) e dal codice privacy (artt. 59 e 60 "codice in materia di protezione dei dati personali" d.lgs. 196/2003) in tema di rapporto fra accesso e dati personali ordinari, sensibili (e giudiziari), sensibilissimi¹⁶. Il bisogno di ricercare un siffatto temperamento ha riguardato significativamente anche la tematica dell'accesso agli atti tributari, nell'ottica di bilanciare la riservatezza del contribuente con l'interesse fiscale dell'amministrazione finanziaria alla pronta acquisizione dei tributi e ad un efficiente svolgimento delle attività di accertamento volte a scongiurare gravi, e sempre più diffusi, fenomeni patologici: su tutti l'evasione fiscale¹⁷.

⁹ F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2015, 170 ss.

¹⁰ E. CARLONI, *Nuove prospettive della trasparenza amministrativa: dall'accesso ai documenti alla disponibilità delle informazioni*, in *Dir. pubbl.*, 2005, 43 ss.

¹¹ B. PONTI, *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013*, n. 33, Santarcangelo di Romagna, 2013, 55.

¹² A. SANDULLI, *Il procedimento*, in *Trattato di diritto amministrativo*, S. CASSESE (a cura di), Milano, 2000, 367 ss.

¹³ Sul punto ex multis: G. MANCOSU, *Trasparenza amministrativa e open data: un binomio in fase di rodaggio*, in *federalismi.it*, fasc. 17, 2012, 23; G. GARDINI, *Il Codice della trasparenza: un primo passo verso il diritto dell'informazione amministrativa?*, in *Giornale dir. amm.*, 2014, 98; F. DI DONATO, *Lo stato trasparente. Linked open data e cittadinanza attiva*, Pisa, 2011, 67; B. COCCAGNA, *Open data, trasparenza elettronica e codice aperto*, in *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Milano, 2012, 31.

¹⁴ A. CORRADO, *Conoscere per partecipare: la strada tracciata dalla trasparenza amministrativa*, Napoli, 2018, 17.

¹⁵ D. LATHROP, *Open government: collaboration, transparency in practice*, O'Reilly Media, Sebastopol, 2010; C. LEONE, *Il ruolo del diritto europeo nella costruzione dell'amministrazione digitale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2011, 145.

¹⁶ V. PARISIO, *La tutela dei diritti di accesso ai documenti amministrativi ed alle informazioni nella prospettiva giurisdizionale*, in *www.federalismi.it*, 2018, 12; F. PATRONI-GRIFFI, *La trasparenza della pubblica amministrazione fra accessibilità totale e riservatezza*, in *www.federalismi.it*, 2013, 27.

¹⁷ M. LIPARI, *Il diritto di accesso e la sua frammentazione dalla legge n. 241/1990 all'accesso civico: il problema delle esclusioni e delle limitazioni oggettive*, in *www.federalismi.it*, 2019, 17: «l'art. 24, comma 1, è una disposizione normativa che dovrebbe diventare non una mera vuota retorica, ma effettiva

3. Il generale divieto di accesso agli atti tributari procedimentali: contraddizioni normative.

Nell'attuale quadro normativo che regola il diritto di accesso rispetto agli atti in possesso dall'amministrazione finanziaria viene in rilievo l'art. 24 l. co. lett. b) l. 241/90 che, derogando al generale principio di accessibilità ai documenti amministrativi, prevede l'esclusione di detto diritto nei procedimenti tributari, per i quali restano ferme le particolari norme che lo regolano¹⁸. La "ratio" di tale limitazione risiede nel peculiare obiettivo perseguito tramite la fase istruttoria consistente nell'interesse fiscale all'accertamento di eventuali irregolarità tributarie, funzionale alla corretta acquisizione dei tributi da parte del Fisco, pur sempre nel rispetto dei diritti individuali dei contribuenti¹⁹.

Tuttavia, una preclusione normativa così rigida parrebbe porsi in contrasto con quanto contemplato dall'art. 6 dello Statuto dei diritti del contribuente (l. 212/2000) secondo cui l'amministrazione finanziaria deve assicurare al contribuente l'effettiva conoscenza degli atti a lui destinati.

Il legislatore, però, non specifica il grado né della trasparenza che l'autorità tributaria dovrebbe garantire al contribuente né della segretezza che essa potrebbe opporre al richiedente, né, tantomeno, la fase procedimentale in cui la suddetta "effettiva" conoscenza del contribuente debba essere assicurata, la quale anzi parrebbe essere esclusa a priori dalla legge sul procedimento amministrativo²⁰.

Altra fonte rilevante in materia di accesso tributario è rappresentata dal d.m. 603/1996, il quale indica le categorie di documenti tributari sottratte all'accesso. Nel dettaglio, gli articoli 2, 3 e 5 prevedono l'inaccessibilità a tutti i documenti relativi alle attività ispettive, di controllo e di indagine fiscale poiché la loro diffusione potrebbe compromettere le scelte di politica tributaria, monetaria e valutaria dello Stato, nonché la quantificazione del gettito fiscale desumibile dall'attività di accertamento. L'art. 5, in particolare, vieta l'accesso a determinate categorie di documenti fiscali per ragioni di *privacy* e sicurezza²¹.

Al fine di sopperire al *vulnus* del mancato rispetto del principio di conoscenza affermato dallo Statuto, deve registrarsi il vano tentativo legislativo di introdurre in via generale un, seppur limitato, principio di accessibilità ai documenti tributari²².

affermazione di regola operativa secondo lo schema del rapporto logico tra regola ed eccezione: la regola è la trasparenza, mentre l'eccezione è costituita dalla sottrazione all'accesso ... Le esclusioni dovrebbero essere positivamente individuate e, al di fuori di tali confini, l'accesso dovrebbe essere sempre consentito»; G. Dellabertola, *Diritto di accesso agli atti del procedimento tributario (quasi) senza limiti*, in *Corr. trib.*, 2018, 6, p. 459.

¹⁸ L. FERRAJOLI, *La tutela del contribuente nelle procedure di accertamento tributario: linee evolutive*, in *il fisco*, 2004, 3815.; G. FRANSONI, *Le indagini tributarie*, Torino, 2020, 367.

¹⁹ M. BASILAVECCHIA, M. Di Siena, R. Lupi, *I principi generali del diritto amministrativo "salvano" l'accesso agli atti tributari*, in *Dial. trib.*, 2009, 1, 43.

²⁰ M. PIERRO, *Il dovere di informazione dell'Amministrazione finanziaria*, Torino, 2013, 71.

²¹ G. MAINOLFI, *Indagini bancarie e tutela della privacy: l'allegazione dell'autorizzazione alla richiesta di acquisizione di copia dei conti*, ex art. 18 della l. n. 413/1991, in *il fisco*, 2003, 5137.

²² R. MICELI, *La partecipazione del contribuente alla fase istruttoria*, in AA. VV., *Statuto dei diritti del contribuente*, Milano, 2005, 673.

L'art. 9 l co. lett. b) della legge di delega fiscale dell'11 marzo 2014 n. 23 aveva fissato, a favore del Governo delegato, il principio secondo il quale occorre prevedere l'obbligo di garantire l'assoluta riservatezza nell'attività conoscitiva e di controllo fino alla completa definizione dell'accertamento.

Sicché, oltre la fase istruttoria del procedimento, l'amministrazione non avrebbe potuto mantenere alcuni riserbo sui dati, notizie ed informazioni concernenti il contribuente nei confronti del quale si è in procinto di emettere l'atto impositivo, ossia quell'atto con cui l'amministrazione finanziaria, a conclusione dell'iter procedimentale, esercita la potestà simpositiva diretta ad assicurare l'interesse dell'Erario²³. Ebbene, la delega è rimasta inattuata, ma dal principio del legislatore delegante emerge la centralità dell'obiettivo della trasparenza quale cardine intorno al quale far ruotare una "correttezza procedimentale" del Fisco verificabile dall'interlocutore in via anticipata²⁴.

Difatti, è tramite la conoscenza preventiva dei documenti che il contribuente può controllare e valutare la legittimità dell'esercizio del potere pubblico, prima che l'emissione di un provvedimento illegittimo determini al privato un pregiudizio ingiustificato: si otterrebbe così una tutela immediata anziché differita²⁵.

Inoltre, la trasparenza permetterebbe di attuare il più ampio principio del "giusto" procedimento il quale, ancorché non espressamente previsto a livello normativo, sta trovando significativo riconoscimento nella giurisprudenza eurounitaria.

Esso è volto ad assicurare la collaborazione fra amministrazione statale e privato garantendo la partecipazione di quest'ultimo al procedimento preordinato all'adozione dell'atto finale, permettendo di rendere verificabile e controllabile dall'esterno l'operato dell'amministrazione nell'ottica di due altri principi cardini del diritto tributario: quello di pubblicità degli atti ex art. 97 Cost., nonché quello di matrice eurounitaria del contraddittorio endoprocedimentale²⁶ che impone all'amministrazione, prima dell'emissione di un provvedimento sfavorevole, di ascoltare l'interessato²⁷.

²³ F. GALLO, *Contraddittorio procedimentale e attività istruttoria*, in *La concentrazione della riscossione dell'accertamento*, Milano, 1997, 374.

²⁴ A. GUIDARA, *Accordi e azione amministrativa nel diritto tributario*, Pisa, 2020, 287.

²⁵ M. MANCA, *Partecipazione del cittadino-contribuente al procedimento amministrativo tributario*, in *il fisco*, 2003, 186.

²⁶ Cfr. Corte di giustizia, 18 dicembre 2008, causa C-349/07, *Sopropé*; *Id.* 3 luglio 2014, cause riunite C-129/13 e C-130/13, *Kamino International Logistics e Datema Hellmann Worldwide Logistics*. Per ulteriori approfondimenti in tema di accesso agli atti endoprocedimentali cfr. P. Provenzano, *Il procedimento amministrativo e il diritto ad una buona amministrazione*, in D.U. Galletta, *Diritto amministrativo nell'Unione europea*, Torino 2020, 119; G. della Cananea, C. Franchini, *I principi dell'amministrazione europea*, Torino 2020, 111 ss.

²⁷ In tal senso, con specifico riferimento alla materia tributaria, si può vedere, tra i più recenti contributi, M. PIERRO, *"Il dovere di informazione dell'Amministrazione finanziaria e il diritto al contraddittorio preventivo"*, in *Riv. dir. fin. sc. fin.*, 2016, I, pag. 218 ss.; in precedenza, può tra gli altri vedersi: L. DEL FEDERICO, *"I rapporti tra lo Statuto e la legge generale sull'azione amministrativa"*, in *Rass. trib.*, 2011, par. 2. In senso contrario, può invece richiamarsi R. SCHIAVOLIN, *"La portata, rispetto all'ordinamento tributario italiano, dei 'diritti fondamentali' di cui all'art. 41 della Carta UE"*, in *NEQTEPA*, n. 2/2018, pag. 27, pag. 7 ss., secondo il quale "... da un lato, la collocazione di questo rinvio sotto la rubrica 'principi generali e l'affiancamento di esso ai criteri di efficacia, economicità, imparzialità, ecc., distinti dalle 'modalità' dell'azione amministrativa previste dalla stessa Legge n. 241/1990 e da singole normative, mi sembra escludano la volontà del legislatore italiano di attribuire a detti principi la forza necessaria a sostituirsi a discipline speciali, come quelle dei procedimenti tributari. Dall'altro lato, come riconosciuto dall'attuale giurisprudenza di legittimità,

Sul punto, occorre rilevare che attualmente trova significativo riscontro quell'orientamento che desume il contraddittorio "pregiurisdizionale" tributario nell'art. 12 dello Statuto²⁸. Infine, giova rammentare che il summenzionato principio del "giusto" procedimento si evince dall'art. 41 della Carta dei diritti fondamentali dell'Unione europea che prevede il diritto di ogni individuo di essere ascoltato prima che nei suoi confronti venga adottato un provvedimento individuale che gli rechi pregiudizio²⁹.

l'art. 13, comma 2, Legge n. 241/1990 esclude i procedimenti tributari dagli istituti partecipativi previsti dal capo III di detta legge, aggiungendo che per essi 'restano parimenti ferme le particolari norme che li regolano', e manifestando così la volontà di lasciare le scelte in materia alla normativa speciale. Tale regola è chiaramente incompatibile con un generale riconoscimento di un diritto al contraddittorio attraverso il rinvio all'art. 41 Carta UE, operante anche in materia di procedimenti tributari (pagg. 10-11). Della prima Autrice, anche in risposta alle obiezioni di Schiavolin, si veda altresì M.C. PIERRO, "La collaborazione e la partecipazione 'informata del contribuente nei procedimenti tributari e il diritto ad una buona amministrazione", in *Innovazione e diritto*, n. 4/2018, par. 3.

²⁸ F. FARRI., *Per il contraddittorio endoprocedimentale tributario occorre un nuovo art. 12-bis nello statuto del contribuente, non l'art. 5-ter del d.lgs. 218/1997*, in *Riv. dir. trib.*, 2020, È ben noto, inoltre, il contrasto delle Sezioni Unite in tema di contraddittorio: cfr. Cass. sez. un. sent. 29 luglio 2013 n. 18184 e 18 settembre 2014, n. 19667 e la successiva sentenza della Cass. sez. un. 9 dicembre 2015, n. 24823 che ha completamente modificato i precedenti orientamenti escludendo il contraddittorio preventivo per i tributi non armonizzati. Sul tema più ampiamente tra i numerosi autori v. G. RAGUCCI, *Il contraddittorio nei procedimenti tributari*, Torino 2009; A. MARCHESELLI, *Il "giusto procedimento" tributario. Principi e discipline*, Milano, 2012; F. TUNDO, *Procedimento tributario e difesa del contribuente*, San Giuliano Milanese, 2013; P. ACCORDINO, *Problematiche applicative del "contraddittorio" nei procedimenti tributari*, Milano, 2018. cfr. L. NICOTINA, *Il contraddittorio tributario in funzione deflativa: una premessa/promessa che non può essere tradita*, in *Riv. trim. dir. trib.*, 2014, 415; Cfr. A. RENDA, *Il contraddittorio quale nucleo insopprimibile di rilievo sostanziale nell'ambito del procedimento tributario: le conferme della giurisprudenza comunitaria e di legittimità*, in *Dir. prat. trib.*, 2015, II, 593 e dello stesso autore, *Il contraddittorio preventivo tra speranze (deluse), rassegnazione e prospettive*, in *Dir. prat. trib.*, 2016, II, 732; R. IAIA, *Il contraddittorio anteriore al provvedimento amministrativo tributario nell'ordinamento dell'Unione Europea. Riflessi nel diritto nazionale*, in *Dir. prat. trib.* 2016, II, 105; A. LOVISOLO, *Sulla c.d. 'utilità' del previo contraddittorio preventivo procedimentale*, in *Dir. prat. trib.*, 2016, II, 720; G. CORASANITI, *Il principio del contraddittorio nella giurisprudenza nazionale e dell'Unione Europea*, in *Dir. prat. trib.*, 2016, IV, 1575; C. BUCCICO, *Il contraddittorio endoprocedimentale nella giurisprudenza europea*, in *Inn. dir.*, 2016, 5, 65-90; A. COMELLI, *I diritti della difesa, in materia tributaria, alla stregua del diritto dell'unione europea e, segnatamente, il "droit d'être entendu" e il diritto ad un processo equo*, in *Dir. prat. trib.*, 2020, IV, 1315.

²⁹ In generale, sull'art. 41 della Carta, possono tra gli altri vedersi in dottrina: M. Richardson, "The EU and ECHR Rights of the Defence Principles in Matters of Taxation, Punitive Tax Surcharges and Prosecution of Tax Offences", in *EC Tax Law Review*, 2017/6, pag. 323 ss.; P. Piva, "Commento all'art. 41 Carta dei diritti fondamentali dell'Unione Europea", in R. Mastroianni et al. (a cura di), Milano, 2017, pag. 753 ss.; P. Leino, "Efficiency, Citizens and Administrative Culture. The Politics of Good Administration in the EU", in *European Public Law*, 20, n. 4/2014, pag. 681 ss.; P. Craig, "Commento all'art. 41 The EU Charter of Fundamental Rights", in S. Peers et al. (a cura di), Oxford and Portland, Oregon, Hart Publishing, 2014, pag. 1069 ss.; J. Mendes, "Good Administration in EU Law and the European Code of Good Administration Behaviour", in *EUI Working Paper Law*, n. 9/2009, European University Institute, S. Domenico di Fiesole (FI), 2009; D.U. Galetta, "Il diritto ad una buona amministrazione europea come fonte di essenziali garanzie procedurali nei confronti della Pubblica amministrazione", in *Riv. it. dir. pubbl. comunit.*, 2005, pag. 819 ss.; K. Kaňska, "Towards Administrative Human Rights in the EU. Impact of the Charter of Fundamental Rights", in *European Law Journal*, vol. 10, n. 3/2004, pag. 296 ss. Propongono una lettura svalutativa dell'art. 41 della Carta: R. Boust, "Who Said There Is a 'Right to Good Administration'? A Critical Analysis of Article 41 of Charter of Fundamental Rights of the European Union", in *European Public Law*, 19, n. 3/2013, pag. 481 ss.; J. Dutheil de la Rochère, "The EU Charter of Fundamental Rights, Not Binding but Influential: the Example of Good Administration", in A. Arnall et al. (a cura di) *Continuity and Change in EU Law: Essays in Honour of Sir Francis Jacobs*, Oxford University Press, 2008, spec. pag. 168 ss. Un esame circa l'attuazione del diritto alla buona amministrazione nel Regno Unito si trova in P. Birkinshaw, "The Right to Good Administration in the United Kingdom", in *federalismi.it*, n. 2/2008.

3.1. Segue: il riserbo “relativo” sull’attività istruttoria dell’amministrazione finanziaria. Primi passi in direzione di un’apertura verso l’accessibilità agli atti tributari nonostante le ancora numerose limitazioni “settoriali”.

Nel sistema tributario le considerazioni formulate, in termini di tendenziale apertura³⁰, nel procedimento amministrativo devono essere temperate con l’interesse pubblico erariale perseguito dall’attività impositiva e con l’esigenza dell’amministrazione finanziaria di mantenere la segretezza fino alla formazione ed alla notifica del provvedimento impositivo³¹.

Il Consiglio di Stato, in merito, ritiene che il diniego di accesso ai documenti tributari abbia come obiettivo quello di mantenere la riservatezza nella fase dei controlli fiscali condotti dall’amministrazione finanziaria finché l’azione di accertamento non sia stata conclusa mediante la notifica dell’atto finale del contribuente³².

Al riguardo, si è sostenuto che l’inaccessibilità agli atti del procedimento tributario non sia assoluta ma relativa, posto che essa è temporalmente limitata alla fase di pendenza dello stesso³³. Ne consegue che, una volta conclusa la fase procedimentale ed adottato il provvedimento finale mediante il quale si estrinseca il potere impositivo del Fisco, verrebbe meno la causa di inaccessibilità, ossia l’esigenza di segretezza, con immediata riespansione del diritto del contribuente alla conoscenza, in via prodromica all’esercizio del diritto di difesa ex art. 24 Cost³⁴.

Da ultimo, si consideri la recentissima pronuncia dell’Adunanza Plenaria del Consiglio di Stato che ha riconosciuto pacificamente l’accesso alla cartella di pagamento, in quanto atto impositivo che si colloca in una fase successiva rispetto a quella del procedimento, ossia l’esecuzione esattoriale mediante ruolo, strumento di riscossione coattiva³⁵.

³⁰ L. SALVINI, *Accesso agli atti del procedimento tributario*, in S. Cassese (a cura di), *Dizionario di diritto pubblico*, Milano, 2006: «tanto più si ritiene pregnante l’obbligo dell’amministrazione di motivare l’atto impositivo e di indicare espressamente nella motivazione anche gli atti formati, raccolti o comunque acquisiti nel corso del procedimento e di cui l’amministrazione stessa intende valersi a fini probatori, tanto più l’art. 7 dello Statuto del contribuente tutela l’effettiva e diretta conoscenza da parte del contribuente di questi ultimi atti».

³¹ M. PIERRO, *Il diritto ad una buona amministrazione nei procedimenti tributari*, Milano, 2019, 117.

³² Cons. Stato, sez. IV, 6 agosto 2014, n. 4209 in www.giustizia-amministrativa.it.

³³ M. BASILAVECCHIA, *Contraddittorio preventivo e accesso al fascicolo*, in *Corr. trib.*, 2020, 74.

³⁴ Corte di Giustizia UE, causa C-46/16, EU:C:2017:839, punti 39-40. Può essere utile, ai fini dell’esatta comprensione delle affermazioni della Corte, riportare quanto in proposito sostenuto l’Avvocato Generale J. Kokott nelle conclusioni presentate nella causa in questione il 30 marzo 2017, EU:C:2017:247, punto 77: “A carico delle autorità nazionali grava..., in sede di applicazione del diritto dell’Unione, un obbligo generale di motivazione. È vero che l’art. 41 della Carta dei diritti fondamentali non trova immediata applicazione nel caso dell’attuazione del diritto dell’Unione da parte degli Stati membri... Il diritto ad una buona amministrazione ivi garantito rispecchia tuttavia un principio generale del diritto dell’Unione con la conseguenza che uno Stato membro è tenuto a osservare i requisiti da esso derivanti in sede di attuazione del diritto dell’Unione...”. Nel senso della sentenza *LS Customs Services*, si può altresì vedere: Corte di Giustizia UE, 17 luglio 2014, cause riunite C-141/12 e C-372/12, YS, EU:C:2014:2081, punti 67-68. La sentenza *LS Customs Services* afferma inoltre, ai punti 51-52, che l’imparzialità costituisce un corollario del principio generale della buona amministrazione.

³⁵ Ad. Plen. Cons. Stato, 14 marzo 2022, n. 4 in www.giustizia-amministrativa.it.

In sintesi, assicurare la conoscenza documentale solo dopo che l'attività istruttoria sia esaurita consente all'AF di preservare l'interesse fiscale e di evitare che il contribuente possa interferire con l'attività di indagine³⁶.

Tuttavia, pur in presenza di consolidati principi, ancora oggi il dibattito non pare sopito ed il diritto alla conoscenza in alcuni casi sembra ancora ingiustificatamente sacrificato³⁷. Si pensi ai casi in cui la segretezza dell'agire fiscale non sia funzionale ad evitare possibili alterazioni probatorie da parte del contribuente, come può accadere in presenza di documenti pervenuti all'amministrazione finanziaria e non modificabili dal privato³⁸. In ipotesi siffatte, non si comprende perfettamente perché l'istanza di accesso debba essere intesa come idonea ad ostacolare o alterare l'attività impositiva. Non è comprensibile la logica sottesa al rigetto opposto dall'autorità tributaria alla richiesta di ostensione presentata dal contribuente, quando invece è la prima a chiedere al secondo di fornire informazioni necessarie ai fini dell'accertamento, che altrimenti sarebbe più difficoltoso se non impossibile reperire³⁹.

Ulteriore tipologia di limitazione al diritto di accesso agli atti tributari (però di tipo permanente e non, come quelle testè menzionate, semplicemente differito fino alla conclusione del procedimento finale di accertamento) afferisce alle indagini sorte per effetto dello scambio di informazioni fra amministrazioni finanziarie di diversi Stati.

Trattasi delle note vicende internazionali di furto di informazioni bancarie da parte di ex dipendenti degli istituti di credito, spesso situati in paradisi fiscali. Fra tutte vedasi la "lista Falciani"⁴⁰, la "lista Pessina" e la "lista Vaduz"⁴¹.

Il Consiglio di Stato⁴² in più pronunce ha definitivamente chiarito che i documenti tributari, detenuti dall'amministrazione finanziaria nazionale, a seguito di uno scambio di informazioni avvenuto con autorità fiscali di altri Paesi, non

³⁶ G. RAGUCCI, *Gli istituti della collaborazione fiscale. dai comandi e controlli alla self-regulation*, Torino, 2019, 67.

³⁷ A. MARCHESELLI, *Contraddittorio e procedimento tributario, un passo indietro e due avanti*, in *Corr. trib.*, 2011, 55.

³⁸ A. R. CIARCIA, *L'accesso agli atti dell'Amministrazione Finanziaria (tra aperture europee e limiti della normativa amministrativa interna)*, in *Riv. dir. trib.*, 2021, 24.

³⁹ D. U. GALETTA, *Il diritto ad una buona amministrazione nei procedimenti amministrativi oggi (anche alla luce delle discussioni sull'ambito di applicazione dell'art. 41 della Carta dei diritti UE)*, in M. C. PIERRO (a cura di), *Il diritto a una buona amministrazione nei procedimenti tributari*, Milano, 2019, 79.

⁴⁰ Corte di Giustizia UE, sentenza del 24 febbraio 2022, causa C-175/2020, *Valsts ierņēmumu dienests (Traitement des données personnelles à des fins fiscales)*, ECLI:EU:C:2022:124. In particolare, per ciò che è di specifico interesse in questa sede tale pronuncia la Corte di Giustizia ha chiarito la soggezione delle amministrazioni tributarie nazionali dei paesi membri ai dettami del GDPR, precisando, altresì, come le stesse risultino vincolate al rispetto dei principi stabiliti in dall'art. 5 in tema di liceità del trattamento.

⁴¹ Si veda, a tale riguardo, A. MARCHESELLI, *"Lista Falciani": le prove illecite sono utilizzabili nell'accertamento tributario?*, in *Corr. trib.*, 2011, 3910 ss.; F. D'AYALA VALVA, *Acquisizione di prove illecite. Un caso pratico: la "lista Falciani"*, in *Riv. dir. trib.*, 2011, II, 402 ss.; A. VIGNOLI, R. LUPI, *Sono utilizzabili le informazioni bancarie illecitamente sottratte da impiegati di istituti di credito esteri?*, in *Dialoghi trib.*, 2011, 268 ss.; R. SCALIA, *Note sulle liste di correntisti "provenienti" dall'estero e sul loro impiego nell'accertamento tributario*, in *Riv. dir. trib.*, 2013, II, 185 ss. e, se si vuole, A. MARINELLO, *Prove illecitamente acquisite all'estero e tutela del contribuente: disorientamenti giurisprudenziali*, in *Riv. trim. dir. trib.*, 2015, 485 ss.

⁴² Cons. St. 26 settembre 2013, n. 4821; Cons. St. 21 ottobre 2008, 5144; Cons. St. 14 maggio 2014, n.2472; Cons. St. 25 settembre 2020, n. 19; Cons. St., Sez. IV, 6 novembre 2017, n. 5128; Cons. St., Sez. IV, 9 febbraio 2016, n. 527; Cons. St., Sez. V, 23 marzo 2015, n. 1545; Cons. St., Sez. IV, 29 gennaio 2014, n. 461; Cons. St., Sez. V, 10 gennaio 2007, n. 55. Cons. St., Sez. IV, 6 febbraio 2019, n. 908; Cons. St., Sez. IV, 28 gennaio 2016, n. 317; Cons. St., Sez. VI, 15 febbraio 2012, n. 766.

possono formare oggetto di esibizione, anche quando l'atto di accertamento è stato notificato al contribuente-richiedente, perché ciò pregiudicherebbe le relazioni internazionali intrattenute dallo Stato con detti Paesi.

Per ciò, in ipotesi di richieste di accesso a documenti di indagine fiscale aventi il carattere della transnazionalità, il principio di trasparenza cede il passo al segreto, così da salvaguardare gli interessi pubblici dall'oggettiva messa in pericolo della sicurezza, della difesa nazionale e della tutela delle relazioni internazionali⁴³.

Infine, merita un cenno anche l'inapplicabilità del diritto di accesso agli atti delle istituzioni europee, quali il Parlamento europeo, il Consiglio e la Commissione. L'art. 15 TFUE prevede, infatti, che gli organi politici e quelli amministrativi dell'Unione devono operare nel modo più trasparente possibile, garantendo ai cittadini degli Stati membri il diritto di accesso ai documenti delle istituzioni, diritti i cui limiti devono essere stabiliti mediante regolamenti del Parlamento e del Consiglio europeo.

Secondo l'art. 42 della Carta dei diritti fondamentali dell'Unione europea, l'istanza d'accesso da parte del privato non deve essere subordinata alla prova di un interesse concreto ed attuale, in quanto la richiesta non è sempre preordinata alla tutela di una propria posizione giuridica soggettiva, ma risponde al principio generale di trasparenza, quale strumento di controllo democratico dell'operato delle istituzioni europee.

Nel sistema tributario, il limite del diritto d'accesso, così inteso, verte sostanzialmente sui documenti di indagine fiscale svolte dagli organismi europei, funzionali a contrastare l'evasione di risorse dell'Unione europea.

4. L'orientamento pretorio eurounitario a favore dell'ostensibilità dei documenti tributari in un'ottica di maggiore garanzia dei diritti del contribuente.

L'indirizzo affermatosi in seno alla Corte di Giustizia dell'Unione europea è completamente opposto a quello della giurisprudenza amministrativa nazionale⁴⁴.

Difatti, il giudice europeo ha di recente sostenuto il principio secondo cui il diritto di accesso da parte dei contribuenti, anche se esercitato antecedentemente all'emissione di un provvedimento impositivo, deve essere generalmente consentito, potendo essere negato solo al ricorrere di obiettivi di interesse generale da contrapporre agli interessi dei soggetti richiedenti⁴⁵.

Nella pronuncia si evince che per esercitare efficacemente il diritto di difesa, è fondamentale per il contribuente conoscere tutti gli elementi che fondano la contestazione che l'amministrazione finanziaria è in procinto di avanzare già nel

⁴³ M. LOGOZZO, *Il diritto ad una buona amministrazione e l'accesso agli atti nel procedimento tributario*, in M. PIERRO (a cura di), *Il diritto ad una buona amministrazione nei procedimenti tributari*, Milano, 2020, 77.

⁴⁴ Corte di Giustizia UE, 9 novembre 2017, C-298-16, *Teodor Ispas e Anduta Ispas/Directia Generala a Finantelor Publice Cluj*, in www.curia.europa.eu.

⁴⁵ G. MERONE, *Diritto al contraddittorio preventivo e frodi iva: illegittimi i recuperi effettuati in assenza di partecipazione del contribuente ai procedimenti "connessi"*, in *Dir. e prat. trib. intern.*, 2020, 2.

corso del procedimento istruttorio. Così operando, sarebbe possibile fornire spiegazioni o far valere motivi rispetto al punto di vista dell'AF⁴⁶.

Dunque, la giurisprudenza unionale, a differenza di quella amministrativa nazionale, ammette in via generale nel procedimento tributario il diritto di accesso e ciò a prescindere dal fatto che vengano in considerazione tributi armonizzati.

Tale diritto è ammesso anche nella fase istruttoria, con l'unico limite rappresentato dall'esigenza di bilanciamento con i predetti obiettivi di interesse generale⁴⁷. La Corte riconosce che fra questi ultimi possono essere ricompresi il diritto alla riservatezza delle persone fisiche, il segreto professionale, nonché le fattispecie in cui la conoscenza dei documenti potrebbe nuocere all'effettiva attività investigativa dell'amministrazione e, quindi, all'interesse erariale.

Com'è noto, in virtù del sistema di gerarchia delle fonti, il diritto eurounitario, così come interpretato dalla Corte di Giustizia, prevale su quello interno contrastante ex art. 117 I co. Cost., con la conseguenza che i postulati giurisprudenziali di derivazione europea potrebbero rimettere in discussione l'orientamento giurisprudenziale interno.

Ciò anche considerando l'art. 1 I co. l. 241/90 secondo cui l'attività amministrativa nazionale è retta e deve essere esercitata secondo le modalità previste dai principi dell'ordinamento comunitario, a testimonianza dell'intenso legame fra l'azione amministrativa interna ed il diritto europeo, di fonte sia normativa che pretoria.

D'altronde, si consideri che le sentenze della Corte sono annoverabili fra le fonti del diritto unionale intermedio (o complementare) le quali, secondo l'opinione prevalente, posseggono la medesima diretta applicabilità propria dei Trattati e delle altre fonti di diritto primario. Ne deriva che le stesse sono da considerarsi direttamente applicabili negli ordinamenti giuridici degli Stati membri, incontrando come unico limite la contrarietà con i principi supremi dell'ordinamento costituzionale in ordine alla c.d. "teoria dei controlimiti" elaborata dalla Corte Costituzionale.

In definitiva, si deve rilevare che in ambito tributario il diritto di accesso incontra i medesimi limiti che vigono nel procedimento amministrativo e che dovranno essere declinati avendo riguardo alle particolarità ed alle fasi in cui è scandita l'attività impositiva⁴⁸.

Specificamente, con riguardo all'accesso difensivo, viene in considerazione il limite della riservatezza delle persone fisiche⁴⁹.

Difatti, l'esigenza difensiva dell'interessato deve essere bilanciata con la tipologia di dati personali altrui contenuti nella documentazione di cui si richiede l'ostensione.

⁴⁶ Sul punto, v. G. VANZ, *I poteri conoscitivi e di controllo dell'Amministrazione finanziaria*, Padova, 2012, 42 ss.; A. VIOTTO, *Recenti modifiche normative in tema di accertamenti bancari: tra tutela del diritto alla riservatezza ed interesse generale alla repressione dell'evasione*, in Riv. trim. dir. trib., 2017, 822 ss.

⁴⁷ M. P. NASTRI, *Lo scambio di informazioni in materia fiscale: la tutela giurisdizionale effettiva e il diritto alla protezione dei dati*, in Dir. e prat. trib. intern., 2020, 4.

⁴⁸ L. STRIANESE, *Rapporto giuridico d'imposta e contraddittorio endoprocedimentale: un ragionamento permanente sull'illusoria parità delle armi tra Amministrazione Finanziaria e contribuente*, in C. BUCCICO, S. FIORENTINO, A. MERONE, (a cura di), *Civiltà fiscale. Riflessioni sul progetto "ideale" di Statuto dei diritti del Contribuente*, Milano, 2020, 76.

⁴⁹ A. M. TROPEA, *Il limite al diritto di accesso agli atti aventi natura tributaria*, in Riv. trim. dir. trib., 2017, 1, 12.

Dalla lettura della summenzionata sentenza della Corte⁵⁰, emerge la volontà di fornire al contribuente maggiori garanzie in termini di tutela dei propri diritti, tramite il pieno coinvolgimento dello stesso già nella fase procedimentale, storicamente preclusogli dalla legislazione nazionale come fin qui esaminato.

La partecipazione “pregiurisdizionale” del contribuente rispecchierebbe quei diritti già espressamente previsti nella fase giurisdizionale dagli artt. 6 CEDU, 111 Cost. : il diritto di difesa, il diritto alla parità delle armi, il diritto di essere ascoltati⁵¹, il diritto ad un equo processo⁵².

D'altronde, è difficile immaginare un “giusto” processo senza un “giusto” procedimento che lo preceda.

5. Il pericolo di un'ipertutela del contribuente a discapito di un'ingiusta menomazione dell'interesse fiscale: il tema della lotta all'evasione nel rapporto con la riservatezza del contribuente affrontato dalla Corte europea dei diritti dell'uomo.

Dall'analisi fin qui svolta emerge, dunque, una tendenziale apertura verso un'accessibilità anche agli atti tributari procedimentali nonostante le rigide preclusioni imposte dal legislatore. E ciò in ragione di un antropocentrismo garantista, il quale permea specialmente gli indirizzi giurisprudenziali eurounitari che attribuiscono massimo valore alla tutela dei diritti della persona. Tale aspetto costituisce elemento centrale e caratterizzante del *rule of law*.

In ambito tributario la portata valoriale dello Stato di diritto dovrebbe ammantare tanto la fase processuale quanto quella procedimentale, stante i valori speculari che in essi emergono (ed a cui già si è accennato): uguaglianza delle parti, certezza del diritto, prevedibilità, legittimo affidamento, *ne bis in idem*, difesa, diritto di essere ascoltati, diritto ad una buona amministrazione e, per l'appunto, diritto d'accesso.

Tali principi non concernono tanto, o comunque solo specificamente, il diritto tributario ma rappresentano l'essenza di ogni Stato democratico.

⁵⁰ Cfr. nota n. 35.

⁵¹ Cfr. F. PACELLI, P. PALAZZI, DAC 6: *ennesimo obbligo di trasparenza o nuova spinta alla compliance preventiva?*, in *Corr. trib.*, 2020, 9, 719 A. VOZZA, *La difesa nelle indagini innescate dallo scambio di informazioni previsto dalla dac 6*, in *Corr. trib.* 2021, 3, 261. Nella giurisprudenza della CGUE, sebbene sia stato riconosciuto il diritto del detentore delle informazioni di contestare la legittimità della richiesta, non vi è stato alcun riconoscimento di *participation rights* a favore dei contribuenti oggetto delle indagini; la Corte, infatti non si è espressa in merito al diritto di conoscere l'avvenuta richiesta di informazioni (*notification rights*), né sul diritto di essere ascoltato prima della trasmissione delle informazioni (*consultation rights*), dichiarando legittime le norme nazionali che escludono il diritto di intervenire con la possibilità di bloccare la trasmissione nel caso sia consentita ai contribuenti una contestazione dell'ingiunzione recante la richiesta di informazioni, sebbene solo “in via incidentale” nel giudizio d'impugnazione dell'atto impositivo. Il riconoscimento del diritto del contribuente di accesso al fascicolo sarebbe fondamentale per esercitare efficacemente il contraddittorio endoprocedimentale. L'autore auspica che la Corte di giustizia, alla luce del proprio orientamento più recente possa in futuro ampliare l'ambito di applicazione, riconoscendo *notification e consultation rights*.

⁵² G. VANZ, “Buona amministrazione” di cui all'art. 41 della Carta dei diritti fondamentali dell'Unione Europea e diritto tributario nazionale, in *Rass. trib.*, 2019, 15.

Tuttavia, la previsione di così tanti ed ampi strumenti di garanzia per il contribuente non deve sfociare in un'ipertutela di quest'ultimo che "svilisca" il contrapposto interesse fiscale⁵³.

Di questa problematica si è occupata, in una recentissima pronuncia,⁵⁴ la Corte europea dei diritti dell'uomo, chiamata a bilanciare il rispetto della vita privata e dei dati personali del contribuente con il perseguimento dello scopo legittimo di protezione del sistema fiscale in uno alla finalità di contrastare, in maniera efficace, il dilagante fenomeno dell'evasione⁵⁵. Occorre chiarire quando l'ingerenza pubblica risulti sproporzionata⁵⁶.

In via preliminare, i giudici sovranazionali hanno statuito che la pubblicazione di un elenco di "grandi" evasori, corredato di dati personali dei contribuenti, sul sito *web* di un'autorità fiscale nazionale non contrasta con l'art. 8 CEDU in tema di protezione della vita privata e del diritto alla riservatezza⁵⁷.

Dall'esegesi della sentenza si ricava che tramite la pubblicazione dei dati tributari dei maggiori evasori fiscali, il legislatore interno persegue lo scopo legittimo di mantenere un discreto margine di valutazione nella selezione delle misure più idonee a prevenire e contrastare tale fenomeno patologico.

⁵³ A. CONTRINO, *Banche dati tributarie, scambio di informazioni fra autorità fiscali e "protezione dei dati personali": quali diritti e tutele per i contribuenti?*, in Riv. dir. trib. online, 29 maggio 2019, 7.

⁵⁴ Corte Europea dei Diritti dell'Uomo, sez. IV, sentenza del 12 gennaio 2021, n. 36345/16.

⁵⁵ Per approfondimenti, si veda G. CHIARIZIA, *La pubblicazione della lista di evasori (caso L.B. c. Ungheria): il fine giustifica sempre i mezzi?*, in Giustizia insieme, 6 maggio 2021, 3 ss.

⁵⁶ Cfr. H.C. YOURROW, *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence*, The Hague, 1996, 188 ss.; Y. ARAI TAKAHASHI, *The defensibility of the margin of appreciation doctrine in the ECHR: value-pluralism in the European integration*, in *Revue Europeenne de Droit Public*, 2001, 1162 ss.; F. DONATI, P. MILAZZO, *La dottrina del margine di apprezzamento nella giurisprudenza della Corte europea dei Diritti dell'Uomo*, in *Rivista AIC*, 2002, 21 ss.; M.A. CASE, *Community Standards and the Margin of Appreciation*, in *Human Rights Law Journal*, 2004, 10 ss.; J.A. BRAUCH, *The Margin of Appreciation and the Jurisprudence of the European Court of Human Rights: Threat to the Rule of Law*, in *Columbia Journal of European Law*, 2004, 113 ss.; P. TANZARELLA, *Il margine di apprezzamento*, in M. Cartabia (a cura di), *I diritti in azione*, Bologna, 2007, 149 ss.; I. ANRÒ, *Il margine di apprezzamento nella giurisprudenza della Corte di giustizia europea e della Corte europea dei diritti dell'uomo*, in *La funzione giurisdizionale nell'ordinamento internazionale e nell'ordinamento comunitario: atti dell'incontro di studio tra i giovani cultori delle materie internazionalistiche* / edizione, 9-10 ottobre 2009, Napoli, 2010, 7 ss.

⁵⁷ A mente del quale, lo si ricorda, ogni persona "ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 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". Nello stesso senso, si veda altresì l'art. 12 della Dichiarazione universale dei diritti dell'uomo, adottata dall'Assemblea delle Nazioni Unite il 10 dicembre 1948, ove si riconosce che nessun individuo "potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni".

Per ciò, la misura può essere ritenuta indispensabile in un sistema democratico e proporzionato⁵⁸ con riferimento ai dati personali oggetto di pubblicazione ed alle modalità di quest'ultima⁵⁹.

Il tema della tutela dei dati personali e, quindi, della riservatezza del contribuente genera un significativo interesse in un'ottica di contemperamento con l'interesse pubblico alla pronta riscossione dei tributi ed al contrasto dell'evasione fiscale, in particolare se si prende in considerazione lo sviluppo del massivo utilizzo di strumenti tecnologici ed informatici ad opere delle autorità fiscali nazionali, in uno agli strumenti internazionali di scambio di informazioni.

La problematica promanante da tale operazione di bilanciamento atterrebbe alla censurata finalità perseguita dalla pubblicazione dei dati personali dei contribuenti in una sorta di *black list* degli evasori fiscali⁶⁰.

Difatti, si potrebbe ritenere che l'unico scopo preso di mira risieda nello screditare pubblicamente tali soggetti, esponendoli al pubblico ludibrio. Una misura così descritta non sarebbe caratterizzata da alcuna finalità legittima.

A ciò si aggiunga che la misura non potrebbe essere ritenuta idonea a raggiungere l'effetto di deterrenza auspicato rispetto alla reiterazione dell'evasione fiscale.

Tuttavia, sul punto si consideri che l'art. 8 CEDU, al paragrafo 2, stabilisce che le ingerenze sono giustificabili se previste dalla legge e sempreché rappresentino misure necessarie al perseguimento di finalità generali di significativo rilievo sociale, identificate nella sicurezza nazionale, nella pubblica sicurezza, nel benessere economico del paese, nella difesa dell'ordine pubblico, nella prevenzione dei reati, nella protezione della salute o della morale o ancora nella protezione dei diritti e delle libertà altrui.

⁵⁸ Più ampiamente sul principio di proporzionalità, v. G. MOSCHETTI, *Il principio di proporzionalità come "giusta misura" del potere nell'evoluzione del diritto tributario*, Milano, 2017, 1-22; P. BORIA, *Diritto tributario europeo*, 3ª ed., Milano, 2017, 208 ss.; G. MELIS, *Ragionevolezza, proporzionalità e giudizio di legittimità costituzionale in materia tributaria*, in Atti del Convegno di Napoli, 12 ottobre 2018; è noto che l'interesse pubblico all'attuazione e al controllo circa la corretta applicazione della normativa fiscale, è un interesse primario che deve essere perseguito dall'Amministrazione finanziaria sul punto v. anche G. E. DEGANI, *Il principio di proporzionalità nel rapporto tra contribuente e amministrazione finanziaria*, in *Dir. prat. trib. int.*, 4/2018, p. 1062 ss.; V.G. VANZ, *I principi della proporzionalità e della ragionevolezza nelle attività conoscitive e di controllo dell'Amministrazione finanziaria*, in *Dir. prat. trib.*, 2017, 1914; G. PETRILLO, *Il principio di proporzionalità nell'azione amministrativa di accertamento tributario*, Roma, 2015; A. FORNIELES GIL, *Il principio di proporzionalità*, (a cura di A. DI PIETRO, T. TASSANI, *I principi europei del diritto tributario*), Padova, 2014, 159; M.V. SERRANO, *Il rispetto del principio di proporzionalità e le garanzie del contribuente*, in *Riv. trim. dir. trib.*, 2014, 422 ss.; G. BIZIOLI, *Il processo di integrazione dei principi tributari nel rapporto fra ordinamento costituzionale, comunitario e diritto internazionale*, Bergamo, 2008, 110 ss.; A. MONDINI, *Coerenza fiscale e principio di proporzionalità: crisi del sistema o dell'armonizzazione*, in *Riv. dir. fin.*, 2007, 3, 41 ss.

⁵⁹ Sul rapporto tra il principio di proporzionalità e la dottrina del margine di apprezzamento, si veda A. MOWBRAY, *A Study of the Principle of Fair Balance in the Jurisprudence of the European Court of Human Rights*, in *Human Rights Law Review*, 2010, 10, 289 ss.; E. BINDI, *La Corte EDU alla ricerca del giusto equilibrio tra politica fiscale e tutela dei diritti fondamentali* (sentenza 1 maggio 2013, N.K.M. v. Ungheria), cit., 26; D. MCGOLDRICK, *A defence of the margin of appreciation and an argument for its application by the Human Rights Committee*, in *International and Comparative Law Quarterly*, 2016, 21 ss.

⁶⁰ G. MARINO, *Paradisi fiscali: dalle black list alle white list, dallo scambio di informazioni alla ricettazione di informazioni*, in G. FRANSONI (a cura di), *Finanziaria 2008*, Quaderni della rivista di diritto tributario, Milano, 2008, 213 ss. In argomento, si veda altresì A. BUCCISANO, *Cooperazione amministrativa internazionale in materia fiscale*, in *Riv. dir. trib.*, 2012, I, 704.

Sulla scorta di tale dettato normativo, i giudici della Corte Edu hanno affermato la meritevolezza dell'interesse di ogni persona, che voglia intrattenere rapporti economici con altri soggetti, ad ottenere le informazioni relative all'attitudine di questi ultimi ad osservare gli obblighi fiscali e, in sostanza, alla relativa affidabilità in ordine alle obbligazioni economiche contratte⁶¹.

Da ciò si evince che la divulgazione di informazioni private non tende ad appagare soltanto una mera curiosità, finanche morbosa, dell'opinione pubblica, bensì mira a garantire l'accesso ad informazioni utili per la correttezza degli scambi, la trasparenza dei negozi giuridici nonché per il buon andamento dell'economia all'interno di un sistema statale democratico.

Al riguardo si consideri che tale pubblicazione costituirebbe l'adeguata risposta ad un pressante bisogno sociale derivante dalla prevenzione e dalla repressione all'evasione fiscale tramite l'implementazione degli strumenti funzionali a tale scopo.

Occorre rilevare, inoltre, che la misura in esame risulterebbe proporzionata poiché limitata solamente ai "grandi" evasori e destinata alla cessazione immediata in caso di adempimento del debito fiscale da parte del contribuente.

Infatti, in qualsiasi Stato di diritto ogni misura statale che, pur nel perseguimento di finalità meritevoli di tutela, è idonea a recare un pregiudizio al relativo destinatario non deve mai eccedere quanto sia strettamente necessario per conseguire tale scopo⁶².

Dunque, l'esigenza di garantire la protezione dei dati personali è tendenzialmente superata dall'interesse erariale qualora si tratti di dati fiscali pubblicati col fine di fornire adeguato strumento di lotta alla corruzione.

Questo, chiaramente, non implica che i diritti fondamentali della riservatezza della vita privata e della protezione dei dati personali debbano ritenersi ogni volta recessivi nei confronti dell'interesse fiscale.

Difatti, si deve osservare che, per quanto meritevole di tutela, siffatto interesse non può spingersi fino a legittimare la profilazione indiscriminata o il trattamento generalizzato, incondizionato ed automatico, di dati personali di massa dei contribuenti. Trattasi di operazioni sproporzionate rispetto alle logiche garantiste contemplate dagli artt. 7 e 8 CEDU.

A tal proposito un fenomeno patologico da evitare, frequente nel contesto della cooperazione fiscale internazionale, è quello delle cc.dd. *fishing expeditions*⁶³, consistente in quelle misure finalizzate al raccoglimento di mezzi di prova inerenti ad una determinata condotta potenzialmente punibile, senza che esista ancora alcun indizio di portata sufficientemente obiettiva e concreta concernente l'esistenza di tale condotta⁶⁴.

⁶¹ Al riguardo, si veda per tutti l'ampio studio di A. VIOTTO, *Il "diritto al rispetto della vita privata e familiare" nell'ambito delle indagini tributarie, nel quadro della giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in Riv. trim. dir. trib., 2019, 153 ss.

⁶² M. P. NASTRI, *L'habeas data in materia tributaria fra procedimento amministrativo e diritto europeo*, in Dir. e prat. trib. intern., 2021, 3.

⁶³ Corte di Giustizia UE, sentenza del 25 novembre 2021, C-437/19, ECLI:EU:C:2021:953.

⁶⁴ Per una definizione del concetto, e per approfondimenti anche in chiave comparatistica, si veda P. BERNASCONI, S. SCHURCH, *Fishing expedition e rogatorie di gruppo nella cooperazione internazionale con la Svizzera in materia fiscale. Norme e prassi recenti e imminenti*, in Riv. dir. trib., 2015, 109 ss.

6. Riflessioni conclusive.

Dalle considerazioni svolte si evince, in via tendenziale, una sempre maggiore apertura verso l'accesso anche in ambito tributario e, pertanto, sarebbe opportuno che il diniego delle relative istanze venisse opposto dall'amministrazione finanziaria al contribuente soltanto in via eccezionale, sulla base cioè di un'esigenza di segretezza già individuata dalla legge, senza che l'autorità fiscale possa esprimere alcuna valutazione discrezionale sull'an del diritto, così garantendo la legalità e la correttezza dell'agire amministrativo.

Eventuali determinazioni discrezionali non ancorate al dettato normativo, difatti, rischierebbero di restringere il grado di trasparenza della PA, sebbene la discrezionalità spesso si presenti come valore fondamentale, in termini di ragionevolezza, al fine di adottare la soluzione migliore per il caso concreto così come esso si presenta nella sua unica, ed irripetibile, manifestazione reale.

In quest'ottica dovrebbe essere l'ordinamento a selezionare i casi in cui l'interesse fiscale debba essere tutelato mediante la compressione di un diritto del contribuente (come si è visto nel caso sull'evasione fiscale affrontato dalla Corte Edu nel 2021) e quando, invece, il suddetto interesse generale e tale diritto soggettivo possano coesistere ed essere entrambi preservati, a nulla rilevando la fase in cui perviene l'istanza e, dunque, l'avvenuta formazione dell'atto impositivo.

Chiaramente, trattasi di una prospettiva *de iure condendo*, che si inserisce in un più ampio processo già in atto di cambiamento della visione del rapporto Fisco-contribuente, sempre più improntato alla collaborazione, alla partecipazione ed alla trasparenza, come dimostra il nuovo regime di adempimento collaborativo ossia uno strumento che attua una cooperazione preventiva che eviti l'irregolarità stessa.

Il progressivo ampliamento della c.d. *tax compliance* testimonia come necessariamente si debba passare attraverso una ridefinizione del rapporto intercorrente fra amministrazione finanziaria e contribuente che si fondi anche sull'accesso agli atti tributari, finanche procedimentali, laddove compatibile con gli obiettivi previsti e tutelati dall'ordinamento. Questo risulterebbe, altresì, conforme agli orientamenti attuali e prevalenti in seno alla giurisprudenza eurounitaria.

Tutto ciò senza mai perdere la bussola: la stella polare che deve guidare i giuristi, in senso lato, deve sempre risiedere nel bilanciamento fra opposti interessi meritevoli, in astratto, di tutela con la conseguenza che, da un lato, certamente occorre evitare ingerenze sproporzionate dell'amministrazione finanziaria nella sfera soggettiva personale privata del contribuente e, dall'altro lato, occorre però stare attenti a non fornire un'ipertutela alle garanzie del contribuente, dalle quali potrebbe scaturire un ingiusto sacrificio dell'interesse fiscale.



Necro-robotica e circolazione dei dati personali post mortem.

Necro-robotics and post-mortem circulation of personal data.

REMO TREZZA 

Ph.D. in Civil Law and Contract Professor of Private law
Università degli Studi di Salerno

Abstract

Il saggio affronta la delicata questione della necro-robotica e le sue implicazioni etico-giuridiche. Il contributo, inoltre, si concentra sull'analisi della normativa in materia di protezione dei dati personali post mortem e sulla loro disponibilità ora per allora, con un approccio sistematico-applicativo della normativa in tema di disposizioni anticipate di trattamento.

The essay deals with the delicate question of necro-robotics and the ethical-legal implications of the problem. Furthermore, the contribution focuses on the analysis of the legislation on the protection of post-mortem personal data and their availability now by then, with a systematic-application approach of the law on advance processing provisions.



Keywords: artificial intelligence; necro-robotic; *post mortem* personal data protection; advance digital processing provisions.

Summary: [Introduction](#). – [1. Necro-algoritmica: vantaggi e svantaggi](#). – [2. Tecniche neuro-scientifiche e privacy neuronale. Cenni sul c.d. neuro-marketing](#). – [3. Il diritto civile “algoritmico”: eredità digitale e circolazione dei dati personali post mortem](#). – [Conclusions](#).

Introduction.

La vita della persona umana, sin dal suo inizio, è costellata di “tecniche artificiali¹”. Durante il suo sviluppo, ancora, è aiutata da “intelligenze artificiali²”. Sino, si può dire, alla sua morte. Sì, perché nelle fasi terminali della vita umana o successivamente alla vita umana stessa, l’intelligenza artificiale e la robotica possono essere di ausilio alla persona – umanizzazione della macchina³ –. Si pensi allo sviluppo di robot che riproducono la fisionomia e le fattezze fisiche e materiali di una persona cara estinta. Coloro che, restando in vita, non accettano o fanno fatica ad accettarne la morte, possono adoperare una tecnica necro-robotica che possa aiutarli ad accettarne la mancanza. Ciò va sotto il nome di “terapia psicologica accettazione⁴”.

Tale aspetto implica che l’intelligenza artificiale, tra cui gli algoritmi che la costituiscono, debba essere costruita *ex ante* e perfezionata *in itinere* ed *ex post* per il fine continuativo ed ultimo di protezione della persona umana (*ethics by design/ethics by default*). Per tale ragione, i sistemi intelligenti sembrano dover essere proiettati ad una valutazione di meritevolezza “ciclica” e, anche qualora il sistema dovesse subire modifiche (*rebus sic stantibus* artificiale), questo dovrà sempre essere vagliato nella sua meritevolezza⁵. L’algoritmo, dunque, deve essere “protettivo”, mai “distruttivo” (si pensi ai droni militari e al potenziamento umano), né “sostitutivo” (si pensi al giudice-robot)⁶.

¹ Si faccia riferimento alle tecniche artificiali di procreazione assistita, molte delle quali disciplinate dalla famosa Legge n. 40/2004, sulla quale non pochi problemi vengono sollevati – molto spesso – dalla dottrina e dalla giurisprudenza più avvedute. Sul punto, si rinvia a S. ALBANO, *Tecniche di procreazione assistita e direttive di fine vita*, in *Questione giustizia*, 4 maggio 2015, consultabile online; A. CARRATO, *La procreazione medicalmente assistita e le tematiche connesse nella giurisprudenza costituzionale*, in *Servizio Studi Corte costituzionale*, marzo 2021, pp. 1-54, consultabile online; G. CAPIZZI, *Procreare: diritto, interesse o mera aspirazione? Brevi osservazioni di teoria generale in margine*, in *Rivista di biodiritto*, 2011, pp. 1-27, consultabile online. Da ultimo, si faccia riferimento alle nuove tipologie di procreazione: quella *post mortem* e quella *post matrimonio*, su cui si consenta rinviare a R. TREZZA, *Fecondazione post mortem: sopravvivenza del consenso del coniuge espresso in vita, rettificazione dell'atto dello stato civile e attribuzione del cognome paterno* (Corte di Cassazione, Prima Sezione Civile, sentenza n. 13000 del 15 maggio 2019), in *Giustizia insieme*, 12 settembre 2019, pp. 1-29, con ampi riferimenti bibliografici e R. TREZZA, *La fecondazione omologa post matrimonio: l'embrione crioconservato è “concepito”?*, in *Famiglia*, 15 febbraio 2022, pp. 1-20, con ricca e recente bibliografia.

² Sul punto, si consenta rinviare a R. TREZZA, *I diritti della persona tra “tecniche” e “intelligenze” artificiali. Casi, questioni, prospettive*, Cile, 2021.

³ Cfr. R. TREZZA, *Diritto e intelligenza artificiale. Etica, Privacy, Responsabilità, Decisione*, Pisa, 2021.

⁴ Si rinvia, a tal uopo, a S. AMATO, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Torino, 2020.

⁵ Sia consentito il riferimento a R. TREZZA, *Artificial Intelligence Act. Giudizio “ciclico” di meritevolezza e accountability intelligenti*, Roma, 2021.

⁶ Su tale specifica questione, sia consentito rinviare a R. TREZZA, *L'algoritmo “protettivo”: gli istituti di protezione della persona alla prova dell'Intelligenza Artificiale*, in *Tecnologie e diritto*, n. 1/2021, p. 217 ss.

La persona umana – agente – lascia disseminati però, con tali sistemi e in tali sistemi, una serie di dati personali – molti dei quali anche fin troppo sensibili –.

Come possono essere trattati tali dati dopo la morte del titolare?

Secondo le disposizioni del GDPR, armonizzato con il D. Lgs. n. 101/2018, questi dati cadono in eredità e possono essere accessibili a chi dimostra di avere un interesse meritorio di tutela, salvo che il titolare ne abbia espressamente vietato l'accesso⁷.

È possibile però che il titolare di tali dati, nel rispetto del suo diritto all'oblio – *right to be forgotten*⁸ – di cui può disporre prima della sua morte, ma che ha effetti ultra-attivi, possa accordarsi con le piattaforme, che tali dati detengono, affinché i dati medesimi vengano distrutti?

Sarebbe possibile approdare ad una risposta affermativa qualora si traslasse la disciplina, già adottata nel 2017, in tema di disposizioni anticipate di trattamento, anche ai dati personali *post mortem* (in tal caso, appunto, potrebbe parlarsi di “disposizioni anticipate di trattamento digitale”).

Adottando tale misura, dunque, sarebbe possibile decidere sui propri dati “ora per allora”.

È il caso di dire che il consenso *ex ante* per la circolazione dei propri dati personali *ex post* sia del tutto “negoziato”⁹. La *privacy* è un diritto fondamentale che muore con la persona o continua a produrre i suoi effetti anche dopo?¹⁰

A tal punto, qualora la traslazione di disciplina fosse possibile, la persona potrebbe anche nominare un esecutore testamentario (se si esprime un

⁷ A tal proposito, si vedano le pronunce del Tribunale di Bologna e di Milano del 2021 e del Tribunale di Roma, proprio di recente, del 10 febbraio 2022, sulla c.d. “eredità digitale”. In dottrina, I. MARTONE, *Sulla trasmissione a causa di morte del “patrimonio digitale”*, in *Tecnologie e diritto*, n. 2/2020, p. 420 ss.; A. VESTO, *Successione digitale e circolazione dei beni online. Note in tema di eredità digitale*, Napoli, 2020. Da ultimo, si rinvia a R. E. DE ROSA, *La trasmissibilità mortis causa dei dati digitali*, in *Famiglia*, 5 aprile 2022, consultabile *online*, la quale individua tre direttrici sulle “cause di eredità digitale”, ovvero: «... [1] tutte le ordinanze originano da ricorsi presentati ai sensi dell'art. 700 c.p.c. Invero, ciò non sorprende, posta l'assenza di altri specifici rimedi giurisdizionali; [2] in tutti i casi la legittimazione dei ricorrenti all'esercizio *post mortem* dei diritti digitali del defunto viene rinvenuta nella sussistenza di «ragioni familiari meritevoli di protezione». Invero, tali ragioni non risultano ben esaminate e finiscono per ridursi all'accertamento del mero vincolo di coniugio o di parentela tra il ricorrente ed il *de cuius*; [3] in tutti i casi si esclude che la volontà del defunto – finalizzata all'esclusione della trasmissione del suo *account* – possa rinvenirsi nell'adesione alle condizioni generali di contratto predisposte unilateralmente dai Invero, non sembra che i giudici si siano interrogati sulla possibilità di ricavare *aliunde* la manifestazione di volontà specifica, libera ed informata, cui fa riferimento l'art. 2-terdecies, comma 3, D. Lgs. n. 101/2018».

⁸ Si rinvia alla disamina che ne fa F. LAZZARELLI, *Tutela dei dati personali nell'età globale: il diritto all'oblio*, in *Le Corti salernitane*, n. 1/2021, p. 3 ss.

⁹ Cfr., sul punto, C. IRTI, *Consenso “negoziato” e circolazione dei dati personali*, Torino, 2021.

¹⁰ A tale interrogativo, oltre a rispondere in maniera più esaustiva nel corso del contributo, può affiancarsi il riferimento alla c.d. Proposta *Data Act* dell'Unione europea del 23 febbraio 2022, la quale ha come obiettivo principale quello di garantire un'armonizzazione europea della disciplina dei dati e, in particolar modo, la funzione specifica di garantire la libera circolazione dei dati personali (portabilità). I principi cardine della Proposta possono essere, infatti, così enunciati: «Scorrendo l'articolato ritroviamo, ancora una volta, alcuni principi cardine di tanta parte dell'attuale disciplina europea del settore, divenuti ormai familiari ai più, come il principio di accessibilità dei dati (“ove possibile diretta”) previsto dell'art. 3 e gli obblighi informativi “in un formato chiaro e comprensibile” (sempre art. 3); ma troviamo, anche, il “diritto di accedere ai dati” e il “diritto di condividere i dati con terzi” (inseriti agli artt. 4 e 5); e, ancora, il meccanismo compensativo per la messa a disposizione dei dati, (previsto dall'art. 9), che pur nella sua necessaria “ragionevolezza” sottolinea ulteriormente il valore di tali dati; infine, la possibilità, per le PMI (micro e piccole, come da definizione consolidata Ue) di utilizzare le condizioni contrattuali, non vincolanti, che la Commissione svilupperà e raccomanderà, clausole *standard* che aiuteranno le PMI a negoziare contratti di condivisione dei dati più equi ed equilibrati con le aziende che godono di una posizione di maggior forza contrattuale». Tale inciso è preso da M. RAGONE, V. PATRUNO, *Data Act: cosa prevede la proposta europea sui dati e cosa cambierà per PA e imprese*, in *Forum PA*, 5 aprile 2022, consultabile *online*.

consenso del genere nell'atto di ultima volontà) il quale dovrebbe procedere a far rispettare il diritto all'oblio del disponente. E se non vi fosse un testamento, allora bisognerà nominare un curatore dei dati personali. È a tal proposito che anche l'autonomia contrattuale, insieme con il giudizio di meritevolezza di una eventualità di un contratto atipico, quale può essere il "contratto di oblio", dovrà essere rivista¹¹.

Temi, dunque, che vanno affrontati con solerzia e rigore, anche in un'ottica squisitamente comparatistica¹². Il tutto per garantire un diritto fondamentale della persona umana ex art. 2 Cost. qual è il diritto all'autodeterminazione digitale e informativa¹³.

¹¹ Su tale indirizzo, si rinvia a M. ZANICHELLI, *Il diritto all'oblio tra privacy e identità digitale*, in *Informatica e diritto*, n. 1/2016, pp. 9-28; R. PARDOLES, *L'ombra del tempo e (il diritto all')oblio*, in *Questione giustizia*, n. 1/2017, specie p. 85, ove l'A. afferma che: «Al netto dei suoi tanti (e inevitabili) contorcimenti, il diritto all'oblio, nella sua versione *time-honored* – quella che declina la contrapposizione di privacy e libertà d'informazione, riallacciandosi a una tradizione risalente ma in via di continua ridefinizione –, appare in grado di fronteggiare la ricerca di equilibri accettabili anche in un mondo di nativi digitali»; A. COLARUOTOLO, *Il passato che non passa. La parola delle Sezioni Unite sul delicato rapporto esistente tra memoria storica, cronaca e oblio*, in *Diritto Mercato Tecnologia*, 13 dicembre 2019, specie p. 42, ove, in maniera del tutto condivisibile con la prospettiva dello scrivente, l'A. evidenzia che: «la protezione dei diritti inviolabili della persona deve costituire il principale criterio di orientamento per l'interprete nell'esegesi del quadro normativo e nel bilanciamento tra diritti fondamentali al fine di assicurare il rispetto della dignità umana. Nello spazio giuridico europeo, quest'ultima va a delineare il "contenuto essenziale" (*Wesensgehalt*) dei diritti fondamentali, anche ai sensi delle previsioni di cui agli artt. 1 e 52 CDFUE. Siffatta prospettiva appare l'unica compatibile e conciliabile con il principio personalistico di cui all'art. 2 Cost. che concepisce la persona come un valore in sé da tutelare rispetto a ogni strumentalizzazione dell'individuo per fini eteronomi»; M. BIANCA, *Memoria ed oblio: due reali antagonisti?*, in *Media Laws*, n. 11/2019, specie p. 36, ove l'A. sottolinea che: «Quanto al diritto all'oblio, anche se tradizionalmente contrapposto alla memoria, esso ne è l'altra faccia. Il diritto all'oblio, in quanto diritto all'identità aggiornata, è un "diritto all'identità attuale della persona". La diversa articolazione del tempo nei due diritti non è tale da offuscare il filo rosso comune che è l'esigenza del soggetto di avere una fedele rappresentazione di sé. Intesa in questi termini la memoria non può essere intesa come antagonista del diritto all'oblio ma come il medesimo diritto che riceve una diversa connotazione diacronica».

¹² Vedi le pronunce della Corte federale tedesca sull'eredità digitale oppure la legge sul patrimonio digitale svizzera o, ancora, la piattaforma digitale già istituita in Spagna (prende il nome di *Mylegadodigital*). Sul primo punto, si rinvia a A. CAPOLUONGO, *Social, privacy ed eredità digitale: la pronuncia della Corte tedesca fa scuola*, in *Cyber Laws*, 31 luglio 2018, consultabile *online*, ove si legge che: «La parola fine sulla vicenda, però, l'ha scritta di recente la Corte di Cassazione (BGH) di Karlsruhe che con sentenza del 12 luglio 2018, in aperto contrasto con la pronuncia della Corte d'Appello, ha statuito che "il contratto che riguarda l'account di un utente con un social network è trasferito agli eredi del detentore originario dell'account" e che gli eredi "hanno diritto a rivendicare dall'operatore l'accesso all'account, compresi i dati della comunicazione". È facile comprendere, quindi, la rilevanza della pronuncia che ha riconosciuto per la prima volta l'esistenza di una vera e propria "eredità digitale", considerando la password, il profilo social, i post e i messaggi privati alla stregua di beni materiali quali le lettere e i diari del *de cuius*. Fino ad oggi, infatti, le alternative su Facebook in caso di decesso erano solo tre: l'utente aveva la possibilità di identificare una persona specifica quale "contatto erede"; i parenti di una persona deceduta potevano comunicare alla piattaforma se chiudere il profilo oppure potevano renderlo un account commemorativo, ma di certo era negato qualsivoglia diritto ereditario».

¹³ Di tale "nuovo diritto" se n'è dato atto nella c.d. Dichiarazione dei diritti di Internet, elaborato dalla Commissione per i diritti e i doveri relativi ad Internet a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015, in particolare all'art. 5, co. 4, secondo il quale: «4. I dati devono essere trattati rispettando i principi di necessità, finalità, pertinenza, proporzionalità e, in ogni caso, prevale il diritto di ogni persona all'autodeterminazione informativa». Non si dimentichi la sentenza n. 1846/2015 del Tribunal Constitucional del Perù proprio in tema di diritto all'autodeterminazione informativa. In dottrina, tra i tanti, si rinvia a A. PALUMBO, *Il diritto all'autodeterminazione informativa. L'esperienza tedesca in materia di protezione dei dati personali*, tesi di dottorato discussa nell'anno 2015-2016 presso il Dipartimento di Giurisprudenza dell'Università Bicocca di Milano, specie p. 103, ove si legge: «Come indicato da Luhmann, i concetti di uomo, società e comunicazione non possono più essere considerati isolatamente: vivono di una relazione simbiotica, in cui si rinforzano e si arricchiscono reciprocamente di significato. All'individuo, inteso come "un soggetto (*Persönlichkeit*) che si sviluppa all'interno di una comunità sociale e che dipende dalla comunicazione", va quindi riconosciuto il diritto

1. Necro-algoritmica: vantaggi e svantaggi.

Un tema assai dibattuto, specie in questi ultimi periodi, è quello relativo, oltre al potenziamento umano¹⁴, che desta moltissime perplessità¹⁵, quello della necro-algoritmica, fenomeno per il quale si fa “risuscitare” virtualmente una persona deceduta per il bene di un caro ancora in vita¹⁶.

In merito alla questione del potenziamento umano¹⁷, ove l’I.A. viene utilizzata per la preparazione dei soldati (specie in America) affinché questi possano affrontare al meglio la guerra e qualsiasi altro tipo di battaglia per sconfiggere definitivamente e con tutti i mezzi possibili (si veda, per esempio, i droni-bomba¹⁸ o le tecnologie innescanti guerre cibernetiche¹⁹) il nemico, viene da chiedersi se

fondamentale di essere informato sull'utilizzo dei propri dati e, in determinate circostanze, di poter influenzare questo processo».

¹⁴ Sul punto, si rinvia a S. AMATO, *Biodiritto 4.0.*, cit., p. 120. Inoltre, si rinvia allo scritto interessante di P. PERLINGIERI, *Note sul “potenziamento cognitivo”*, in *Tecnologie e diritto*, n. 1/2021, p. 209 ss.

¹⁵ Sull'uomo c.d. “aumentato”, si veda S. CUCCHETTI, *Homo creativus. Nuove sfide per la bioetica*, in *Il Regno – Attualità*, n. 16/2019, p. 477, ove si evidenzia che: “Le questioni delle tecniche d'intelligenza artificiale, d'integrazione uomo-macchina, di gestione dei dati e di potenziamento umano richiedono una verifica attenta e un discernimento serio sulle strutture di *governance* che le guidano e le regolano. Il pericolo più grande che si possa realizzare è una gestione che non conosca il potenziale di queste tecniche e il loro funzionamento, mentre la questione etica si traduce in un discernimento sulle strutture socio-economiche e sulla idea d'innovazione e progresso che le nutre”; A. DI CORINTO, *Siamo pronti a vivere nell'età dell'essere umano “aumentato”? Il potenziamento del corpo umano è ormai una realtà tecnologica. Ora la sfida è mettere al sicuro i dati e prevenire gli attacchi informatici*, in *www.wired.it*, 24 marzo 2021, consultabile online, ove si legge che: “Le riflessioni relative al potenziamento biologico ripercorrono almeno 30 anni di dibattito, dalle cyberstrategie protesiche di Stelarc al ruolo delle tecnologie dell'intelligenza di Pierre Lévy e al successo del Partito Transumanista di Istvan Zoltan che, immaginando un futuro di esseri potenziati dalla tecnologia, predica il potenziamento umano per sconfiggere morte e malattie. Un futuro che è già presente. Così tanto presente da porci serie domande su come evolverà il nostro già stretto rapporto con la tecnologia. A cominciare dal fatto che ogni dispositivo artificiale può essere hackerato. Includere le protesi che sono connesse in rete e la cui sicurezza è fondamentale. Come ha detto Modesta, che sente “di aver bisogno di una sorta di maggiore sicurezza, per il rapporto intimo che tutti abbiamo con la tecnologia”, e che “ci obbliga”, secondo David Jacoby di Kaspersky, a farlo prima di immettere nuove tecnologie sul mercato: “Se non ci pensiamo oggi dovremo pensarci domani”, visto che nel futuro prossimo queste tecnologie saranno economiche e disponibili a tutti”; M. SARTORI, *Potenziamento umano e vulnerabilità: la lezione di Coeckelbergh*, in *www.colloquidibioetica.com*, 21 marzo 2021, consultabile online, il quale propone una “regolamentazione giuridica del fenomeno”. In chiave completamente critica rispetto al fenomeno, si rinvia a E. PERUCCHIETTI, *Cyberuomo. Dall'intelligenza artificiale all'ibrido uomo-macchina. L'alba del transumanesimo e il tramonto dell'umanità*, Geraci Siculo, 2020.

¹⁶ Si veda, nel rapporto corpo e nuove tecnologie, C. MACCAFERRI, *Il corpo nell'era digitale: dal simulacro alla performance capture*, tesi di dottorato discussa presso l'Università del Sacro cuore di Milano nell'anno accademico 2011-2012, consultabile online.

¹⁷ Cfr. S. AMATO, *Neuroscienze e utilizzazione militare delle tecniche di potenziamento umano*, in *Ethics & Politics*, n. 2/2014, pp. 182-198.

¹⁸ Su tale aspetto, è intervenuta la Risoluzione del Parlamento europea del 21 gennaio 2021, proprio sui temi del diritto internazionale militare e le implicazioni sull'utilizzo delle nuove tecnologie in guerra. Sul punto, A. AZZARITI, *Attacchi con i droni: profili di diritto internazionale*, in *Cyber Laws*, 19 novembre 2018, consultabile online. Inoltre, si veda il Rapporto di ricerca dell'Istituto di Ricerche Internazionali Archivio Disarmo – IRIAD, Roma, aprile 2017, consultabile online, dal titolo “*Droni militari: proliferazione o controllo?*”.

¹⁹ Cfr., sul punto, L. MARTINO, *La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica*, in *Center for Cyber Security and International Relations Studies*, consultabile online, pp. 1-60.

il limite della dignità umana²⁰ venga, in tal caso, rispettato²¹.

Si conduca, poi, un'indagine sulla responsabilità – anche sul profilo internazionale²² – derivante dai danni (anche da morte ingiusta²³) provocati dai droni militari²⁴ guidati da un essere umano al fine di “localizzare” velocemente il

²⁰ Cfr., sul punto, G. AZZONI, *Dignità umana e diritto privato*, in *Ragion pratica*, n. 1/2012, p. 75 ss.; C. PICIOCCHI, *La dignità come rappresentazione giuridica della condizione umana*, Padova, 2013, specie p. 246, ove si evidenzia che: “Se la dignità come nucleo fondante gli ordinamenti costituzionali è un dato acquisito del secondo dopoguerra, la dignità nel suo rapporto con la libertà degli individui rappresenta invece una delle sfide contemporanee, fornendo però una chiave di lettura importante per comprendere il panorama giuridico attuale, rappresentando sia acquisizione sia programma, ma sicuramente ponendosi come risorsa cruciale”; G. M. FLICK, *Elogio della dignità (se non ora, quando?)*, in *Rivista AIC*, n. 4/2014, specie p. 31, ove si mette in luce che: “Infatti, tutti i diritti fondamentali tutelati dalla Costituzione – osserva la Corte – sono in rapporto di integrazione reciproca fra di loro. Nessuno di essi può avere la prevalenza assoluta sugli altri; nessuno di essi può espandersi illimitatamente e divenire “tiranno” nei confronti dell’insieme delle altre situazioni giuridiche costituzionalmente protette, che è espressione della dignità della persona”; N. GUASCONI, *La dignità umana come fondamento e limite del sistema delle libertà*, in *Riv. trim. sc. amm.*, n. 2/2015, pp. 83-100; F. VIOLA, *Dignità umana, diritti e legge naturale*, in *Prudentia Iuris*, n. 83/2017, p. 31 ss.; L. LEO, *Dignità e costituzione: storia di un diritto controverso*, in *Cammino Diritto*, n. 8/2020, pp. 1-25; F. MASTROMARTINO, *Due concetti di dignità per due concetti di autonomia?*, in *Diritto e Questioni pubbliche*, n. 1/2021, p. 239 ss.

²¹ Questione centrale dibattuta anche da S. AMATO, *Biodiritto 4.0.*, cit., p. 167 ss.

²² Cfr., in tema, L. PARONA, *Prospettive europee e internazionali di regolazione dell'intelligenza artificiale tra principi etici, soft law e self-regulation*, in *Rivista della regolazione dei mercati*, n. 1/2020, consultabile online; A. CONFALONIERI, *L'AI deve apprendere i valori dell'UE e il rispetto dei diritti umani*, in www.unionedirittumani.it, 31 marzo 2021, consultabile online; R. SAMPERI, *Brevi riflessioni in merito al possibile impatto dell'Intelligenza Artificiale sui diritti umani*, in *Cammino Diritto*, n. 7/2021, consultabile online.

²³ Sul punto, la Redazione della Rivista *Opinio Iuris* ha pubblicato un Report, il 1° settembre 2021, dal titolo “I droni che uccidono”, consultabile online, ove si legge che: “Non è da dimenticare, comunque, che molti giuristi sostengono che l’attuale quadro normativo del diritto internazionale sia già sufficiente a regolamentare efficacemente l’uso dei droni armati senza ulteriore codificazione. Ciò può essere vero, ma di fronte alla centralità che i droni stanno assumendo nei conflitti armati contemporanei la necessità di norme giuridiche chiare ed efficaci che disciplinino la condotta dei droni armati dovrebbe essere una priorità per la comunità internazionale”.

²⁴ Cfr., sul punto, soprattutto alla luce del clima di guerra che si respira nel continente europeo all’indomani dell’invasione dell’Ucraina da parte della Russia, F. RUSCHI, *Il volo del drone. Verso una guerra post-umana? Una riflessione di filosofia del diritto internazionale*, in *Jura Gentium*, n. 1/2016, p. 12 ss.; P. RIVELLO, *Gli aspetti giuridici connessi all’uso dei droni*, in *Il diritto penale della globalizzazione*, 31 maggio 2018, consultabile online, il quale osserva che: “Bisogna, semplicemente, in aderenza alle indicazioni offerte dal Working Group art. 29, essere particolarmente attenti agli effetti potenzialmente invasivi ricollegabili al loro uso, in quanto sottratti alla percezione dei singoli eventualmente sottoposti ad operazioni di sorveglianza “dall’alto”. Non a caso il Gruppo dei Garanti costituenti il Working Group ha raccomandato ai costruttori di droni l’adozione di misure di *privacy by default* e l’adozione di misure volte a rendere quanto più possibili visibili ed identificabili i droni utilizzati a fini commerciali. Valgono, per il resto, i criteri generali in tema di captazioni di immagini, volte a vietare le riprese all’interno di luoghi di privata dimora ed al contempo a consentire le riprese in luoghi pubblici, giacché in tal caso le persone inquadrare nelle riprese possono essere considerate parte integrante del paesaggio ripreso, in quanto “necessariamente” consapevoli della loro esposizione”; C. MELONI, *Droni armati in Italia e in Europa: problemi e prospettive*, in *Diritto penale contemporaneo*, 2017, pp. 1-48; N. COLACINO, *Impiego di droni armati nella lotta al terrorismo e accesso alla giustizia da parte delle vittime*, in *Rivista di diritto dei media*, n. 2/2018, p. 1 ss.; L. DAMIANO, F. SONGINI, *Se l’intelligenza artificiale uccide, senza controllo umano: ecco i punti chiave del dibattito*, in *Agenda digitale*, 10 giugno 2021, consultabile online. Sull’utilizzo dei droni “ordinari” e la loro implicazione sul diritto alla *privacy*, si rinvia a E. DAMIANI, *L’utilizzo dei droni e le inerenti ricadute sul diritto della privacy e della responsabilità civile*, in *Diritto Mercato Tecnologia*, n. 5/2021, specie p. 53, ove l’A. conclude in tali termini: “nel contesto normativo attuale, risulta sempre più diffusa la creazione e la diffusione di “regole tecniche” che delineano in maniera chiara le caratteristiche strutturali e gli *standards* di sicurezza dei mezzi aerei a pilotaggio remoto. La giuridicizzazione di questi parametri tecnici – da realizzare previo richiamo degli stessi attraverso le fonti di normazione primaria – può risultare di grande utilità al fine di garantire l’efficace funzionamento del mercato ed una sana competizione tra gli operatori del settore nell’Unione europea”; ID., *Privacy e utilizzo dei droni in ambito civile*, in *European Journal of Privacy Law & Technologies*, n. 1/2021, p. 158 ss.

nemico e “annientarlo”.

In merito alla seconda questione, invece, bisogna dire che tecniche, come quelle messe a punto da Neuralink²⁵, o anche le *chatbot* risuscitative²⁶ di morti creino dei problemi, oltre che sul piano strettamente etico, anche sul piano giuridico.

Anche qui, è bene ribadire che qualsiasi “nuova creazione artificiale” debba sempre passare attraverso il vaglio di meritevolezza etica e giuridica.

Neuralink, per esempio, potrebbe, tra i vantaggi percepibili, essere in grado, attraverso il collegamento diretto “strumento informatico-cervello umano”, di ridonare le capacità fisiche e riabilitative ad un atleta paraplegico²⁷.

I *robot* tridimensionali che ricreano la fisionomia virtuale del defunto potrebbero, invece, avere il vantaggio di curare l'assenza fisica di una persona cara che ha provocato delle condizioni degenerative a livello psichico nella persona che resta in vita. Il limite all'utilizzo di quest'ultima invenzione deve essere scandito dal tempo di rielaborazione del lutto, attraverso una vera e propria “terapia accettazionale” che porta al percorso psicologico di accettazione dell'evento-morte e al riacquisto della serenità psicologica della persona umana ancora in vita²⁸.

Solo in tale dimensione, anche le *chatbot*, ovvero i ripetitori verbali di conversazioni con la voce dei defunti, potranno essere utilizzate.

Vi dovrà sempre essere un vaglio meritevole e una finalità altrettanto meritevole che vada nel senso della *best human protection*²⁹. Anche in tal caso,

²⁵ Neuralink Corporation è una azienda statunitense di neuro-tecnologie, fondata da un gruppo di imprenditori, tra cui Elon Musk, che si occupa di sviluppare interfacce neurali impiantabili. La sede dell'azienda è a San Francisco; è stata avviata nel 2016 e fu riportata pubblicamente per la prima volta a marzo 2017. Il marchio “Neuralink” è stato acquistato dai precedenti proprietari a gennaio 2017.

²⁶ Voci internazionali fanno sapere che addirittura alcuni ricercatori americani sarebbero alla ricerca di cellule staminali capaci di far ripartire il cervello, dopo la morte, da zero e progredire dallo stadio di sviluppo zero a quello ultimo del ciclo naturale. Questo, ad esempio, sarebbe un chiaro esempio di “disumanizzazione” dell'uomo.

²⁷ È recente, infatti, la notizia che degli elettrodi impiantati nel midollo spinale possano far ritornare la dinamica fisica alle persone. Si veda, in tal senso, *Tre pazienti paralizzati tornano a camminare grazie a elettrodi impiantati nel midollo spinale*, su *Focus*, consultabile online.

²⁸ Sul binomio I.A.-psicologia, si veda R. CUBELLI, *Psicologia e intelligenza artificiale tra ampliamento della conoscenza e innovazione tecnologica*, in *Giornale italiano di psicologia*, n. 1/2018, p. 105 ss.; M. LAZZERI, *Intelligenza artificiale e psicologia, un binomio possibile: il punto sulle ricerche*, in *Agenda digitale*, 20 ottobre 2021, consultabile online; E. GALLETTI, *Intelligenza artificiale e benessere psicologico: l'idea di IDEGO presentata all'European Conference on Digital Psychology*, in *State of Mind – Il giornale delle scienze psicologiche*, 12 marzo 2021, consultabile online; C. GALANTE, *L'AI incontra la Psicologia: l'Intelligenza Artificiale Emotiva*, in *www.psicologinews.it*, 11 gennaio 2022, consultabile online. Il robot risuscitativo, dunque, potrebbe avere gli stessi effetti di uno psicologo, ma quest'ultimo – come figura umana – non potrà essere soppiantato totalmente, ma va considerato come strumento ausiliario finalizzato al raggiungimento di un benessere psicologico della persona umana che ha subito un trauma. Cfr., in chiave provocatoria, R. AVICO, *Un robot come psicologo? Intelligenza artificiale e chatbot, facciamo il punto*, in *www.psiche.it*, 4 luglio 2019, consultabile online, ove si legge, così come già detto dallo scrivente, che: “Esistono diversi studi che hanno valutato l'efficacia di un percorso di psicoterapia fatto tramite Bot. Allo stato attuale, la sensazione (perché di questo si tratta) che non si abbia a che fare con un individuo, e mancando quindi in pieno l'aspetto relazionale e affettivo, rende lo strumento utile, ma non del tutto efficace o risolutivo se si ragiona in termini di trattamento o cura di un determinato disturbo. Lo psicoterapeuta virtuale, per lo stato attuale delle cose, non riesce a sostituire un terapeuta umano formato, ponendosi più realisticamente come supporto integrativo in grado di assolvere a funzioni minori (come il triage iniziale di un paziente, il fornire reperibilità costante, avere un costo nullo, l'indirizzamento su una pagina internet a un giusto recapito), nell'ambito dell'erogazione di servizi di supporto alla salute mentale”.

²⁹ In tal senso, come già detto, si rinvia nuovamente a R. TREZZA, *I diritti della persona tra “tecniche” e “intelligenze” artificiali*, cit., p. 27.

dunque, la necro-robotica dovrà essere sempre più necro-etica³⁰.

2. Tecniche neuro-scientifiche e *privacy* neuronale.

Un ulteriore aspetto dell'I.A. è quello relativo alle nuove dimensioni della scienza neurologica e cognitiva³¹. Molti sono gli strumenti intelligenti che consentono di migliorare la salute neurologica della persona umana³² (e per ciò stesso sono meritevoli di essere costruiti, sempre improntati a variabili “salutari” e di essere utilizzati) e di prevedere comportamenti, specie criminali³³. O, ancora, molta è l'attenzione verso l'utilizzo delle tecniche neuro-scientifiche nel campo del *marketing*³⁴ che porta con sé non pochi risvolti sulla tutela dell'utente-consumatore³⁵. Per non parlare del rapporto che intercorre tra le neuroscienze e

³⁰ In tali termini, S. AMATO, *Biodiritto 4.0.*, cit., pp. 172-179, ove si mette in collegamento la necro-etica con la bioetica.

³¹ Su tale aspetto, si rinvia a L. PALAZZANI, R. ZANNOTTI, *Il diritto nelle neuroscienze. Non «siamo» i nostri cervelli*, Torino, 2013; N. LETTIERI, S. FARO, E. FABIANI, *Diritto, neuroscienze, scienze della cognizione*, Napoli, 2015; A. SANTOSUOSSO, *Le neuroscienze e il diritto*, Milano, 2009; C. GRANDI, *Neuroscienze e responsabilità penale. Nuove soluzioni per problemi antichi?*, Torino, 2016; V. ZAMBRANO, *Le neuroscienze, la capacità e la radiografia della macchina del pensiero*, in *Comp. dir. civ.*, 2018, pp. 1-27; O. DI GIOVINE, *Ripensare il diritto penale attraverso le (neuro-)scienze?*, Torino, 2019; R. TREZZA, *Los tratamientos neurocientíficos en detenidos: perfil civilista del consentimiento a las técnicas*, in E. QUARTA, *Dalla lectio magistralis del Ministro della Giustizia Marta Cartabia agli indici di rifrazione della metamorfosi della pena. Dal paradigma punitivo delle Erinni al paradigma riconciliativo delle Eumenidi. Lo sguardo nuovo sul sistema penitenziario nei dialoghi dei giuristi tra Italia, Perù e Cuba*, Roma, 2021. Per una differenza tra “scienza giuridica” e “scienza cognitiva”, si consenta rinviare a R. TREZZA, *Diritto e intelligenza artificiale*, cit., p. 100 ss.; P. PERLINGIERI, *Note in tema di “potenziamento cognitivo”*, cit., p. 216, ove l'A., in maniera del tutto condivisibile, si esprime in questi termini: “Il giurista ha il compito di contribuire a realizzarla (la dignità della persona), proponendo soluzioni adeguate”.

³² In tema, L. TAFARO, *Neuroscienze e diritto civile: nuove prospettive*, in *Rivista di biodiritto*, n. 3/2017, specie p. 257, la quale pone in evidenza: “Il riflesso delle neuroscienze nello specchio del diritto civile si coglie anzitutto con riferimento alla scoperta dei cc.dd. neuroni-specchio, quei particolari neuroni che, com'è noto, sono in grado di indurre istintivamente, nella interazione con gli altri, partecipazione empatica e comportamenti imitativi. Per essa occorre domandarsi se l'uso delle conoscenze neuroscientifiche relative al loro funzionamento possa profilare nuove aggressioni e, di conseguenza, nuovi bisogni di tutela della persona umana”.

³³ Sul punto, si rinvia a D. ONORI, A. R. VITALE, *Neuroscienze e diritto: quale sorte per la libertà?*, in *Centro studio Livatino*, 15 marzo 2021, consultabile online; M. DI FLORIO, *Colpevolezza, conseguenze sanzionatorie e neuroscienze in rapporto al diritto penale*, Pisa, 2021.

³⁴ Sul c.d. “neuromarketing”, si rinvia a L. TAFARO, *Neuromarketing e tutela del consenso*, Napoli, 2018, specie p. 64 ss., con recensione di R. PICARO, in *Tecnologie e diritto*, n. 1/2020, p. 378, il quale evidenzia che: “l'utilizzo delle tecniche di *neuromarketing* nella contrattazione interferisce con la libera formazione della volontà del consumatore, condizionandone la libertà economica e contrattuale” così andandosi ad innestare “nei processi decisionali, inducendo i contraenti a compiere scelte di consumo suggerite dall'uso strumentale della conoscenza delle loro preferenze ed abitudini di vita, ossia dati concernenti il nucleo della sua identità e della personalità stessa del consumatore”. Ancor prima, si veda F. VINCENZI, *Neuromarketing e web: un connubio legale?*, in *Cyberspazio e diritto*, n. 3/2017, p. 615 ss.; R. CATALANO, *Neuromarketing e tutela civile dei dati personali biometrici*, in *Comp. dir. civ.*, 2019, pp. 1-18.

³⁵ Su tale aspetto, tra i primi, si rinvia a M. IMBRENDA, *Persona e scelte di consumo tra conoscenze neuroscientifiche e nuove frontiere tecnologiche*, in *Actualidad Jurídica Iberoamericana*, n. 14/2021, p. 833, ove l'A. evidenzia che: “L'infrastruttura digitale si disvela essere il tramite di un percorso emancipatorio del “consumatore” che, oltre ad agire sul mercato in veste di arbitro (si pensi alle potenzialità offerte dalla *blockchain* per monitorare il processo produttivo e quindi orientare le proprie scelte di consumo sulla base delle informazioni e dei riscontri acquisiti), approda al ruolo ibrido di “prosumer”, tramutandosi in un vero e proprio attore economico. Dinanzi a questo complesso scenario, fatto di luci ed ombre, diviene ancora più stringente l'invito, rivolto a suo tempo all'interprete – compito primario del quale è l'identificazione e la tutela delle posizioni di libertà civili ed economiche della persona –, a non rifugiarsi nell'astrazione per impegnarsi nella definizione di nuove tecniche di attuazione e concretizzazione dei principi”. Da ultimo, interessante è la riflessione che propone A. MENDOLA, *Atto di consumo e libertà di scelta nel social media marketing*, in *Rivista di diritto privato*, 2022, specie p. 29, la quale propone di utilizzare la categoria della nullità di protezione qualora un consumatore-utente venga “frodato” (*rectius* dolo negoziale) in rete e, dunque, violata

la capacità umana³⁶.

Dal punto di vista del processo penale, invece, le neuroscienze potrebbero essere in grado di far capire il motivo per il quale una persona abbia commesso un fatto-reato o, in un'ottica preventiva, quando potrà e se potrà nuovamente compiere lo stesso fatto (recidiva)³⁷.

A tal proposito, è scontato riferirsi alle tradizionali teorie lombrosiane per mezzo delle quali, attraverso l'analisi cerebrale dei criminali, si poteva individuare la conformazione fisiologica di "inclinazione" alla commissione dei crimini. Un simile studio è descritto come "determinismo biologico"³⁸.

Non va affatto sottaciuto, però, che oltre ad un determinismo fisiologico, svariate altre possano essere le variabili o le circostanze che spingono a commettere dei reati, ovvero il fattore sociale (c.d. determinismo sociologico), il fattore economico (c.d. determinismo economicistico), il fattore psicologico (c.d. determinismo psicologico o "psicologismo"), il fattore tecnologico³⁹. In tale ultima prospettiva, proprio perché vi è il rischio di perpetrazione di reati anche nella realtà liquida della rete⁴⁰ (*deep web*⁴¹, *cybercrime*⁴² e così via), si potrebbe parlare di un nuovo tipo di determinismo, ovvero quello "tecnologico".

L'elemento che qui maggiormente interessa è il seguente: il portato finale degli esperimenti, ovvero tutti i dati neuronali raccolti, che tutela possiede?

I "dati neuronali" rientrano sicuramente nella categoria dei dati sensibili e vanno trattati secondo la disciplina del nuovo GDPR in tema di protezione dei dati personali⁴³. Per ciò stesso si dovrebbe iniziare anche a disquisire di "privacy

sarebbe la sfera della sua libertà di scelta. L'A. mette anche in luce le teorie avverse, quelle enucleabili l'applicabilità della disciplina della annullabilità al caso prospettato. In realtà, sul punto, non può che rilevarsi la lungimiranza nelle argomentazioni di G. PERLINGIERI, *L'inesistenza della distinzione tra regole di comportamento e di validità nel sistema italo-europeo*, Napoli, 2013, p. 93 ss., ove l'A. avverte che: "il contratto sia viziato funzionalmente, ossia nullo per una condotta illecita che, in un rapporto causa-effetto, è risultata capace di colorare il regolamento di interessi"; R. PICARO, *Relazioni consumeristiche, intelligenza artificiale e nuove identità*, in *Rass. dir. civ.*, n. 4/2020, p. 1485 ss. Ancora, proprio di recente, si rinvia a L. CARRUBBO, A. MENDOLA, *Le scelte "inconsapevoli" nelle nuove dinamiche d'acquisto. Il neuromarketing e la tutela del consumatore-follower*, Padova, 2022.

³⁶ Sul punto, si rinvia, tra tutti, a E. LECCESE, *Capacità e neuroscienze cognitive: un dialogo con il Prof. Stanzone*, in *Comp. dir. civ.*, n. 3/2020, p. 87 ss.

³⁷ Si veda A. FORZA, *Neuroscienze e diritto*, in *Rivista penale*, n. 3/2009, p. 253; P. PIETRINI, *La macchina della verità alla luce delle recenti acquisizioni delle neuroscienze*, in *Cassazione penale*, 2008, p. 141 ss.

³⁸ Sul punto, tra tanti, si veda P. MARTUCCI, *All'inizio era il male: determinismo biologico e destino nella criminologia di Cesare Lombroso*, in *Rassegna italiana di criminologia*, n. 1/2013, p. 52 ss.

³⁹ Sui vari tipi di "determinismo", si rinvia, da ultimo, per un approfondimento attualizzante, a G. BRACCILI, *Teorie bio-antropologiche nel XIX secolo: la scuola positiva di Cesare Lombroso, Enrico Ferri e Raffaele Garofalo*, in *Scienze criminologiche*, 21 marzo 2021, consultabile online.

⁴⁰ Mutuando l'espressione dal grande Z. BAUMAN, *Modernità liquida*, Roma-Bari, 1999.

⁴¹ Sul *deep web*, tra tanti, si rinvia a R. MEGGIATO, *Il lato oscuro della Rete: Alla scoperta del Deep Web e del Bitcoin*, Adria, 2014; M. FACCIOI, *Minori nella rete. Pedofilia, pedopornografia, deep web, social network, sexting, gambling, grooming e cyberbullismo nell'era digitale*, Roma, 2015; L. VARRIALE, *La prigione dell'umanità. Dal deep web al 4.0, le nuove carceri digitali*, Bologna, 2017; G. MALATO, *Deep web*, Forlì, 2019; E. FLORINDI, *Deep web. Vizi privati e pubbliche virtù della navigazione in rete*, Torino, 2020.

⁴² Sul tema, si rinvia a A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, Milano, 2019; E. BASSOLI (a cura di), *I crimini informatici, il dark web e web room*, Pisa, 2021. Da un punto di vista rimediario, si rinvia a J. KULESZA, F. DELERUE, *Cybersecurity in the Year of the Plague: Due Diligence as a Remedy to Malicious Activities*, in *Tecnologie e diritto*, n. 2/2020, p. 404 ss.; A. ROTONDO, *Prevenzione e contrasto della minaccia informatica in Europa: note a margine del Regolamento (UE) 2019/881*, in *Tecnologie e diritto*, n. 1/2020, p. 195 ss.

⁴³ Tale è la sollecitazione proveniente da P. PERLINGIERI, *Note in tema di "potenziamento cognitivo"*, cit., specie p. 214.

neuronale⁴⁴". Inoltre, è possibile donare, anche *post mortem*, tali dati alla scienza per finalità di ricerca (appunto) scientifica⁴⁵?

3. Il diritto civile "algoritmico": eredità digitale e circolazione dei dati personali *post mortem*.

L'I.A. ha investito, con le sue innovazioni e le sue tecniche, tutti i settori del diritto. Per i fini che qui interessano, è d'uopo soffermarsi, seppur in maniera schematica, sul rapporto tra I.A. e diritto civile⁴⁶, prendendo in esame, tra

⁴⁴ Questa espressione viene utilizzata da S. AMATO, *Biodiritto 4.0.*, cit., p. 122. In tal senso, però, si legga anche l'intervento del Presidente dell'Autorità Garante della privacy, prof. Pasquale Stanzone, del gennaio 2021, il quale ha sottolineato che, oltre all'*habeas corpus* e all'*habeas data*, vi sia anche l'*habeas mentem* a cui apprestare tutela. In sintonia anche M. IMBRENDA, *Nuove tecnologie e dinamiche regolatorie dell'autonomia privata*, in R. M. AGOSTINO, G. DALIA, M. IMBRENDA, S. PIETROPAOLI (a cura di), *Frontiere digitali del diritto*, cit., p. 112 ss.

⁴⁵ Sembra che una risposta a tale interrogativo possa essere affermativa, specie prendendo in considerazione la nuova Legge n. 10/2020 "*Norme in materia di disposizione del proprio corpo e dei tessuti post mortem a fini di studio, di formazione e di ricerca scientifica*", la quale, all'art. 3, prevede l'obbligo informativo, il consenso informato, la possibilità di nomina di un "fiduciario" e la revocabilità del consenso *in extremis* – essendo un diritto fondamentale della persona umana –. Cfr., sul punto, R. TREZZA, *La revocabilità per facta concludentia del consenso all'anonimato e il diritto a conoscere le proprie origini "in espansione"*, in *Nomos – Le attualità nel diritto*, n. 1/2021, pp. 1-12; ID., *La fecondazione omologa post matrimonio: l'embrione crioconservato è "concepito"?*, cit., ove si evidenzia che il consenso all'impianto può essere revocato sino a quando l'embrione artificiale non venga impiantato nell'utero materno. In accordo con lo scrivente, anche G. GIAIMO, *Frozen embryos, frozen law. Brevi notazioni, in chiave comparatistica, su di una recente decisione in tema di procreazione medicalmente assistita*, in *Dir. fam. pers.*, n. 3/2021, p. 1331 ss.). Sulla Legge suddetta, che è passata in sordina per molti perché pubblicata in un tempo problematico quale quello epidemico, si veda M. TOMASI, *L. 10/2020: disposizione del proprio corpo a fini di ricerca scientifica*, in *Rivista di biodiritto*, 4 marzo 2020, consultabile online; L. ATZENI, *Brevi note a margine della legge 10 febbraio 2020, n. 10 in tema di disposizione del proprio corpo e dei tessuti post mortem a fini di studio, di formazione e di ricerca scientifica*, in *Rivista AIC*, n. 5/2020, specie p. 67, ove l'A. afferma che: "D'altra parte, al fine di rendere effettivo il diritto al rispetto delle proprie volontà espresse in vita, e, al contempo, al fine di garantire il diritto alla riservatezza, è fondamentale che, in conformità con l'articolo 9 del Decreto del Ministero della Salute del 18 dicembre 2019, quest'ultimo Ministero svolga una costante attività di monitoraggio volta a verificare l'idoneità della regolamentazione della banca dati nazionale destinata alla registrazione delle DAT, nonché il suo puntuale aggiornamento. Infatti, solamente nel caso in cui il diritto all'autodeterminazione fisica e il diritto all'autodeterminazione informativa del disponente vengano contestualmente garantiti, si potrà rendere effettiva la tutela della libertà e della dignità della persona umana"; M. GHIONE, *Luci e ombre della l. n. 10/2020 in materia di disposizione del proprio corpo e dei tessuti post mortem*, in *Famiglia*, n. 4/2020; R. MASONI, *In G.U. disposizioni del proprio corpo post mortem*, in *Il familiarista*, 11 marzo 2020, consultabile online; G. GIAIMO, *Il lascito del proprio corpo a fini didattici e di ricerca. Il nobile (ma vano) intento della legge 10/2020*, in *Rivista di biodiritto*, n. 2/2021, specie p. 190, ove, in chiave critico-legislativa, si afferma che: "Ancora una volta, allora, la legge n. 10/2020 dimostra le sue evidenti insufficienze alle quali occorre rimediare in via di interpretazione, sempre in attesa del regolamento attuativo che, finalmente, ne consentirà l'effettiva applicazione. Ciò che resta, tuttavia, è un sentore di irrisolutezza, dovuto a un legislatore rimasto a metà del guado tra quei provvedimenti che hanno ispirato il suo agire (la normativa in materia di trapianti e quella relativa alle disposizioni anticipate di trattamento) e incapace di prevedere quei semplici accorgimenti che avrebbero potuto condurre a una disciplina capace di ambire a farsi modello per gli altri ordinamenti ma che, invece, ha il gusto insipido delle occasioni non colte".

⁴⁶ Sul punto, si consenta rinviare a R. TREZZA, *Artificial intelligence, civil law and ethics in Italy: a possible interaction*, in *Cultura giuridica e diritto vivente*, n. 9/2021, p. 12. Inoltre, non si può, sul punto, non rinviare a E. CATERINI, *L'intelligenza artificiale «sostenibile» e il processo di socializzazione del diritto civile*, Napoli, 2020, specie p. 32, ove si legge che: "Il processo di soggettivazione dell'intelligenza artificiale, generato dalla capacità regolativa che è propria dell'autonomia dei privati, tanto nel perseguimento di interessi generali che particolari, unitamente alla connessione di essa con la dignità dell'uomo, avviano senza esitazioni gli autori algoritmici e gli attanti macchinici verso un processo di responsabilizzazione. Non è soltanto una responsabilità civile ma anche sociale che induce ad impedire che l'AI divenga causa di aggravamento delle differenze piuttosto che veicolo di eguaglianza. L'interprete di ogni angolo della galassia giuridica deve assumere una posizione coerente con la legge fondamentale della Repubblica e ogni ritrovato

tantissime questioni, quelle che si reputano essere più interessanti, ovvero il caso degli *smart contracts*⁴⁷, della determinazione algoritmica dell'oggetto del contratto⁴⁸ e dell'eredità digitale⁴⁹, oltre a quello già tanto discusso della "soggettività giuridica dei *software*"⁵⁰, su cui, per ragioni di sistema, non ci si

della scienza non deve sottrarsi al primato del diritto come strumento per la costruzione di una società giusta. La lenezza dell'interprete, brandita come inno alla libertà, spesso malcelata la scelta ideologica di chi vuole far prevalere la giustizia della forza (economica o tecnica) piuttosto che la forza della giustizia. Le Costituzioni contengono delle "ideologie reali", ideologie, perché portatrici della speranza di un progetto ideale, reali, perché munite della precettività della norma giuridica. Gli interpreti e applicatori devono avere la consapevolezza della responsabilità di non disattendere la speranza di un'ideologia imperativa. Anche l'umanità automata deve assolvere alla funzione sociale di consentire e agevolare l'"accessibilità a tutti" di quelle applicazioni dell'intelligenza artificiale che garantiscono il "minimo vitale". Altrimenti, se è possibile che il leone e il vitello giacciono insieme, è pur vero che il vitello dormirà poco".

⁴⁷ Si faccia riferimento a D. DI SABATO, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto e impresa*, n. 2/2017, p. 378; S. COMELLINI, M. VASAPOLLO, *Blockchain, criptovalute, I.C.O. smart contracts*, Santarcangelo di Romagna, 2019; A. CONTALDO, F. CAMPORA, *Blockchain, criptovalute, smart contract*, industria 4.0, Pisa, 2019; G. GALLONE, *La pubblica amministrazione alla prova dell'automazione contrattuale. Note in tema di smart contracts*, in *Federalismi*, n. 20/2020, pp. 142-170; A. STAZI, *Automazione contrattuale e "contratti intelligenti". Gli smart contracts nel diritto comparato*, Torino, 2019; A. STAZI, *Automazione contrattuale e "contratti intelligenti". Gli smart contracts nel diritto comparato*, Torino, 2019; T. PELLEGRINI, *Prestazioni auto-esecutive. Smart contract e dintorni*, in *Comp. dir. civ.*, n. 3/2019, p. 843 ss.; A. DAVOLA, *"Blockchain" e "Smart Contract as a Service" (SCaaS): prospettive di mercato a criticità normative delle prestazioni BaaS e SCaaS alla luce di un'incerta qualificazione giuridica*, Relazione al Convegno "La grande innovazione e le sue regole: Intelligenza artificiale, Data analysis, Tecnologia blockchain", Parma, 25 ottobre 2019, in *Il Diritto industriale*, n. 2/2020, pp. 147-156; I. FERLITO, "Smart contract". *Automazione contrattuale ed etica dell'algoritmo*, in *Comp. dir. civ.*, n. 2/2020, p. 661 ss.; F. BRUSCHI, *Le applicazioni delle nuove tecnologie: criptovalute, "blockchain" e "smart contract"*, Relazione al Convegno "La grande innovazione e le sue regole: Intelligenza artificiale, Data analysis, Tecnologia blockchain", Parma, 25 ottobre 2019, in *Il Diritto industriale*, n. 2/2020, pp. 162-164; C. PERNICE, *Distributed ledger technology, blockchain e smart contracts: prime regolazioni*, in *Tecnologie e diritto*, n. 2/2020, p. 490 ss.; M. GIACCAGLIA, *Il contratto del futuro? Brevi riflessioni sullo smart contract e sulla perdurante vitalità delle categorie giuridiche attuali e delle norme vigenti del Codice civile italiano*, in *Tecnologie e diritto*, n. 1/2021, p. 113 ss. Ancora più di recente, si veda F. GAMBINO, *Blockchain, smart contract e diritto sradicato*, in *Tecnologie e diritto*, n. 2/2021, p. 29 ss.; J. FORTUNA, *Smart contract e formazione del contratto: un'analisi comparatistica della nascita del vincolo giuridico*, in *Comp. dir. civ.*, n. 2/2021, p. 595 ss.

⁴⁸ Sul punto, si veda M. D'AMBROSIO, *Arbitraggio e determinazione algoritmica dell'oggetto*, Napoli, 2020.

⁴⁹ Si faccia riferimento alla pronuncia del Tribunale di Milano del 9 febbraio 2021, in *Diritto di Internet*, 10 febbraio 2021, consultabile online. Sul punto, alcune riflessioni, sono state proposte da I. MARTONE, *Sulla trasmissione a causa di morte del "patrimonio digitale"*, cit., p. 420 ss.; R. BERTI, S. ZANETTI, *L'eredità digitale tra norma e tecnologia: come le big tech stanno risolvendo un problema giuridico con strumenti informatici*, in *Media Laws*, 29 luglio 2021, consultabile online, ove si legge, condivisibilmente, che: "La situazione attuale vede quindi un acceso conflitto fra la dimensione giuridica, ancorata ai concetti di contenuto economico, diritti morali degli eredi e riservatezza dei defunti, e dimensione tecnologica, che traduce la dimensione contrattuale in un rapporto ritagliato sul singolo utente, violato dalla condivisione delle credenziali salvo questa sia "incanalata" nelle procedure eventualmente messe a disposizione dal fornitore del servizio/dispositivo per trasmettere a terzi il servizio/dispositivo stesso. All'aumentare dell'importanza materiale e morale dei valori inseriti in queste piattaforme/servizi sorgono dei conflitti, gestiti in sede giudiziale solamente perché la tecnologia non ha, ad oggi, per interessi propri o disinteresse verso questo tema delicato, saputo fornire soluzioni adeguate al problema. Dal canto suo nemmeno il diritto è in grado di fornire soluzioni appaganti in quanto è di tutta evidenza che al giudice è richiesta una difficile valutazione di bilanciamento da effettuare caso per caso fra il diritto dei parenti ad accedere ai dati ed al patrimonio ereditario del defunto e il diritto alla riservatezza del defunto stesso, che verosimilmente avrebbe voluto escludere da questa condivisione almeno una parte dei contenuti dallo stesso privatamente condivisi in vita"; A. D'ARMINIO MONFORTE, *La successione nel patrimonio digitale*, Pisa, 2020. Di recente, sulla stessa lunghezza d'onda, anche il Tribunale di Roma, con ordinanza del 10 febbraio 2022, con la quale si è ordinato alla società Apple di prestare assistenza alla ricorrente per il recupero dei dati dell'*account*, anche mediante consegna delle credenziali di accesso, sulla base dell'art. 2 terdecies del d.lgs. 101/2018.

⁵⁰ Si rimanda, per un approfondimento, a G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto*, in *Contratti e impresa*, 2022, II, p. 456 ss.; C. PERLINGIERI, *L'incidenza dell'utilizzazione della tecnologia robotica nei rapporti civilistici*, in *Rassegna di diritto civile*, 2015, p. 1235 ss.; G. TEUBNER, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, a cura di P. Femia, Napoli, 2019; E. MOROTTI, *Una soggettività a geometrie variabili per lo statuto giuridico dei robot*, in F. BILOTTA, F. RAIMONDI (a cura di),

sofferma.

La determinazione algoritmica degli interessi delle parti⁵¹, attraverso un coacervo di interessi telematici fatti percepire al *software*, fa sì che si possa parlare di “autonomia contrattuale elettronica”⁵², ove, a maggior ragione, gli interessi delle parti, così come già accade ai sensi dell’art. 1322 c.c.⁵³, dovranno oltrepassare la scure del vaglio di meritevolezza⁵⁴. Un simile contratto, però, potrebbe generare “ontologicamente” o “successivamente” uno squilibrio del sinallagma che si ripercuote sul rapporto contrattuale⁵⁵ e, di conseguenza, sul fascio di situazioni giuridiche (sia esistenziali sia patrimoniali) appartenenti alla persona-contraente⁵⁶. Va evitata, quindi, un’“asimmetria” algoritmica⁵⁷ ed

Il soggetto di diritto. Storia ed evoluzione di un concetto nel diritto privato, Napoli, 2020; U. RUFFOLO, *Il problema della “personalità elettronica”*, in *Journal of Ethics and Legal Technologies*, n. 2/2020, p. 87, ove si pone in luce: “Dobbiamo, proattivamente, allora, porci già il problema del che fare, e come “trattare” la creazione - poco importa, ai nostri fini, quanto illecita - di entità “intelligenti”, e magari emotive e senzienti, di tipo diverso dal nostro. Da che momento - se si vuole, da quale grado di intelligenza - esse diventano insopprimibili e tutelabili, o comunque “disciplinabili”? È severamente vietata sia la clonazione sia la creazione di chimere (v. legge n. 40/2004, art. 13). Ma, qualora tali pratiche ricevessero - poco importa quanto illecita - attuazione, gli “esseri” così venuti al mondo sarebbero entità comunque “viventi” (qualsiasi cosa questo voglia dire). Come andrebbero trattati e classificati? Quale *status* e tutela (e libertà, e diritti) potrebbero/dovrebbero essere loro attribuiti? I “diritti umani”, se considerati come universo esaustivo, sono ormai troppo antropocentrici?”.

⁵¹ In merito, si rinvia a M. DE FELICE, *Decisione robotica negoziale. Nuovi “punti di presa” sul futuro*, in A. CARLEO (a cura di), *Decisione robotica*, cit., p. 179 ss. Nello stesso volume, ancora, F. DE STEFANO, *Spunti di riflessione sulla decisione robotica negoziale*, p. 215 ss.; G. GITTI, *La decisione robotica negoziale*, p. 251 ss.

⁵² Sul punto, si rinvia alla lettura di S. ACETO DI CAPRIGLIA, *Contrattazione algoritmica. Problemi di profilazione e prospettive operazionali. L’esperienza “pilota” statunitense*, in *Federalismi*, n. 18/2019, specie p. 60, ove l’A. conclude in tal modo: “È possibile ed è consigliabile, però, offrire agli interpreti criteri ermeneutici dedotti dai principi generali e dalle esperienze straniere più avanzate che (a prescindere dal mutamento dei tempi e della tecnica), sono destinati a costituire il faro che illumina la buia foresta delle molteplici forme di negoziazione digitale. All’uopo, quest’ultima risulta certamente uno strumento utile, ma è necessario che venga presa in considerazione dal legislatore eurounitario oltre che da quello domestico, e che sia circondata da apposite tutele e accorgimenti. Tali cautele normative dovranno essere attentamente predisposte affinché il dominio negli algoritmi non si trasformi, in ultima analisi, nell’abuso da parte di soggetti tecnologicamente più avanzati e quindi dotati di competenze tali da tiranneggiare il *quavis de populo*, oggi più che mai esposto al rischio di sfruttamenti e raggiunti sul piano consumeristico”.

⁵³ Sul punto, in merito alle dinamiche dell’autonomia negoziale, si rinvia a F. CRISCUOLO, *Autonomia negoziale e autonomia contrattuale*, Napoli, 2008, p. 1 ss.; S. GIOVA, G. PERLINGIERI, L. TULLIO (a cura di), *Autonomia negoziale e successioni mortis causa*, Napoli, 2020; AA. VV., *L’autonomia negoziale nella giustizia arbitrale*, Napoli, 2016.

⁵⁴ Si consenta rinviare a R. TREZZA, *Il contratto nell’era del digitale e dell’intelligenza artificiale*, in *Il diritto dell’economia*, n. 2/2021, pp. 287-319.

⁵⁵ Si rinvia, anche in chiave comparatistica, a P. D’ELIA, *Digital relationships and private autonomy in the EU legal framework*, in *Comp. dir. civ.*, n. 2/2021, p. 629 ss. Inoltre, è meglio parlare di “rapporti negoziali”, laddove anche il negozio, qualora dovesse essere “trattato algorithmicamente”, dovrebbe avere le medesime cautele. Sul punto, E. PALMERINI, *Negoziato e automazione: appunti per una mappa concettuale*, in A. CARLEO (a cura di), *Decisione robotica*, cit., p. 291 ss.

⁵⁶ Sul punto, si rinvia a P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 715 ss.

⁵⁷ Su tale concetto, si rinvia a S. ORLANDO, *Gli smart contracts come prodotti software*, in S. ORLANDO, G. CAPALDO (a cura di), *Annuario 2021. Osservatorio Giuridico sulla Innovazione Digitale*, Roma, 2021, specie p. 252, ove l’A. differenzia l’asimmetria informativa da quella informatica: “L’asimmetria informatica, nel senso sopra delineato, è ben distinguibile dall’asimmetria informativa, perché mentre quest’ultima esprime la mancanza di conoscenza di informazioni rilevanti, secondo le circostanze, da parte di un contraente, a fronte della conoscenza delle medesime informazioni da parte di un altro contraente, l’asimmetria informatica, nel senso sopra inteso e riferito allo *smart contract*, esprime la mancanza di conoscenza da parte di un contraente del linguaggio nel quale un altro contraente pretenderebbe che fosse dichiarato il contenuto di un contratto, ossia il linguaggio in cui è espresso un programma per elaboratore. Per tale motivo, laddove anche il programma per elaboratore di uno *smart contract* venga reso accessibile in open source (ciò che anche negli ecosistemi *blockchain* dipende sempre da una precisa scelta del predisponente), non per questo solo potrà ritenersi che esso è stato reso conoscibile alla generalità dei

esperiti tutti i rimedi affinché questa possa cessare⁵⁸, così che il contratto possa davvero essere, alla luce delle umane vicissitudini, “intelligente⁵⁹”.

Inoltre, anche l'intenzione “comune” delle parti andrà valutata secondo una dimensione “elettronica⁶⁰”. L'interpretazione della legge in generale, e ancora del contratto, dovrà essere necessariamente conformata alle nuove regole algoritmiche⁶¹. Insomma, il diritto privato *tout court* inteso subisce una evoluzione continua, ma le regole civilistiche sembrano ben resistere⁶², specie nel fatto che

potenziali contraenti secondo l'ordinaria diligenza, essendo viceversa ostativa a questa conclusione la carenza di intelligibilità (qui non coincidente con la conoscibilità) del medesimo programma, a cagione dell'ignoranza del linguaggio nel quale esso è espresso”.

⁵⁸ Sul punto, tra tutti, si rinvia a A. FEDERICO, *Equilibrio e contrattazione algoritmica*, in *Rass. dir. civ.*, n. 2/2021, p. 483 ss. Un simile squilibrio, di per sé, si è verificato anche con l'evento pandemico. Sul punto, si rinvia a C. COSENTINO, *Eteronomia giudiziale e contratto diseguale*, in *Comp. dir. civ.*, pp. 1-20, consultabile online; A. S. M. ROSETI, *Il COVID-19 riaccende l'eterno conflitto tra il principio pacta sunt servanda e il principio rebus sic stantibus*, in *Il diritto del risparmio*, pp. 1-20, consultabile online; N. CIPRIANI, *L'impatto del lockdown da COVID-19 sui contratti*, in *Rivista di diritto bancario*, n. 4/2020, p. 652 ss.; C. PILIA, *Le tutele dei diritti durante la pandemia Covid 19: soluzioni emergenziali o riforme strutturali?*, in *Persona e Mercato*, n. 5/2020, p. 77 ss.; T. SICA, *Sopravvenienze contrattuali da Covid-19 e rapporti concessori. Scelta del rimedio e profili regolatori*, in *Osservatorio del diritto civile e commerciale*, n. 2/2021, p. 507 ss.; F. PIRAINO, *Contratto ed emergenza sanitaria in Italia*, in *Revista de Direito da Cidade*, n. 3/2021, p. 1531 ss.; M. FRANZONI, *El Covid 19 y la ejecución del contrato*, in *Revista cubana de derecho*, n. 2/2021, p. 247 ss.; C. MARCHETTI, *Pacta sunt servanda ai tempi del Covid-19*, in R. E. CERECCHIA (a cura di), *Percorsi di diritto comparato*, Milano, 2021, p. 57 ss.; O. CLARIZIA, *Coronavirus ed esonero da responsabilità per inadempimento di obbligazione ex art. 1218 c.c.: impossibilità sopravvenuta oppure inesigibilità della prestazione?*, in *Actualidad Jurídica Iberoamericana*, n. 12/2020, pp. 352-365; E. DAMIANI, *Le tutele civilistiche per i contratti iniqui stipulati a causa della diffusione del coronavirus*, in *Judicium*, 9 maggio 2020, consultabile online; V. DI CATALDO, *Pandemia, imprese e contratti di durata*, in *Osservatorio del diritto commerciale*, n. 3/2020, consultabile online; A. LESTINI, *La c.d. “clausola di irrisolvibilità”: tra sopravvenienze e rimedi contrattuali preventivi*, in *Ratio iuris*, 30 marzo 2021, consultabile online; A. FEDERICO, *Misure di contenimento della pandemia e rapporti contrattuali*, in *Actualidad Jurídica Iberoamericana*, n. 12bis/2020, pp. 236-249; G. CARAPEZZA FIGLIA, *Coronavirus e locazioni commerciali. Un diritto eccezionale per lo stato di emergenza?*, in *Actualidad Jurídica Iberoamericana*, n. 12bis/2020, pp. 422-433; E. TUCCARI, *Sopravvenienze e rimedi ai tempi del Covid-19*, in *Jus civile*, n. 2/2020, p. 465 ss.; V. ROPPO, R. NATOLI, *Contratto e Covid-19*, in *Giustizia insieme*, 28 aprile 2020, consultabile online; S. ACETO DI CAPRIGLIA, *Effetti del lockdown sui contratti di diritto privato. Un dialogo tra esperienze giuridiche*, in *Federalismi*, n. 3/2022, p. 1 ss.

⁵⁹ In tal senso, si veda V. BELLOMIA, *Il contratto intelligente: questioni di diritto civile*, in *Judicium*, 10 dicembre 2020, consultabile online, ove l'A. evidenzia che: “Emerge da questa breve panoramica che lo studio sulla compatibilità tra la *blockchain*, in particolare pubblica e *permissionless*, e la vigente *data protection law* è ampiamente e tuttora in corso, alla ricerca delle indispensabili soluzioni tecniche. Se queste ultime saranno trovate e si riveleranno efficaci e conformi alla legislazione vigente – la quale non è peraltro affatto escluso possa aggiornarsi nel prossimo futuro con espresso riferimento proprio a tali fenomeni ed alle irrisolte problematiche – il sistema potrà legittimamente e proficuamente trovare applicazione nell'ordinamento, anche da questo punto di vista”; A. M. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale: cinque questioni e due scenari*, in *Riv. dir. civ.*, n. 1/2021, p. 1 ss.; G. CASTELLANI, *Smart contracts e profili di diritto civile*, in *Comp. dir. civ.*, pp. 1-14 consultabile online; A. GALIANO, A. LEOGRANDE, S. F. MASSARI, A. MASSARO, *I processi automatici di decisione: profili critici sui modelli di analisi e impatti nella relazione con i diritti individuali*, in *Rivista italiana di informatica e diritto*, n. 2/2019, p. 41 ss.; M. CRISAFULLI, *L'era degli Smart Contracts: potenzialità e limiti di uno strumento rivoluzionario*, in *Diritto Mercato Tecnologia*, n. 3/2021, p. 1 ss.

⁶⁰ Ciò spiega il motivo per il quale anche l'interpretazione della norma in generale, e più specificamente l'interpretazione del contratto, siano costrette a subire una modifica. In tal senso, per un adeguamento interpretativo, si legga, E. DAMIANI, *Trasformazione digitale ed evoluzione dell'interpretazione giuridica*, in *Tecnologie e diritto*, n. 2/2021, p. 13 ss.

⁶¹ Sul punto, si rinvia a P. PERLINGIERI, *Struttura algoritmica e interpretazione*, in *Tecnologie e diritto*, n. 2/2020, p. 484 ss.

⁶² In tal senso, si veda C. PERLINGIERI, *Diritto privato delle nuove tecnologie*, in *Tecnologie e diritto*, n. 2/2021, p. 71, la quale pone in evidenza che: “(...) alla luce di queste considerazioni necessario è il tentativo di riflessione sull'attuale ruolo del civilista seriamente minacciato dal dominio tecnologico (...), ma la tempo stesso fortemente convinto di volere salvaguardare il diritto nel suo essere umano al fine di impedire la

il contratto debba realizzare (e, in questa dimensione, va letto e interpretato) sempre e comunque i diritti della persona⁶³.

La determinazione algoritmica, invece, dell'oggetto del contratto è consentita per le stesse ragioni poc'anzi esposte. Tutto ciò che è mero procedimento potrebbe essere sostituito dalla macchina. Una valutazione standardizzata, ad esempio, potrebbe essere facilmente rimpiazzata da un *software*⁶⁴.

Tema interessante, che sta emergendo sempre con più forza, è quello relativo all'eredità digitale. Tutto ciò che una persona lascia disseminato in rete, sui *social networks*, sulle piattaforme *online*⁶⁵ e così via, dopo la sua morte, che tutela

formazione di un diritto nuovo e diversamente declinato dall'applicazione delle procedure algoritmiche frutto del solo pensiero calcolante".

⁶³ Si veda, proprio in tal senso, L. VALLE, *Il contratto e la realizzazione dei diritti della persona*, Torino, 2020, specie p. 7, ove l'A. ben mette in evidenza che: "Questa separazione tra diversi ambiti dell'ordinamento giuridico, del diritto contrattuale rispetto a quello dei diritti della persona, che si è associata alla distinzione tra la regolazione della sfera delle situazioni e dei rapporti giuridici patrimoniali rispetto quella delle situazioni e dei rapporti non patrimoniali, appare oggi non più attuale alla luce del concorso di più fattori". In completo accordo si trova la visione, sempre attuale, di P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 715, ove si criticano i c.dd. "diritti della personalità". Questa è la logica per la quale si legge l'art. 2059 c.c. in ottica costituzionalmente orientata, come una clausola aperta, esattamente come l'art. 2 Cost.

⁶⁴ Si pensi all'adozione di un decreto ingiuntivo in ambito processuale civile, ove al giudice spetta solo la valutazione della sussistenza dei presupposti di legge ex art. 633 ss. c.p.c. Si pensi, ancora, sempre in ambito processuale, alla valutazione dei presupposti per la declaratoria di inammissibilità dei ricorsi (artt. 348bis e 360bis c.p.c.). In tal caso, con delle banche date di tracciamento, potrebbe essere semplice uno snellimento accelerato del processo, anche per perseguire ragioni di economicità e durata ragionevole del processo. In tal senso, infatti, ovvero nel rapporto tra processo e I.A., bisogna che sia raggiunto sempre il rispetto di tutti i valori contenuti nell'art. 111 Cost., tanto che si potrebbe parlare di un "giusto processo elettronico". Su tale aspetto, anche in un'ottica di abbattimento del contenzioso, si rinvia a A. CARLEO, *Sugli algoritmi nel contratto? per ridurre il contenzioso?*, in ID. (a cura di), *Decisione robotica*, cit., p. 203 ss.

⁶⁵ A proposito delle piattaforme, altro tassello necessario è l'individuazione di un "responsabile" qualora i contenuti "presentati", "immessi" o "ospitati" sulle stesse cagionino dei danni patrimoniali o non patrimoniali alla persona umana. Nell'ambito dei servizi della società dell'informazione, la responsabilità dell'*hosting provider*, prevista dall'art. 16, d.lgs. 9 aprile 2003, n. 70, sussiste in capo al prestatore di servizi che non abbia provveduto alla immediata rimozione dei contenuti illeciti, nonché se abbia continuato a pubblicarli, pur quando ricorrano congiuntamente le seguenti condizioni: a) sia a conoscenza legale dell'illecito perpetrato dal destinatario del servizio, per averne avuto notizia dal titolare del diritto leso oppure *aliunde*; b) l'illiceità dell'altrui condotta sia ragionevolmente constatabile, onde questi sia in colpa grave per non averla positivamente riscontrata, alla stregua del grado di diligenza che è ragionevole attendersi da un operatore professionale della rete in un determinato momento storico; c) abbia la possibilità di attivarsi utilmente, in quanto reso edotto in modo sufficientemente specifico dei contenuti illecitamente immessi da rimuovere. Sulla c.d. "responsabilità civile dell'*hosting provider*" (pur in mancanza di un obbligo generale di sorveglianza, gli *internet service provider* rispondono civilmente del contenuto dei servizi se, richiesti dall'autorità giudiziaria o amministrativa, non agiscano prontamente per impedire l'accesso al contenuto di tali servizi), si rinvia a C. D'URSO, *I profili informatici nella valutazione della responsabilità dell'*Hosting Provider**, in *Rivista italiana di informatica e diritto*, n. 1/2021, p. 79 ss.; A. LA ROSA, *I profili di responsabilità di Amazon in quanto hosting attivo*, in *Diritto di internet*, 7 aprile 2021, consultabile online; R. COSIO, *La responsabilità del prestatore di servizi di hosting*, in *Jus civile*, n. 4/2020, p. 887 ss.; G. D'ALFONSO, *Verso una maggiore responsabilizzazione dell'*hosting provider* tra interpretazione evolutiva della disciplina vigente, innovazioni legislative e prospettive de jure condendo*, in *Federalismi*, n. 2/2020, p. 108 ss.; S. SICA, *Giurisprudenza nazionale ed europea e frammentazione legislativa della responsabilità civile del provider*, in *Comp. dir. civ.*, n. 2/2019, p. 353 ss.; M. D'AMBROSIO, *Tutela dei diritti della personalità nella rete: ruolo del provider nella fruizione dei servizi online e (a) territorialità dell'ingiunzione di rimozione dei contenuti illeciti*, in *Tecnologie e diritto*, n. 2/2020, p. 582 ss.; M. FOTI, *Contraffazione online: il ruolo degli Internet Service Providers nell'uso illecito del marchio altrui*, in *Tecnologie e diritto*, n. 2/2020, p. 604 ss.; M. BELLÌ, *Sui presupposti e sui limiti della tutela esperibile nei confronti dell'*internet service provider* (hosting e caching) la Cassazione tenta di fare chiarezza*, in *Tecnologie e diritto*, n. 1/2020, p. 299 ss. Si veda, ancora, E. TOSI, *Responsabilità civile degli hosting provider e inibitoria giudiziale dei contenuti digitali illeciti equivalenti tra assenza dell'obbligo di sorveglianza ex ante e ammissibilità ex post*, in *Il diritto degli affari*, n. 1/2020, p.p. 23-24, ove l'A. evidenzia che: "Non si tratta, infatti, di imporre giudizialmente un obbligo generale ex ante – vietato, come si è rilevato *supra*, dall'art. 17 del D.lgs. 70/2003 – quanto, invece, di un obbligo particolare – circostanziato – di prevenzione o rimozione di nuove violazioni, ormai prevedibili, relativamente

avrà?

Si pensi, per esempio, anche al testamento olografo elettronico che, in realtà, come detto in apertura del lavoro, potrebbe rientrare nella branca dell'informatica giuridica, in quanto mero mezzo giuridico-telematico di snellimento procedurale. In tale ultimo caso, si riuscirebbe a garantire il rispetto della data, della presenza (fisica o anche "da remoto" dei testimoni) e della sottoscrizione (in presenza o "da remoto")? Collegando le norme del codice civile in tema di testamento olografo, con quelle relative al codice dell'amministrazione digitale e – se si vuole – con quelle relative al contenimento dell'epidemia da Covid-19, che sempre più stimolano ad una "digitalizzazione" precoce e repentina per far fluire i traffici commerciali ed economici, è auspicabile che una soluzione di sistema possa essere sicuramente approntata⁶⁶.

allo stesso contenuto digitale illecito già in precedenza comunicato formalmente all'ISP o a contenuti digitali equivalenti che presentino minime differenze rispetto al contenuto oggetto di inibitoria, tali da non richiedere autonoma valutazione da parte del prestatore di servizi della società dell'informazione. Richiedere tale condotta attiva al prestatore di servizi successivamente all'individuazione di contenuti digitali illeciti da parte del titolare dei diritti di proprietà intellettuale e industriale – *rectius ex post* – al fine di prevenire la reiterazione della condotta illecita in relazione allo stesso contenuto digitale illecito – o a contenuti digitali equivalenti – pare senza dubbio compatibile, anche a mente del generale principio di bilanciamento dei diritti contrapposti, con la tutela costituzionale della libertà di impresa e più in generale del diritto comunitario"; M. TESCARO, *Una proposta ricostruttiva contrastante con il diritto vivente in tema di responsabilità civile dell'internet provider nel diritto italiano tra Direttiva 2000/31/CE, Regolamento UE 2016/679 e Direttiva UE 2019/790*, in *Jus civile*, n. 1/2020, p. 106, ove, in chiave critica, fa osservare: "Se tutto ciò è esatto, possiamo concludere che il quadro normativo esaminato – che poteva senz'altro essere più chiaramente delineato dal legislatore europeo e da quello nazionale – è, in fin dei conti, ancora orientato a contemperare le varie posizioni tendenzialmente favorendo quella del provider, ciò che può giustificarsi in considerazione dei rilevanti interessi collettivi e individuali che con detta posizione d'ordinario coincidono, essendo del resto il «mercato [...] ancora oggi [...] il perno intorno al quale ruota gran parte del sistema normativo e delle politiche comunitarie». Ma abbiamo anche veduto come larga parte della giurisprudenza tenda e prevedibilmente continuerà a tendere in futuro a modificare il citato contemperamento in favore piuttosto dei titolari di quei diritti, per esempio ma non solo quello alla privacy, che possono entrare in conflitto con la posizione del provider". Da ultimo, dal punto di vista giurisprudenziale, si rinvia a Cass. civ., sez. I, 13 dicembre 2021, n. 39763, in *E-lex*, 12 gennaio 2022, consultabile *online*, con nota di D. MALANDRINO, *La Cassazione torna a pronunciarsi sulla responsabilità delle piattaforme per contenuti di terzi*, la quale ha statuito che: "n tema di diritto d'autore, la violazione del diritto d'esclusiva che spetta al suo titolare costituisce danno *in re ipsa*, senza che incomba al danneggiato altra prova del lucro cessante che quella della sua estensione, a meno che l'autore della violazione fornisca la dimostrazione dell'insussistenza, nel caso concreto, di danni risarcibili, e tale pregiudizio è suscettibile di liquidazione in via forfettaria con il criterio del prezzo del consenso di cui alla L. 22 aprile 1941, n. 633, art. 158, comma 2, terzo periodo, che costituisce la soglia minima di ristoro".

⁶⁶ Si legge su *AdnKronos*, 26 ottobre 2021, consultabile *online*, che: "Arriva il primo testamento digitale e che viaggia sulla *blockchain*. A lanciare l'innovazione è la *startup* innovativa Lastello fondata nel 2016 con l'obiettivo di aiutare con la tecnologia le persone che devono affrontare un lutto e le sue implicazioni anche attraverso la tecnologia *blockchain* per garantire le ultime volontà. Da oggi la *startup* romana guidata da Gianluca Tursi annuncia la nascita direttamente dal proprio sito del primo testamento digitale che può essere registrato grazie alla tecnologia *blockchain*, una procedura guidata con *wizard* intelligente che aiuterà l'utente nel corso della compilazione attraverso semplici domande e che consente così di predisporre le proprie volontà in modo facile e sicuro; (...) il documento sarà validato dalla procedura informatica creata secondo le norme di compilazione e l'utente dovrà solo trascrivere di proprio pugno e firmare il testo per ottenere il proprio testamento olografo. Per garantire la data di compilazione dell'atto e le volontà in esso contenuto, e quindi renderlo a prova di contraffazione, con Lastello, sarà possibile caricare il testamento sulla *blockchain* di *Ethereum*. Ogni anno si compilano 80.000 di testamenti, circa il 13% della popolazione vuole assicurarsi che le proprie volontà siano rispettate, per un giro d'affari di 30 milioni di euro". Ma la *blockchain* è affidabile per "consacrare" il testamento olografo? Secondo qualcuno, la risposta deve essere affermativa, in quanto le caratteristiche che rendono la *blockchain* così affidabile sono: decentralizzazione: le informazioni sono registrate tra più nodi del sistema; tracciabilità: ogni elemento del registro è rintracciabile; assenza di intermediari: non vi sono enti centrali, ogni operazione viene effettuata e registrata attraverso i nodi; trasparenza: il contenuto del registro è visibile e consultabile da chiunque; immutabilità: una volta che i dati vengo registrati, non possono essere più modificati senza il consenso della rete. Cfr., sul

Da ultimo, oltre al noto caso del “simulacro digitale”, che rientra nell’alveo della necro-robotica sulla quale ci si è già soffermati, si faccia riferimento alla recentissima pronuncia del Tribunale di Milano del 9 febbraio 2021, con la quale si è dato ordine ad “Apple” di consegnare a due genitori foto e video del figlio morto⁶⁷.

In tale dimensione, ovvero quella dei “beni digitali” (foto, video, scritti e così via), quali regole dovrebbero applicarsi dal punto di vista successorio?⁶⁸

Non c’è bisogno di aggiungere nuove norme a quelle già esistenti che, ancora una volta, sono in grado di sostenere il peso dell’innovazione (si pensi al combinato disposto dell’art. 810 c.c. con gli articoli del codice civile relativi alla successione *mortis causa*).

Ulteriore profilo è relativo alla tutela della *privacy*⁶⁹ che la circolazione di tali beni digitali nel mondo globale (basta un *like*, un *click* per la condivisione affinché continuino a circolare) impone⁷⁰. Il diritto alla *privacy* si estingue con la morte del titolare⁷¹? Se si estinguesse, dovrebbero estinguersi anche i beni digitali presenti nella rete e ancora circolanti nel momento nel quale non se ne possa più disporre⁷².

Si potrebbe disporre per testamento, anche mediante l’istituzione di un legato (disposizione testamentaria a titolo particolare), che alcuni dati/beni digitali continuino ad essere amministrati? Oppure, si può provvedere alla nomina di un esecutore testamentario che abbia il compito di eseguire le ultime volontà, anche relative ai beni digitali, del *de cuius*⁷³? Inoltre, la persona può, *ante mortem*, decidere di accordarsi con il gestore delle piattaforme digitali (magari sottoscrivendo delle DATD: “disposizioni anticipate di trattamento digitale”, un po’ sulla stessa scorta delle DAT: disposizioni anticipate di trattamento in tema di

punto, A. DE LUCIA, *Testamento digitale: finalmente è possibile*, in www.altalex.it, 16 dicembre 2021, consultabile *online*.

⁶⁷ A tal proposito, su di una c.d. “funzionalizzazione” del diritto alla riservatezza, si rinvia alla riflessione di T. M. UBERTAZZI, *Functional evolution of the right to privacy*, in *Comp. dir. civ.*, n. 3/2021, p. 857 ss.

⁶⁸ In dottrina, si trovano spunti interessanti in A. VESTO, *Successione digitale e circolazione dei beni online: note in tema di eredità digitale*, cit.

⁶⁹ È d’uopo anche riferirsi al fatto che la *privacy* debba essere ancora più contornata da “maggior tutela” qualora i beni digitali appartengano a minori. In tale ottica, si rinvia a O. LANZARA, *Il caso Tik Tok: privacy e minori di età*, in *Comp. dir. civ.*, n. 3/2021, p. 977 ss.; A. FERRERO, *Ambiente digitale e tutela dei minori online: la strategia europea*, in *Famiglia*, 8 febbraio 2021, consultabile *online*, per la quale: “La Commissione europea rispondendo all’interrogazione parlamentare E-005402/2020 ha recentemente ribadito che «il benessere dei bambini online è una delle priorità della Commissione da quando Internet è divenuta ampiamente disponibile anche a loro ed è perseguito tramite finanziamenti il coordinamento con gli Stati membri e un quadro legislativo adatto all’era digitale». Nell’ambito della strategia europea per un’Internet migliore per i ragazzi, la Commissione cofinanzia in tutta Europa i centri per un’Internet più sicura (*Safer Internet Centres*, SIC), che organizzano campagne di sensibilizzazione, forniscono formazione alle famiglie e alle scuole, gestiscono servizi di assistenza telefonica rispondendo a domande su come reagire a contatti pericolosi quali l’adescamento di minori online e mettono a disposizione linee telefoniche dirette per segnalare in modo anonimo materiale pedopornografico in rete”.

⁷⁰ Sul punto, di recente, si veda L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale*, cit., p. 1 ss.

⁷¹ Ovviamente, salva diversa volontà del titolare, il diritto alla *privacy* non si estingue con la morte. In tal senso, S. ACETO DI CAPRIGLIA, *Vocazione mortis causa negli assets digitali. Una prospettiva comparatistica*, in *Tecnologie e diritto*, n. 1/2021, p. 40, ove l’A. sottolinea che: “l’evento morte non può e non deve essere qualificato come estintivo di questi diritti”. In tale ottica, anche I. SASSO, *La tutela dei dati personali “digitali” dopo la morte dell’interessato*, in *Diritto delle successioni e della famiglia*, 2019, p. 181 ss.

⁷² Dei riferimenti in tal senso sono stati già posti in rilievo da R. TREZZA, *Diritto e intelligenza artificiale*, cit., p. 29 ss.

⁷³ L’intuizione viene fuori dopo aver letto le pagine di V. BARBA, *Contenuto del testamento e atti di ultima volontà*, Napoli, 2018, p. 7 ss.

autodeterminazione della persona umana⁷⁴), alle quali ha prestato il proprio consenso alla circolazione dei suoi dati, per la distruzione degli stessi (diritto di cancellazione dei dati, diritto alla deindicizzazione previsto dal nuovo Regolamento *privacy*, diritto all'oblio⁷⁵) per il tempo in cui avrà cessato di vivere (ora per allora)⁷⁶? E un tale accordo potrebbe essere revocato (*rectius* risolto) prima della morte⁷⁷?

Conclusions.

Evidentemente, la sfida per il civilista⁷⁸ di un "oggi futuristico" è la tutela della circolazione dei dati personali *post mortem*⁷⁹.

La normativa attuale, in tema di beni giuridici⁸⁰, di successione a causa di morte e di protezione dei dati personali, già potrebbe consentire (così come consente), anche attraverso un lavoro giudiziale nel senso di un'interpretazione sistematico-

⁷⁴ Su tale tema, solo per un rapido approfondimento, si rinvia a S. CACACE, A. CONTI, P. DELBON (a cura di), *La volontà e la scienza. Relazione di cura e disposizioni anticipate di trattamento*, Torino, 2019; M. DEL VECCHIO, *I diritti umani nelle disposizioni anticipate di trattamento*, Roma, 2018; M. GABRIELLA DI PENTIMA, *Il consenso informato e le disposizioni anticipate di trattamento. Commento alla l. n. 219/2017*, Milano, 2018; E. CALÒ, *Consenso informato e disposizioni anticipate*, Napoli, 2019; U. ADAMO, *Costituzione e fine vita. Disposizioni anticipate di trattamento ed eutanasia*, Padova, 2018. Da ultimo, si rinvia allo scritto di F. PARENTE, *Le disposizioni anticipate di trattamento: struttura, contenuto, forma e pubblicità*, in *Rass. dir. civ.*, n. 4/2020, p. 1399 ss.

⁷⁵ In tal senso, si veda A. G. PARISI, *Privacy e diritto all'oblio*, in *Comp. dir. civ.*, 2016, pp. 1-11; G. VETTORI (a cura di), *Diritto all'oblio e società dell'informazione*, Padova, 2020; S. MARTINELLI, *Diritto all'oblio e motori di ricerca*, Milano, 2017; R. PARDOLESI, *L'ombra del tempo e (il diritto all') oblio*, n. 1/2017, consultabile online; E. ERRIGO, *Il diritto all'oblio e gli strumenti di tutela tra tradizione e nuovi contesti digitali*, in *Diritti fondamentali*, n. 1/2021, specie p. 669, ove l'A. afferma che: "Pertanto, è ragionevole affermare che la digitalizzazione ha alimentato le occasioni di aggressione agli interessi e ai diritti c.d. nuovi, rendendo ancora più difficoltosa la possibilità di apprestare una tutela immediata. Per altro verso, il rilievo che assume l'autodeterminazione informativa come strumento di protezione delle situazioni esistenziali nel contesto digitale deve condurre a propendere per l'elaborazione di nuovi strumenti di protezione, sempre di tipo precauzionale ma concepiti muovendo proprio dalle caratteristiche della rete e affidati al soggetto interessato. Strumenti, quindi, preventivi ma, al contempo, successivi alla pubblicazione, così come ad esempio il potere ascrivibile all'utente di scegliere la durata di archiviazione delle proprie informazioni online prima della pubblicazione o quello di rimuovere, non soltanto alcuni *link* di collegamento, quanto e piuttosto alcune pagine non più aggiornate: soluzioni, dunque, che consentirebbero pur sempre di tutelare l'identità personale, l'esatta percezione della propria vita, la personalità del soggetto, in vista dell'attuazione effettiva delle situazioni esistenziali"; M. A. Livi, *Quale diritto all'oblio?*, Napoli, 2020, specie p. 113 ss.; F. LAZZARELLI, *Tutela dei dati personali nell'età globale: il diritto all'oblio*, in *Le Corti salernitane*, n. 1/2021, p. 3 ss.

⁷⁶ Sul punto, sembra andare in questa direzione C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit., p. 74 ss.

⁷⁷ Riflessioni "interrogative" che vengono sollecitate dalla lettura attenta delle pagine di G. PERLINGIERI, *Il ruolo del giurista nella modernizzazione del diritto successorio tra autonomia ed eteronomia*, in *Diritto delle successioni e della famiglia*, n. 1/2018, p. 1 ss. Tra l'altro, una ricostruzione simile, è offerta da A. DI PORTO, *Avvocato-robot nel "nostro stare decisis". Verso una consulenza legale "difensiva"*, in A. CARLEO (a cura di), *Decisione robotica*, cit., p. 239 ss.; G. LAURINI, G. PERLINGIERI, *Professioni legali e nuove tecnologie. Come sarà il notaio del futuro?*, in *Tecnologie e diritto*, n. 1/2021, p. 170 ss.

⁷⁸ Cfr., in tal senso, A. ALPINI, *La trasformazione digitale nella formazione del giurista*, in *Tecnologie e diritto*, n. 2/2021, p. 11, la quale fa notare che: "ciò che unisce tutte le scienze è la storia dell'uomo e il civilista, assumendo il delicato ruolo di introdurre il giovane studioso alle scienze giuridiche, deve tener conto di questa chiave di lettura".

⁷⁹ Si veda T. E. FROSINI, *Le sfide attuali del diritto ai dati personali*, in S. FARO, T. E. FROSINI, G. PERUGINELLI (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, p. 35 ss.

⁸⁰ Su tale aspetto, sembra convenire anche F. CALISAI, *Dati, informazioni e conoscenza: inquadramento giuridico e regolazione. Appunti su un potenziale paradigma appropriativo*, in *Tecnologie e diritto*, n. 1/2020, p. 13 ss.

teleologico⁸¹, risposte dinamiche e soddisfacenti agli interrogativi sopra posti, specie indirizzate ad una tutela piena della personalità umana⁸². È, dunque, il tempo di attribuire ancora più valore alla centralità della persona umana che “naviga” in una cultura ormai fin troppo globalizzata⁸³.

⁸¹ È necessario adoperare una interpretazione teleologico-assiologica, specie in relazione ai nuovi risvolti del diritto civile. In tal senso, P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 580 ss.

⁸² Non si può non rinviare a P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico*, Napoli, 1972, p. 12 ss.

⁸³ Interessanti gli spunti provenienti da A. GORASSINI, *Il valore della cultura giuridica nell'era digitale*, in *Tecnologie e diritto*, n. 2/2021, p. 38 ss.



The fascinating theory of common ownership under the lens of competition law practitioners: any needs to rethink the antitrust toolbox?

MARIANNA MERIANI 
Ph.D. in law at Bocconi University

Abstract

During the last years there has been a prolific academic debate on the possession by institutional investors of minority shareholdings in firms active within the same industry, leading to a potential distortion of market dynamics (the so-called “common ownership” theory). The common ownership doctrine raises a number of questions, and it should be looked at with caution in light of the prejudice that an incorrect antitrust assessment may have over the activities of financial institutions. This article attempts to clarify the reasons why the still new and fascinating theory of common ownership as a means of distortion of market dynamics has a long way to go before being an antitrust enforcement priority. It is debatable the same notion of the existence of a direct causality between common ownership and anticompetitive effects, whereas alternative variables may explain why in a certain period a rise in prices has been observed. In any event, even if potential antitrust risks were effectively found to materialize, the traditional competition law toolkit and the current regulatory obligations to which institutional financial investors have to comply with are suitable and sufficient to deal with the potential concerns that the common ownership theory eventually brings about and case-by-case evaluations are typical of and should guide any competition law theory of harm.



Keywords: competition law; antitrust; economics; institutional investors; investment funds; common ownership.

Summary: [Introduction.](#) – [1. The academic origins of common ownership.](#) – [2. Common ownership and anticompetitive effects in the U.S. industries.](#) – [2.1 The airline industry.](#) – [2.2 The banking industry.](#) – [2.3 The pharmaceutical industry.](#) – [Conclusions.](#)

Introduction.

Starting from the United States, there has been a prolific debate on the idea that the presence of the biggest worldwide institutional investors and of asset management companies (“AMCs”) of the caliber of BlackRock, State Street or Vanguard (*i.e.*, the Big Three) as minority shareholders in a plethora of firms active within the same industries, and allegedly competing in the same relevant markets, distorted market dynamic. This phenomenon has led to the emergence of the novel theory of harm of “common ownership” (“CO”), which assumes that institutional shareholders with minority stakes in competing firms have both the incentive and the ability to coordinate the commercial strategies of their portfolio companies or induce them to refrain from competing since that would increase the minority shareholders’ overall portfolio value.

The premise upon which it relies is open to various criticisms and beforehand competition law practitioners are called to assess the specific course of action of various categories of institutional investors with a view to assess whether their (minimal) presence within the share capital of potentially competing undertakings is sufficient to allow them to control and to influence the market-decisions of these competitors. This may be the case when a minority shareholder is granted special corporate rights in the management of the portfolio company in spite of its minority interest (*e.g.*, veto powers on business plans, or on the appointment of apical managers). Could the biggest institutional investors on a global scale leverage their strength in the financial industry to control the multitude of competing undertakings included within their portfolio and of which they usually hold a minimal share capital percentage (typically highly below 10%)? Differently from corporate structures like interlocking directorates – which, under some circumstances, might raise antitrust criticisms since they create personal connections among independent competing undertakings – institutional minority investors with no relevant veto rights may not be in the position of actively influencing the management of their innumerable portfolio companies.

In this context, this article will evaluate the criticisms raised by the CO theory by analyzing the main doctrines on this topic. On that basis, the theory will be tested by assessing the economic context where it has been observed to question whether the alleged distortions of competition have been caused by CO or rather by other factors.

1. The academic origins of common ownership.

The academic dispute on CO has been led by the eminent Harvard Law School professor Einer Elhauge,¹ who takes the side with those claiming that CO may prejudice competition. Due to their presence in the share capital of competing firms, institutional minority shareholders are presumed to control and then coordinate the market decisions of the minority-owned competing portfolio companies or induce each of them to refrain from competing. These strategies aim at increasing the overall value of institutional investors' common shares, but risk undermining "intra-portfolio" fair competition. In light of these assumptions, the CO theory does not fit within the classic "single firm" profit maximization model, which should indeed characterize competitive markets.

The CO theory preliminarily implies that the firms in which institutional investors hold minority shareholding are horizontal competitors which, because of the presence of common investors in their share capital, opt to coordinate their commercial strategies or to refrain from competing. This is due to the fact that aggressive competition among them would harm common institutional shareholders. In practice, in case of portfolio companies in a horizontal competitive situation, the existence of financial links between them because of common shareholders may be an instrument to exchange confidential information among competing firms concerning the relevant markets where they are active, or anyhow facilitate the emergence of a collusive equilibrium (horizontal *coordinated* effects). In addition, this theory assumes that common shareholders may influence the decision-making power of the minority-owned companies, inducing them to opt for a "quiet life" and to refrain from reciprocally competing (horizontal *unilateral* effects).

In such a complex framework, to deal with the claimed anticompetitive effects of CO, Professor Elhauge calls for the adoption of a severe antitrust scrutiny by applying U.S. merger control rules. In this respect, he proposes to tackle CO under Section 7 of the Clayton Act.² That regulation is the main federal substantive law governing mergers, acquisitions and joint ventures, and it expressly prohibits the acquisitions of stock or assets whose *effect "may be substantially to lessen competition, or to tend to create a monopoly"*.³ According to Professor Elhauge, whenever CO has anticompetitive effects, it violates the Section 7 ban. This rule may thus serve as the key legal device to deem illegal under antitrust law the *presence* of institutional shareholders in competing firms to the extent they distort competitive dynamics. Under this line of reasoning, the scope of Section 7 is broadened to encompass the activities of institutional investors,

¹ E Elhauge, 'How Horizontal Shareholding Harms Our Economy – And Why Antitrust Law Can Fix It' (2020) 10 Harvard Bus. Law. Rev., 2; see also E Elhauge, 'The Causal Mechanisms of Horizontal Shareholding' [2019] working paper.

² 15 U.S.C. § 18.

³ The original version of Section 7, enacted in 1914, only prohibited the acquisitions of stock of one corporation by another and, by its explicit term, it was not applicable to asset acquisitions. To avoid its elusion, the U.S. Congress amended it by passing the Celler-Kefauver Antimerger Act so to include tangible and intangible assets within its scope of application.

even though they are ordinarily exempt from merger control rules if they invest in companies for *sole financial* purposes. In addition, as common shareholders are claimed to favor collusion among competing firms, Section 1 of the Sherman Act that generally prohibits contracts, agreements, or any form of conspiracy in restraint of trade may also apply.

Likewise Professor Elhauge, other scholars – Posner, Scott, Morton and Weyl – have claimed that, in concentrated industries, mutual funds and other institutional investors soften competition among their commonly-owned companies to the extent that they compete within the same markets.⁴ To limit institutional investors from indirectly gaining relevant power in the affected markets, they propose to cap their influence to 1% of the total size of an industry, or to allow them to acquire shares exclusively in one portfolio company *per* industry.

On the opposite, there are authors that even recently contested the assumptions underlying the CO theory and which, on the basis of statistical studies, empirically proved that “*greater common ownership is, all else equal, not robustly related to industry outcomes in a manner consistent with reduced competition*”. As regards the existence of a causal link between common ownership and competition, they claim that “*it is too weak to be identified*” and “*the magnitudes of the [anticompetitive] effect may be too small to detect in an average effect estimated across all industries*”.⁵

In light of these contrasting views, the studies carried out so far on CO in the airline, banking and pharmaceutical industries will be critically looked at to assess whether CO has effectively been the *cause* of the observed adverse pricing effects in those sectors, or whether any alternative factor may have played a role in explaining the high market prices, as confirmed by the cautious approach of the antitrust enforcers so far.

2. Common ownership and anticompetitive effects in the U.S. industries.

2.1 The airline industry.

The idea that CO caused adverse pricing effects in the U.S. airline industry is based on a study carried out by the distinguished scholars Azar, Schmalz and Tecu. They claim to have empirically proved with a 99% statistical confidence level that in the U.S. airline industry high levels of horizontal ownership resulted into an increase of market concentration, causing in turn a rise in airfares.⁶ In this sector, the biggest AMCs allegedly have extremely large market power by having minority shares in most U.S. publicly traded airlines. As a consequence, common shareholders are claimed to influence the executive managers to align commercial strategies of competing airlines. To this end, common investors may use various methods to induce managers to pursue industry performance rather than

⁴ E Posner and others, ‘A proposal to Limit the Anti-competitive Power of Institutional Investors’ (2017) 81(3) Antitrust L. J., 669-728.

⁵ A Koch, M Panayides, S Thomas, ‘Common ownership and competition in product markets’ (2021) 139 J. Fin. Econ., 109-137.

⁶ J Azar, M C Schmalz, I Tecu, ‘Anticompetitive Effects of Common Ownership’ (2018) 73(4) J. Finance, 1513-1565.

the performance of the individual firm, *in primis* incentive schemes that link compensation of managers to industry goals, with the consequence that managers are paid less for their own firm's performance and more in case of an increase in the overall industry performance.⁷ As a result, common shareholders not only have the ability, but also the incentive to induce the executive managers of the minority-owned companies either to coordinate their strategies, or to refrain from engaging in aggressive competition among each other.

By proceeding a step further, the Airline Study then focuses on concentration within the airline industry and looks at the ownership composition of airline companies to assess the extent to which the most representative investors in the various airline companies had also shares of competing airlines. As such, the Study broadens the economic model that O'Brien and Salop developed more than a decade earlier to assess the competitive effects of horizontal joint ventures that post-transaction would have been active in the same relevant markets of the parents. That model still helps antitrust enforcers to evaluate the competitive risks in terms of potential coordination that may arise if a company holds the stocks of a direct competitor, as it is precisely the case of parent companies that will be active in the same relevant market of their controlled joint venture.⁸ The model assumes that, in oligopolistic markets, where the few competitors are interested in maximizing a weighted sum of the overall profits accruing to their common owners, a shareholder's influence in a firm's strategic plan is proportional to the share capital it holds in that firm as well as in commonly owned companies. The same logic is applied to CO involving institutional investors, where partially owned companies are allegedly disincentivized from competing with each other since the increase in the value of one company's shares leads, in turn, to a decrease in the value of shares of competitors to the prejudice of the value of common investors' portfolios. Therefore, under the CO theory, the higher the market concentration index, the higher the intrinsic anti-competitive incentives created by CO.

Under the above assumptions, the Airline Study concludes that, in a situation in which common shareholders were present in various airline carriers active within an already concentrated sector, CO allegedly had a negative impact on airfares. To empirically strengthen the existence of a causal link between CO and the observed adverse effects on prices of airline tickets, the Airline Study evaluated whether the assumed anticompetitive incentives of common shareholders translated into *measurable effects* on product market competition (*i.e.*, on competition on airfares in the relevant market where the commonly owned airline companies were active). In that respect, the study assessed to what extent a variation in CO concentration in a given route over time caused changes in airfares in that route. The authors conclude that competition in airline routes decreased when the shareholders of incumbent airlines acquired

⁷ M Anton and others, 'Common ownership, competition, and top management incentives' [2016] ECGI, finance working paper.

⁸ DP O' Brien, SC Salop, 'Competitive effects of partial ownership: Financial interest and corporate control' (2000) Antitrust L. J. 67, 559-614.

significant ownership (and control rights) in an independent airline serving the same route, contributing to further concentration of the industry. Evidence of this negative effect is claimed to have been significant, in the order of a 3-11% increase of the average U.S. airfare within routes, as compared to a counterfactual scenario of separate ownership.

The Airline Study is certainly interesting as it tries to find one possible explanation to the observed pricing increase within a concentrated sector and it links it to the rise in CO. However, as the same authors make clear, the findings of that study are consistent with standard notions of corporate governance: only CO by the biggest shareholders (usually those ranked first and second) within competitors may have a positive and statistically significant effect on airfares. CO by investors with considerably lower shareholding (as it is usually the case of the Big Three) may have small and less statistically significant effect on prices. This is certainly relevant since this article focuses on the biggest AMCs and on other institutional investors, which typically operate as financial shareholders by holding minimal share percentages (below 10%) in their portfolio companies. Accordingly, under traditional rules of corporate governance, it is questionable that they can effectively influence the managers of their portfolio companies by holding minimal percentages of their share capital.

There are anyhow doubts as to the fact that it was the presence of common investors in airline companies to have certainly caused the observed increase in prices of airline tickets. To take a step further in the analysis, one should contextualize the Airline Study and assess the CO theory in light of the dynamics and events that characterized the U.S. airline industry in the period under investigation. In the following sections there will be hence an analysis of whether other events that occurred in that industry may have played a role in connection with the observed rise in airline ticket prices and may thus act as alternative (or even the only explanatory) variables that led those prices to increase.

The “Airline Study”: any gap in the CO theory of harm?

The Airline study represents an important empirical application of the CO theory of harm in the U.S. airline industry as it explores possible causes of the observed pricing increase within a concentrated market. But was the CO the cause of that price increase or was that increase the effect of sector dynamics? In that context, a further question arises as to whether the antitrust enforcer may have intervened *ex ante* to prevent further concentration of the industry when reviewing concentrations among airlines which triggered the application of merger control rules. Could the antitrust enforcer have taken CO into account in the context of merger reviews as a contextual element in the competitive assessment? In the following sections, a clearer picture on these issues will be provided.

(i) The U.S. airline industry as a tight oligopoly.

In a relatively short period of time, the U.S. airline industry underwent a major wave of consolidation as a result of various mergers, that were reviewed by the antitrust authority. Could the DOJ have been more active

and vetoed some transactions on the assumption that parallel conduct leading to higher prices may have been easier in an oligopolistic structure?

To answer the above question, a preliminary analysis of the trend towards consolidation of the U.S. airline industry, experienced during the last two decades, should be undertaken. In particular, in 2008, the DOJ let Delta Air Lines to merge with Northwest Airlines. Delta was the third largest airline in the U.S. and Northwest was the fifth.⁹ The merger gave rise to what was then the largest commercial airline in the world, with almost eight-hundred aircrafts. Despite the substantial market power that the merged airline would have enjoyed in the U.S. airline industry, after a six-month investigation the DOJ concluded that the merger would have produced substantial and credible efficiencies to the benefit of U.S. consumers.¹⁰

Two years later, in 2010, the DOJ cleared United Airlines' acquisition of Continental Airlines, after the companies divested some airport slots to Southwest Airlines.¹¹ To solve the anticompetitive concerns identified by the antitrust enforcer, United Airlines and Continental Airlines agreed to transfer takeoff and landing rights' slots and other assets at Newark Liberty Airport to a third-party, *i.e.* Southwest Airlines. Thereafter, the DOJ cleared Southwest's acquisition of AirTran Airways.¹² After a thorough investigation, the antitrust authority concluded that the merger was not likely to substantially lessen competition.

Again, in November 2013, the DOJ allowed U.S. Airways to merge with American Airlines' parent company (AMR) under commitment to divest a certain number of airport slots.¹³ In this respect, the merging parties entered

⁹ In particular, Delta carried more than seventy-million passengers *per annum* and with regional affiliates serving more than three-hundred destinations in almost sixty countries, whereas Northwest carried at the time more than fifty-million passengers and serving almost two hundred and fifty destinations in twenty countries in North America, Asia and Europe.

¹⁰ 'Statement of the DOJ on Its Decision to Close Its Investigation of the Merger of Delta Air Lines Inc. and Northwest Airlines Corporation' [2008] DOJ press release, 08-963. The clearance decision valued the fact that the two airlines competed with a number of other legacy and low-cost carriers (LCCs) in the offer of scheduled air passenger services on the vast majority of non-stop and connecting routes. In addition, the merger would have produced efficiencies in terms of cost savings for airport operations, information technology, supply chain economics and fleet optimization. Furthermore, the combination under single ownership of the complementary aspects of the airlines' networks increased the quality of airport services.

¹¹ 'United Airlines and Continental Airlines Transfer Assets to Southwest Airlines in Response to Department of Justice's Antitrust Concerns – DOJ Closes Investigation, Transfer of Newark, N.J., Assets Resolves Competition Concerns' [2010] DOJ press release, 10-974. In particular, United Airlines was the third largest carrier in the U.S. by revenue. At the time, it served approximately eighty million passengers and offered service to more than two hundred destinations in the United States and thirty other countries throughout the world. Continental Airlines was the fourth largest carrier in the United States by revenue, carrying almost seventy million passengers and offering service to more than two hundred fifty destinations in the United States and over fifty other countries throughout the world.

¹² 'Statement of the DOJ on Its Decision to Close Its Investigation of Southwest's Acquisition of AirTran' [2011], DOJ press release, 11-523. Southwest Airlines was based in Dallas and, at the time, it carried approximately ninety million passengers, serving seventy cities in the U.S., while AirTran was based in Orlando and carried approximately twenty-five million passengers in seventy cities in the U.S., Mexico and the Caribbean.

¹³ 'Justice Department Requires US Airways and American Airlines to Divest Facilities at Seven Key Airports to Enhance System-wide Competition and Settle Merger Challenge' [2013] DOJ press release, 13-1202. More precisely, AMR was a Delaware corporation which, at the time, carried more than eighty million passengers to more than two-hundred fifty destinations worldwide, but it had undergone a period of financial distress, and in November 2011 filed for bankruptcy. US Airways was

into a settlement which would have incentivized LCCs to invest in new capacity at key U.S. airports and to compete nationwide on non-stop and connecting routes. As a result, airline travelers could benefit from more competitive prices and enhanced travel options. The settlement, which was approved by the District of Columbia in 2014,¹⁴ solved the lawsuit that had been launched by the DOJ and then joined by six State general attorneys (Arizona, Florida, Pennsylvania, Michigan, Tennessee and Virginia) on the ground that the acquisition would have substantially lessened competition for commercial air travel in local markets throughout the U.S.

As the above excursus of the trend of consolidations in the airline sector makes clear, the DOJ did not refer to cross and common ownership as a cause for potential distortion of competitive dynamics within that sector. This is so even though the DOJ's clearance decisions of the notified mergers were adopted in the period covered by the Airline Study. In fact, that study covered some airline carriers that, at the same time, were subject to the DOJ's antitrust scrutiny (such as American Airlines, Southwest Airlines, Delta Air Airlines and Continental). Despite this clear overlap, the Airline Study claims that CO in airline carriers caused the observed rise in airfares, whereas the DOJ cleared the notified transactions which involved these flight carriers also on the basis of efficiency arguments to the benefit of passengers. Among these benefits, the DOJ referred to more competitive airfares. Hence, it is reasonable to assume that the antitrust enforcer would have at least mentioned CO when assessing the ownership structures of the merging airline carriers had CO raised criticisms under antitrust law on the basis that it would have likely caused a rise in airfares.

The above seems even more reasonable if one considers that, in addition to the aforementioned merger reviews, in 2015 the DOJ opened an investigation to assess whether the increase in average airfares was the result of a collusive strategy among airline companies to keep airfares high. Some of the investigated companies appeared as both portfolio companies of institutional investors and as parties to the transactions notified to the antitrust authority under merger control rules (like Delta Air Lines, Southwest Airlines, American Airlines and United Airlines). The antitrust investigation was probably triggered by a concern expressed by the U.S. Senate for an observed increase in airfares to the prejudice of final consumers. In a letter sent in June 2015 to William Baer, at the time Assistant Attorney General, the U.S. senator Richard Blumenthal called the DOJ to investigate the *"apparent anti-competitive conduct potentially reflecting a misuse of market power, and excessive consolidation in the airline industry"*, a process within which the *"DOJ itself played a part ... by approving several mergers and now consumers are paying sky-high fares as airlines engage in market conduct designed to keep capacity artificially low"*. In this context, the DOJ decided to launch an investigation to assess the existence of coordinated effects among the airlines in breach of Section

also a Delaware corporation, carrying more than fifty million passengers to more than two hundred destinations worldwide.

¹⁴ *United States of America et al. v. US Airways Group, Inc. and AMR Corporation* [2014], The U.S. District Court for the District of Columbia, 1:13-cv-01236 (CKK).

1 of the Shearman Act. To this end, it sent to the major U.S. carriers (American Airlines, Southwest Airlines and United Airlines) a letter to request copies of all communications they had exchanged and clarifications about their plans in terms of passenger-carrying capacity. Interestingly, what emerges from the few public available information is a classic conspiracy theory, that could have been achieved through an exchange of confidential information during trade association meetings. Nothing new for antitrust practitioners. However, the DOJ did not find any proof of conspiracy underlying the observed increase in average airfares and, as such, an enforcement action did not consequently follow.

The above explains why, although the CO theory implies that common minority shareholders are in the position to influence the management and to orient the commercial conducts of their portfolio companies, that “presumption” does not appear to have been solidly supported by evidence. Nor the antitrust enforcer should infer by the parallel conduct of the various portfolio companies the existence of an anticompetitive concerted action among them on the assumption that the likelihood for common shareholders to vehicle sensitive information reduced the intrinsic risks of competition.

The dividing line between legitimate parallel conducts and concerted vs unilateral actions is very thin. In this framework, because of the uncertainties as to whether legitimate parallel behavior or other factors (such as CO) may cause price increases, could antitrust enforcers step-in even though there is no evidence of detectable acts of collusion among common shareholders? The answer should be negative in light of the well-known theories on the application of competition law principles to oligopolies. Under the *theory of conscious parallelism*, in an oligopoly conscious parallel conduct is nothing more than a form of tacit collusion, that should be prosecuted under competition law like explicit collusion.¹⁵ On the other hand, according to the *theory of interdependence*, in oligopolies parallel conduct deserves to be prosecuted under antitrust law only if accompanied by detectable acts of collusion which are not the result of legitimate interdependency among the few oligopolists.¹⁶ Therefore, even a supra-competitive market equilibrium in oligopolies is not necessarily due to collusion, but may depend on the interdependency among the few

¹⁵ RA Posner, ‘Oligopoly and the Antitrust Laws: A Suggested Approach’ (1969) 21(6) Stan. L. Rev., 1562-1606. According to this author, conscious parallelism tacitly aims at altering unilateral actions of independent market players. As a consequence, the application of Section 1 of the Shearman Act against that tacit collusion “*would do no violence to the statutory language or purpose*” of the antitrust ban set forth therein “*and while difficult problems of proof and of remedy would be involved, [it is questionable] that they would be insuperable*”.

By applying this theory to the airline sector, if an airline announces a pricing strategy or makes public statements concerning either future airfares or other commercial confidential information, and consequently other airlines implement a similar policy in the absence of any proof of contacts among them (even channeled by common shareholders), that public signaling may be evidence of the attempt to reach an anticompetitive equilibrium.

¹⁶ D Turner, ‘The Definition of Agreement Under the Sherman Act: Conscious Parallelism and Refusals To Deal’ (1962) 75(4) Har. L. Rev., 655-706. To solve any criticisms, when antitrust law may not be applied because of the absence of a probative support as to the existence of a concerted conduct, new regulatory remedies should be framed to deal with the observed distortions of market dynamics whenever oligopolistic markets could not self-discipline.

competitors, that could easily monitor each other and find convenient to mimic each other strategy and converge to that equilibrium.¹⁷

The application of the interdependency theory to the U.S. airline industry, that seems to be more in line with traditional antitrust principles,¹⁸ may help with explaining the observed fluctuations of prices in that sector. This argument finds support in a recent empirical study that observed distortions of competition on quality of airline services. By applying the interdependency theory, the study finds that “*in the US Airline industry ... strategic non-price interactions between firms conform to expected oligopoly behavior*”.¹⁹ In this context, market transparency and interdependency among airlines may be pivotal in shaping the reciprocal commercial strategies as each carrier observes the conducts of competing airlines and modifies its behaviour accordingly. However, nothing new or problematic under antitrust law emerges in such a context.

Even in the civil lawsuit filed before the U.S. Court for the District of Columbia against US Airways and American Airlines to try blocking the merger between the two flight carriers,²⁰ the oligopolistic structure of the market – and *not* common minority shareholders as alleged “owners” of competing airlines – was investigated to assess whether it could have favored the emergence of a supra-competitive airfare price equilibrium.²¹

¹⁷ This course of action exemplifies the legitimate behavior of a “*rational oligopolist*”, who according to Professor Turner behaves “*in exactly the same way [of] the rational seller in a competitively structured industry*”.

¹⁸ In Europe, a similar trend may be observed. In this respect, in the leading Woodpulp II case, the EU Court of Justice clarified “*that parallel conduct cannot be regarded as furnishing proof of concertation unless concertation constitutes the only plausible explanation for such conduct*”. This is so because the ban of anticompetitive agreements catches “*any form of collusion which distorts competition, it does not deprive economic operators of the right to adapt themselves intelligently to the existing and anticipated conduct of their competitors*”. The principle expressed by the EU Court of Justice relies on the economic finding that, in oligopolies, conscious parallelism may arise in the absence of a collusive equilibrium (even tacit) among the few competing undertakings. For more details, see A Rosas, E Levits, Y Bot, *The Court of Justice and The Construction of Europe, Analyses and Perspectives on Sixty Years of Case-law* (T.M.C. Asser Press 2013).

¹⁹ S NOOR, ‘Non-price competition in the U.S. airline industry: a VAR model’ [2017] J. Econ. Stud. In particular, despite not referring to pricing but to another competitive variable, *i.e.* product quality, this study assesses the interactions among the major domestic airlines in the U.S. when taking decisions on product quality to make their services more attractive to travelers. It observes that in oligopolistic industries, where competition is highly influenced by the strategic interaction between a few competing firms, product quality is a relevant aspect of competition which could be easily observed. As a result, airlines are incentivized to improve the quality of readily observable airline services to retain market shares.

²⁰ *United States of America et al. v. US Airways Group Inc. et al.* (2014) The District Court for the District of Columbia, civil action 13-cv-1236 (CKK).

²¹ In particular, in August 2013 the DOJ, six state general attorneys and the District of Columbia filed an antitrust lawsuit alleging that US Airway’s \$11 billion acquisition of American Airlines would have substantially lessened competition for commercial air travel in local markets throughout the United States. The merger would have eliminated two independent competing airlines, ending head-to-head competition between the two on numerous non-stop and connecting routes, leaving the market with only three similar legacy airlines – *i.e.*, Delta, United, and the merged airline. The reduction in the number of airlines from four to three would have shifted the industry towards a tighter oligopoly. In addition, four of the busiest airports in the country – *i.e.*, Reagan National, LaGuardia, John F. Kennedy International, and Newark Liberty International – were subject to slot limitations governed by the Federal Aviation Administration (“FAA”). Slots at these airports were concentrated in the hands of legacy airlines that had little incentive to sell or lease them to more aggressive carriers. Competition would not have been likely neither by non-legacy carriers, nor by new entrants because of the high barriers to entry due to the lack of slots’ availability.

Although the transaction raised some antitrust concerns, the DOJ never referred to CO as a contextual element which may have favoured anticompetitive collusion (for example, in the form of higher airfares and lower quality services to the detriment of passengers).²² Finally, the merger was cleared and the District Court required the merging parties to divest many slots, gates, and additional ground facilities at key airports around the country to incentivize LCCs to invest in new capacity and enter the market.

In this context, the economic theory that underpins the Airline Study – *i.e.*, the existence of a causal link between the increase in CO in U.S. airline companies and the rise in airfares from 2001 to 2013 – seems to lack empirical support, whereas it may have been the shift towards a tight oligopoly that made the market more transparent. In that scenario, competing airlines could have found easier to monitor their actions to implement parallel commercial strategies in the absence of coordination among them, and CO may have played no role in respect to the observed increase in prices.

(ii) CO is the cause, not the “effect” of oligopolistic prices: any (missed) chance for the U.S. antitrust enforcer to intervene?

On a different note, it has been claimed that CO may not be the cause of supra-competitive prices, but its effect. When an industry becomes more concentrated, the biggest institutional investors and AMCs step-in to acquire shares of companies active in that industry. This relies on the assumption that in an oligopoly companies can charge higher prices and increase their profitability. As a result, shares become more “valuable” and institutional shareholders increase the value of their share portfolios by acquiring shares of these companies. There is also a higher chance that these companies are included in financial indexes like the S&P500 – *i.e.*, those referred to in the studies on CO carried out so far and including companies on the radar of the biggest institutional investors. In this context, it is oligopolistic pricing that may contribute to CO, not the other way round.²³

The above distinction (CO cause vs effect of monopoly pricing) is relevant to apply merger control rules and it raises doubts in connection with the solutions proposed so far to solve the alleged anticompetitive effects of CO, such as the wide application of Section 7 of the Clayton Act. That rule only prohibits mergers and acquisitions that have the effect of lessening competition or creating a monopoly. Thus, acquisitions of minority shareholdings that trigger the application of merger control rules, if not carried out for mere financial purposes, may already be blocked if they have the effect of loosening competitive dynamics in a meaningful way, but not

²² More precisely, if one looks at the District Court's decision, the only reference to the ownership structure of the merging parties can be found in one of the settlement conditions. In particular, the merged company was obliged not to reacquire an ownership interest in the divested slots or gates during the term of the settlement. This obligation was merely ancillary to the effective implementation of the divestiture order since the re-acquisition of an interest in the divested slots would have deprived the order of its effects. Clearly, it had nothing to do with the CO theory as a new potential vehicle to influence commercial strategies of competing companies and accordingly distort market dynamics.

²³ BR Dryden, 'Horizontal Shareholding': Is Oligopoly Pricing a Symptom or the Disease?' [2017] ABA Newsletter of the Mergers & Acquisitions Committee.

simply because they might result in consolidation of an industry which in turn “causes” CO.²⁴

The application of Section 7 of the Clayton Act to acquisitions of minority shareholding – although not necessarily by financial investors – has been already scrutinized by the U.S. courts and antitrust enforcers. However, only in the few cases where these transactions raised appreciable competitive concerns, the antitrust enforcers have challenged them.²⁵ In particular, these transactions have been clustered in three main categories²⁶ – transactions in which (i) the acquiring firm is a direct competitor of the target itself;²⁷ (ii) the acquiring firm has a controlling interest in a direct competitor of the target;²⁸ (iii) the acquiring firm has in a direct competitor of the target a non-controlling interest, which in some instances could raise concerns under an antitrust standpoint.²⁹

²⁴ For the sake of completeness, a similar “by effect” analysis should be carried out under European merger control law. In particular, the European merger regulation prohibits concentrations which would likely have the effect of “*significantly imped[ing] effective competition*” in the relevant markets (see, Council Regulation 139/2004 of 20 January 2004 on the control of concentrations between undertakings [2004] OJ L 024/2004, 1 - 22).

The European merger control framework is to a certain extent more stringent than the U.S. one, since minority shareholding acquisitions by financial asset managers and other institutional investors are usually exempted from the merger scrutiny unless, *on jurisdiction*, these transactions grant minority shareholders with at least *de facto control* on the target companies. Should that be the case, the merger is subject to the European Commission’s scrutiny which is called to assess, *on the merits*, whether the transaction is likely to cause prejudicial effects on competitive dynamics.

²⁵ ME Jacobs, ‘U.S. Antitrust enforcement involving minority shareholdings’ [2013] <<https://www.fne.gob.cl/wp-content/uploads/2013/11/Minority-Shareholding-in-the-US.pdf>>.

²⁶ PC Cuomo, C Malaise, C Xu, ‘Partial Acquisitions: Recent MOFCOM Action Suggests Possible Divergence with U.S. Standards’ [2012] CPI Antitrust chronicle.

²⁷ ‘American Airlines cleared to acquire stock in Argentine Airline’ [1998] DOJ press release, 98-320. In particular, the transaction involved the acquisition by American Airlines of 8.5% in its direct competitor, Aerolineas Argentinas and raised antitrust concerns as initially structured. Under the original proposal, American would have had a representative on the Aerolineas board of directors, as well as permanent rights to veto certain large investment decisions by Aerolineas. To solve the antitrust concerns, the parties restructured the transaction and American Airlines would have had no director on the Aerolineas board and limited shareholder rights until the Spanish interests were sold to third parties, at which time it would have become a passive investor. As a result, on July 1998 the DOJ cleared that acquisition, but the clearance did not preclude potential future interventions of the DOJ, which reserved the right to challenge the transaction in the future if American would have acquired the ability to influence Aerolineas’ competitive decisions affecting U.S. markets or engaged in anticompetitive coordination.

²⁸ *United States v. Dairy Farmers of America*, (DFA’s) (2005) U.S. District Court for the Eastern District of Kentucky, Civil Action 6:03-206-KSF. In April 2003, the DOJ filed a lawsuit challenging DFA’s partial ownership interest in two rival dairies (Flav-O-Rich and Southern Belle Dairy). The DOJ alleged that, as a result of the two subsequent acquisitions (the first in Southern Belle Dairy in 2002, and then in Flav-O-Rich), DFA’s ownership interests in both dairies gave it an incentive to reduce competition and facilitate unilateral price increases regardless of any coordination because it would not matter if customers of either dairy switched to the other dairy in response to a price increase. DFA changed its governance rights, converting its common voting stock in the companies that operated both dairies into non-voting stock, with the consequence that it then obtained a motion for summary judgment as it was not anymore in the position to exercise control over the management of the dairies. However, on appeal by the DOJ, the U.S. Court of Appeals for the Sixth Circuit reversed the lower court’s ruling, holding that the DOJ had presented sufficient evidence to prove that DFA’s acquisitions violated antitrust laws. Nor the voluntary relinquishment of voting rights remedied the violation because DFA may have still imposed its voice upon the firm (for example, the firm relied on DFA for additional capital). As a result, DFA decided to sell the Southern Belle dairy plant to another firm.

²⁹ *Competitive Impact Statement, United States v. Univision Communications, Inc.* (2003) U.S. District Court of Columbia, Civil action 1:03CV00758. The transaction concerned the acquisition by Univision (*i.e.*, the largest broadcaster of Spanish language television programming in the United

By contrast, the Section 7 ban should not be applied if the alleged anticompetitive effects depend on the structure of the industry, which in turn causes (and it is not the effect of) horizontal shareholding. In a scenario in which CO may not be the cause of oligopoly pricing but rather its outcome, it should be indeed explored whether the implementation of *ex-ante* regulatory solutions is needed and may be preferable to the wide application of merger control rules to limit the activities of financial investors on a global scale.³⁰ In this respect, the potential negative effects that the introduction of additional regulations to those already applied to the financial sector should be also considered, *in primis* the risk of restraining their ability to diversify investments in a plethora of industries to reduce the economic risks to which final consumers are exposed when investing.

In any event, the fact that CO due to industry consolidation may eventually escape the antitrust scrutiny under merger control rules does not mean that it is exempted from the application of other antitrust rules. To the extent that there is evidence of an anticompetitive coordination among competing portfolio companies imputable to institutional investors in their quality of common minority shareholders of these firms, that conduct may be prosecuted *ex post* as a form of an anticompetitive restraint of trade or as an unfair commercial practice, respectively in breach of Section I of the Shearman Act and of Section V of the FTC Act.³¹ By contrast, if there is no

States) of a partial ownership in the media company HBC, that owned and operated more than 60 radio stations in 18 geographic regions in the United States, most of which broadcast in Spanish. At the time of the transaction, Univision also had a minority interest in another Spanish language media company (Entravision) and significant governance rights, including the right to place two members on Entravision's board and the right to veto certain of Entravision's business decisions. Entravision was HBC's principal competitor in Spanish language radio in many markets. In this context, the DOJ expressed concerns that the acquisition would reduce the incentives of both partially owned companies to compete aggressively against each other in the sale of Spanish language radio advertising time and it would have led to an increase in prices for a significant number of advertisers. To solve the antitrust concerns and avoid enforcement actions, the DOJ and Univision entered into a settlement by which Univision was prevented from participating in Entravision governance or influencing its radio business. In particular, Univision agreed to divest a significant portion of its equity stake in Entravision, relinquish its right to two seats on Entravision's Board of Directors and give up the right to veto certain Entravision business decisions, in addition to reduce its ownership in Entravision to no more than 10%.

³⁰ This may be even more true if one considers that in general in the U.S. neither State laws nor federal law make charging high prices which may cause prejudice to final consumers (and not addressed to exclude competitors) unlawful, since even monopoly prices may serve to stimulate entry and further innovation (*Verizon Communications Inc., v. Law offices of Curtis V. Trinko, LLP* [2004] U.S. Supreme Court, No. 2-682). In this context, antitrust officials have reminded that "*simply condemning a high price... is not antitrust. It is a regulatory action meant to reengineer market outcomes to reflect enforcers' preferences*" (see M K. Ohlhausen, 'What Are We Talking About When We Talk About Antitrust?' [2016] Concurrences Rev.).

³¹ At least in Europe, such conduct by the biggest institutional investors may be also caught by the abuse of dominance prohibition to the extent that the antitrust enforcer succeeds in proving that these investors presented on the market as one collective entity, which abused the single collective dominant position it held to charge supra-competitive prices to exclude competitors of their portfolio companies. The prohibition of abuse of dominance is general and it could also address acquisitions of minority shareholding by institutional investors which are likely to prejudice competitive dynamics in the relevant market. However, abuses of collective dominance are difficult to prove for competition authorities and are quite rarely brought. This is so as to bring a credible abuse of collective dominance case, the authority needs to observe a stable behavioural pattern where the various undertakings, that collectively hold a significant aggregate market share, repeatedly act jointly to implement a series of commercial strategies which are likely to prejudice market dynamics (see Judgment of 21

evidence of a conduct likely to alter market dynamics due to CO in the form of explicit or tacit collusion, the antitrust toolbox should not be applied.

As made clear, in assessing a number of mergers that involved airlines, the U.S. antitrust authority widely looked at sector dynamics but ultimately it did not veto these transactions, even though it may have avoided the further concentration of the industry, which could have minimized the claimed risk that the few common shareholders of competing airlines coordinated their activities. These mergers were indeed cleared on the basis that they did not have the effect of distorting competition. In fact, they were deemed to be beneficial to passengers.³²

In this context, the question is not whether CO in the U.S. airline industry had anticompetitive effects, but whether in assessing a certain number of sequential mergers the U.S. antitrust enforcer should have scrutinized them more in-depth and to what extent the wave of industry consolidation caused (and was not caused by) CO and favoured the alleged coordination on prices. Did the authority adopt a too lenient approach in clearing these transactions, allowing airlines to be shielded from the application of the antitrust ban and to coordinate on prices or flight schedules?³³ In this respect, various studies on airline M&As claim that prices within that industry increased after a merger was completed,³⁴ and the increase in airline dominance within an airport due to a merger resulted in higher barriers to entry and higher fare *premia*.³⁵

The airline mergers discussed above were scrutinized by the antitrust authority and cleared. Whether the enforcer was too lenient in clearing these transactions, or indeed right in assessing their pro-competitive effects rests upon the discretion of the antitrust authority, which may be eventually questioned. In addition, some of the U.S. airline mergers were approved by court orders and thus marked with a judicial seal. Again, the application of traditional antitrust principles was not questioned. In such a context, one could reasonably conclude that when an increase in prices observed within a concentrated market gets attributed to ownership structures of market players, but no evidence of anticompetitive conducts is found, the intervention of antitrust authorities to fill in potential regulatory gaps may not represent the preferable policy solution.

2.2 The banking industry.

February 1973, *Europemballage Corporation and Continental Can Company Inc. v. European Commission*, 6/72, ECLI:EU:C:1973:22).

³² For example, the US Airways/American Airlines merger improved network connectivity, increased flier loyalty programs, and optimized the use of aircrafts. Duplicative activities were also dismissed due to asset combination, inefficient or redundant hubs, or route closure. Furthermore, this merger also led to operational efficiencies through integration of the merged airlines operating systems. The US Airways/American Airlines merger led to a loss of a competitor on non-stop routes, but it still created an effective competitor in several airport-pairs, to the benefit of millions of passengers.

³³ W Gillespie, O Richard, 'Antitrust Immunity and International Airline Alliances' [2001] Economic Analysis Group of the DOJ's Antitrust Division.

³⁴ Testimony of GL Dillingham, 'Airline Industry Consolidation: Hearing Before the Subcommittee on Aviation' [2013]; S Borenstein, 'Airline Mergers, Airport Dominance, and Market Power' (1990) 80 *American Econ. Rev.*

³⁵ S Borenstein, 'Hubs and High Fares: Dominance and Market Power in the U.S. Airline Industry' (1989) 20 *RAND J. Econ.*, 344-365.

The CO theory has also been applied to the U.S. banking sector where horizontal and cross shareholding allegedly caused a significant adverse effect on bank fees and rates.³⁶ The main study reports that over the last decade an increase in fees for banking deposit services has been registered in the U.S. and it has been caused by the high presence of common shareholders in competing banks (the “Banking Study”).³⁷ More precisely, that study claims that during the period subject to investigation institutional investors were among the top five shareholders of the nation’s five largest banks. In addition to CO, cross-ownership links among competing banks strengthened the interconnections among them.

By applying the principles discussed so far on CO, the price increase has been causally linked to the existence of a collusive equilibrium among the common investors, who allegedly made use of various corporate governance mechanisms to explicitly coordinate the commercial strategies of the banks in which they held minority shares (e.g., informal meetings with managers of portfolio banks or adoption of strategies aimed at disincentivizing the management of these participated entities from engaging in head-to-head competition with competing banks). In such a context, the Banking Study calls for the intervention of the antitrust authorities.

The antitrust assessment of the “Banking Study”: any lacuna?

The arguments set forth in the Banking Study rest on the assumption that CO allegedly distorted market dynamics since the biggest institutional investors were in the position to leverage their valuable presence in the banks, within which they held common shares, to induce their management to collude on the increase of prices of banking services. CO by institutional investors was perceived to be critical under competition law and the antitrust enforcer had to step-in, notwithstanding the pivotal role of banks in the economy such as helping clients with diversifying investments and reducing financial risks.

The results of this analysis clearly demonstrate that, instead of resulting in a (not still proved) distortion of competition, CO can bring about several positive effects on market dynamics. Some of these effects do not concern competition as such but the real economy at large. In the financial sector, at a macro level, CO helps with achieving the stability of the financial system, for example, during a liquidity crisis. As said, another valuable pro-competitive effect is at micro level, in terms of benefits to individuals who invest in passive index funds and benefit from the lower transaction costs charged by experienced asset managers and the diversification effects that the passive index funds achieve.³⁸

³⁶ MC Schmalz, J Azar, R Sahil, ‘Ultimate Ownership and Bank Competition’ [2016] CEPR working paper.

³⁷ The assessment relies on the assumption that bank concentration is generally prejudicial to market dynamics as it may impact on monetary policies, slow down the adoption of new technologies, as well as adversely affect consumers, which may receive lower rates on their savings despite paying more for loans.

³⁸ European Parliament, Study of the ECON committee, Barriers to Competition through Common Ownership by Institutional Investors [2020], 53 ff.

In the above framework, even if anticompetitive effects occurred as a result of CO (which should still be proved), the trade-off between detrimental effects and benefits to final consumers would call for a balanced equilibrium between the two. In any case, the application of the CO theory to the banking industry raises doubts under a competition law standpoint, especially in light of the characteristics of that sector.

(i) *The value of “intra-industry” diversification in the banking sector.*

At a micro-economic level, AMCs and other institutional investors are beneficial to final consumers to the extent they help clients with diversifying their investments and reducing financial risks. The fact that institutional investors have in their portfolio financial institutions amplifies the positive effects of investment diversification at a wider macro-economic level. Diversification does not only occur between different financial industries where the portfolio firms held by the AMCs are active (e.g., banking, insurance), but also between different financial products offered by the institutions held by common shareholders. As a consequence, the implementation of measures that would make diversification more difficult could induce financial entities to refrain from making investment decisions, with a negative impact on various economic sectors. This is particularly true in case of important financial entities, whose failure or even a substantial prejudice to their lines of business may have a *domino* effect on other sectors of the economy. In this framework, it is evident that aggressive competition may prejudice the stability of the system. This thin equilibrium between sustainable competition and financial stability risks being jeopardized in case of a rigorous application of antitrust rules to CO. There are recent studies that empirically document that *“the increase in common ownership ... suggests a positive effect on the resilience of the individual banks and the stability of the entire financial system. Common, as compared to non-common, owners may be more willing to help an individual bank suffering a negative shock, if the bank’s financial problems have a knock-on negative effect on other banks”*.³⁹

The arguments above do not imply a more lenient application of competition law to the banking sector, whereas only a case-by-case assessment in view of the specificities of the banking sector before enforcing competition law therein. This analysis should take into account the connections between perfect competition and financial stability: the trade-off between the two is essential and there are situations in which relaxing competitive dynamics and increasing industry concentration may promote financial stability. If that is the case, from a consumer-welfare perspective, under certain circumstances concentration may be preferable to fierce competition.⁴⁰

³⁹ A Banal-Estañol, N Boot, J Seldeslachts, ‘Common ownership patterns in the European banking sector - The impact of the financial crisis’ (2022) 18(1) J. Compet. Law Econ., 135–167; see also, European Parliament, Study requested by the ECON Committee, Barriers to Competition through Joint Ownership by Institutional Investors [2020].

⁴⁰ F Allen, D Gale, ‘Competition and Financial stability’ (2004) 36(3) J Money, Credit and Banking.

From a policy perspective, the arguments above supports the value of sector-specific assessments of the risks implied by the CO theory, which seem to have been overlooked in the Banking Study. The proposal to cap institutional investors' scope of activities, such as the prohibition of holding more than 1% in (any) industry or investing in more than one firm *per* industry, should be carefully assessed before being applied to the banking sector. Even though horizontal shareholders in banking institutions led to more loose competitive dynamics – which, in any event, is controversial – CO may have contributed to financial stability of the industry. Therefore, while in the airline sector one may eventually question the positive effects of CO, which were still present and antitrust enforcers cleared airline mergers precisely on the basis of efficiency arguments, these positive effects are more prominent in the banking industry.

Furthermore, in the few cases in which competition law enforcers have addressed the possible risks to competitive dynamics due to the existence of connections among competing banks, a red flag has not been raised against horizontal shareholders. Other potential interconnections due to personal ties and interlocking directorates have been under the spotlight of the antitrust enforcers. Even with respect to interlockings, that raise a higher degree of antitrust risk, the perceived competition law concerns raised by personal interconnections among competitors have been addressed so far using the traditional antitrust toolkit or opting for *ad hoc* regulatory solutions, and not calling for the adoption of rigorous over-comprehensive measures likely those that have been proposed so far by eminent practitioners to solve the claimed competitive risks raised by CO.

(ii) Again, any role for the oligopolistic structure of the industry on pricing effects?

Like the airline industry, the U.S. banking sector has experienced a wave of consolidations during the last two decades. Such trend begun in the late '80s and continued thereafter, allowing banks to acquire a significant position within the relevant local markets.⁴¹ In such a framework, was the observed price variation of banking services caused by horizontal shareholding or rather the result of a parallel pricing behaviour in a concentrated sector in the absence of conspiracy?

Likewise the airline industry, also the banking sector has been for years on the radar of antitrust enforcers. Still, corporate governance of banking institutions has raised antitrust concerns only in limited circumstances, which mainly had to do with the presence of personal links (*i.e.*, interlocking) among competing banks, not CO. For example, in the U.S. the DOJ has for years looked at conducts in the derivatives markets, and fined individual traders and financial institutions for manipulation of the London interbank offered rate ("LIBOR").⁴² On the basis of the little information available in

⁴¹ DC Wheelock, 'Banking Industry Consolidation and Market Structure: Impact of the Financial Crisis and Recession' (2011) 93(6) Federal Reserve Bank of St. Louis Rev., 419-438. See also, FM Scherer, 'Financial Mergers and Their Consequences' [2013] Harvard Kennedy School, M-RCBG Faculty Working Paper Series.

⁴² Interest rate derivatives (*e.g.*, forward rate agreements, swaps, futures, options) are financial products traded worldwide which are used by banks or companies for managing the risk of interest

the public domain, no reference to corporate structures of the banking institutions involved in those cartels seems to have been under the spotlight of the antitrust enforcer.⁴³

rate fluctuations. They derive their value from the level of a benchmark interest rate, such as the LIBOR – which is used for various currencies including the Japanese yen (JPY) – or the Euro Interbank Offered Rate (EURIBOR), for the euro. These benchmarks reflect an average of the quotes submitted daily by a number of banks who are members of a panel (panel banks). They are meant to reflect the cost of interbank lending in a given currency and serve as a basis for various financial derivatives. Investment banks compete with each other in trading these derivatives.

For more details, 'Deutsche Bank's LIBOR settlement' [2015] DOJ press release, 15-499.

⁴³ A similar investigation has been carried out in Europe for a while. More precisely, in 2013 the European Commission fined international financial institutions for participating in illegal cartels in the markets for financial derivatives (*Euro Interest Rate Derivatives* (Case AT.39914), Commission Decision [2013]). According to the antitrust enforcer, between 2005 and 2008 some of the biggest banking entities (i.e., Barclays, Deutsche Bank, The Royal Bank of Scotland, Société Générale, Crédit Agricole, HSBC and JPMorgan) reached an anticompetitive agreement in connection with interest rate derivatives denominated in the euro currency ("EIRD"), whereas some of them were part of one or more bilateral cartels relating to interest rate derivatives in Japanese yen ("YIRD") in the period from 2007 to 2010. The EIRD cartel was implemented through information exchange among traders of different banks, who discussed their bank's submissions for the calculation of the EURIBOR (i.e., the Euro Interbank Offered Rate), as well as their trading and pricing strategies with the aim of distorting the normal course of pricing components for these derivatives. The YIRD cartels were indeed implemented by traders of the participating banks on certain JPY LIBOR submissions through exchange of commercially sensitive information. The information exchanges enabled traders to make informed market decisions on whether the currencies they had in their portfolios could be either sold or purchased. The conspiracy was led by traders, who did not hold shares within competing financial institutions, but traded currencies on their behalf. Interestingly, if one looks at the corporate structures of some of the undertakings involved in the European EIRD and YIRD cartels in the period when the contested infringement of competition was committed, will note that horizontal ownership or at least connections with the biggest AMCs already existed. However, as mentioned, no reference to any role that they may have played in connection with conducts carried out by their owned financial institutions emerge from the antitrust investigations.

In particular, considering that in 2009 BlackRock acquired Barclays' global asset management branch (i.e., Barclays Global Investors, "BGI"), it is reasonable to assume that, before 2009 and thus at least in part of the period covered by the EIRD cartel, Blackrock might still have connections with Barclays, involved in that cartel (*Blackrock / Barclays Global Investors UK Holdings* (Case COMP/M.5580) [2009]). If this held true, instead of reaching a collusive equilibrium with other AMCs like Vanguard, SSGA or Fidelity to coordinate the conducts of the participated or connected financial institutions, Blackrock opted to purchase BGI, Barclays' branch which directly competed with the biggest AMCs. The presence in the market of companies like Vanguard or SSGA was indeed valued by the European Commission as a pro-competitive element, that minimized the risk of distortion of competitive dynamics as a result of the merger in the only possible segment where the parties would have held more than 15% combined market share, i.e. the passive asset management segment.

Interestingly, Crédit Agricole and Société Générale also had relevant connections which led the two institutions to conclude a merger in 2009. They were both involved in the EIRD cartel together with Barclays, whose asset management branch was acquired by BlackRock. Nevertheless, Crédit Agricole decided to acquire sole control of the asset management branch of Société Générale, which offered several active asset management services, such as the creation and management of mutual funds and the offer of portfolio management services in direct competition with the biggest AMCs, including BlackRock (*Crédit Agricole / Société Générale Asset Management* (Case COMP/M.5728) Commission decision [2009]). In authorizing this merger, the European Commission acknowledged that the concentration of these entities was unlikely to significantly impede effective competition in the European markets for the offer of active asset management services (e.g., other important asset managers remained on the market; institutional investors retained considerable bargaining power since they could have negotiated better management fees or investment conditions with other AMCs had the merged entity increased fees or lowered performance standards; retail customers were not damaged as low barriers to expansion existed in the retail segment for asset management services). The antitrust authority also recognized that independent funds remained in the market and competed on investment returns.

In the merger assessment, as in the U.S., neither corporate governance of the relevant banks nor the structure of the banking industry seems to have played any role. Whereas the acknowledgment that third-party investment funds continued to exercise a competitive constraint is a valuable

In light of the above, considering that financial institutions produce important financial benefits at macro and micro levels and can contribute to the stability of entire sectors of the economy, a rigorous antitrust intervention is not desirable. The antitrust intervention may be indeed justified only in case of evidence of anticompetitive conduct or of corporate governance links that will more likely favor an anticompetitive strategy (e.g., interlocks).⁴⁴

2.3 The pharmaceutical industry.

The CO theory has so far also been applied to sectors where not just pricing, but innovation is a relevant competitive variable, including the pharmaceutical industry. The main study in this field claims that CO between brand and generic-drug manufacturers in the U.S. over the sample period 2003/2016 delayed the entry of generics into pharma markets, which in turn had an adverse effect on prices of pharmaceutical products (the “Pharma Study”).⁴⁵ In particular, the study looked at patent infringement lawsuits launched by originators against generics over that reference period and found that, in almost 22% of the launched lawsuits, there were common shareholders between generics and brand-name manufacturers. On this basis, the Pharma Study asserts that the probability that two drug-companies entered into a settlement agreement by which the brand manufacturer compensated the generic manufacturer to stay out of the market (*i.e.*, pay-for-delay agreement) increased when generics’ shareholders held, at the same time, stakes in the brand-name firm. To support these findings, the study reports that only a small percentage of disputes (16%) led to a trial, whereas the mean settlement rate was found to be at 43.6% and varied across federal district courts, with a dismissal rate of 33%.

In this context, the Pharma Study comes to the conclusion that CO among brand and generic drug manufacturers resulted in an increase of patent settlements. This phenomenon in turn had the effect of artificially extending the brand’s monopoly *status* beyond the expected date of generics’ entry into the relevant markets. This reasoning relies on the premise that generic manufacturers with high ownership stakes in brand companies were induced to settle disputes over validity of the brand-drug manufacturers’ patents since settlements would have maximized the overall profits of common shareholders. As a result, final consumers were

indication of the fact that the European market for asset management services is rather competitive, and evidence of collusion among the biggest AMCs (for example through their portfolio companies) has not emerged so far.

⁴⁴ This argument is further supported by the findings of a market study carried out by the UK Financial Conduct Authority (“FCA”) to identify competitive concerns within the asset management sector and eventually launch enforcement actions. In its concluding report, the FCA did not identify any concern in connection with minority shareholdings held by the biggest AMCs in competing undertakings (FCA, Final report on Asset Management Market Study [2017]). The FCA only referred to the importance of strengthening the requirements for asset managers to act in the best interests of investors and to offer high quality services in a transparent way, on the assumption that this would have increased efficiency of the UK asset management industry to make it more attractive for investors, an issue clearly different from the antitrust theory of harm underlying the CO doctrine.

⁴⁵ J Gerakosy, J Xiez, ‘Institutional horizontal shareholdings and generic entry in the pharmaceutical industry’ [2019] Tuck School of Business, working paper.

prejudiced as they had to pay drugs more than what they would have paid had the generics entered the market.

In the following paragraphs the findings of the Pharma Study will be analyzed with a focus on competition on innovation to assess the soundness of its underlying assumptions. The Pharma Study seems to have overlooked the value of competition on innovation, despite it being a key competitive parameter in the pharmaceutical industry. In addition to pricing effects, generic companies exercise competitive pressure on brand-drug manufactures by incentivizing them to engage in research and development (“R&D”) with the aim of enhancing or producing new drugs which would obtain additional patent protection and shield their market power from generics’ entry into the market. On this basis, the interconnections between patent settlements and innovation should be investigated to assess whether the former may have any positive effect on the incentive of brand-drug manufacturers to engage in R&D.⁴⁶

(i) Common ownership in the pharma industry and IP rights.

The Pharma Study touches upon one of the most debated topics by competition law practitioners, namely the relationship between dynamic competition and intellectual property (“IP”) in a context where IP rights are essential to reward companies for investing in R&D.

The relationship between pay for delay, patent protection and innovation is hence particularly complex as there may be situations in which patent settlements could have a positive impact on the incentives of brand-manufacturers to innovate when they delay market entry of infringing drugs. Moreover, a pay for delay strategy offsets costs that the parties would have incurred should they had gone to trial, with patent validity being upheld at the end of the dispute. In this complex framework, the following sections will discuss whether the starting position that antitrust enforcers should take, when assessing pay for delay in cases where common investors are present within the share capital of brand and generic-drug manufacturers should be one of skepticism, or whether the benefit of doubt should be indeed given in light of the possible positive effects on innovation that patent settlements may have – contrasting with the findings of the Pharma Study.

The Pharma Study almost overlooked the impact of pay for delay on innovation, to focus instead on pricing effects, although innovation is an important dimension over which companies compete in industries characterized by substantial R&D investments, such as the pharmaceutical sector. In case of multinational pharmaceutical companies, which in the pharma industry represent the main target of institutional investors, R&D is particularly relevant as pharma manufacturers rely more on continuous innovation than on short term financial profits. The reason is simple: research may lead to the development of new drugs; the related patent

⁴⁶ ÁL López, X Vives, ‘Overlapping Ownership, R&D Spillovers, and Antitrust Policy (2019) 127 J. Pol. Econ., 2394; M Anton and others, ‘Innovation: The Bright Side of Common Ownership?’ [2018] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099578>; P Borochin, J Yang, R Zhang, ‘Common Ownership Types and Their Effects on Innovation and Competition’ [2020] <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3204767>.

protection covering new drugs shields the brand-name manufacturer from the competitive pressure of generic companies, which in turn has a positive impact on the long-term financial profitability of that pharma company. As such, the relation between innovation and competition is key, although challenging in the context of a pay-for-delay settlement.

Against this background, there is the concern that patent settlements block generic entry and thus limit competition between the originator and the generic companies. This delay has a prejudicial effect on competition on prices since consumers may not benefit from low-cost generic drugs. However, it is also true that pay for delay safeguards patent protection in case of “strong” patents, whose validity may be still proved in court. In that scenario, pay for delay strengthens the originators’ incentives to innovate. In the absence of pay for delay, these incentives may be lower due to the risk for brand-name manufacturers of not recovering the R&D expense to produce a new drug and earn a fair rate of return as a result of the market entry of generic companies, which may challenge the validity of the original patent before its expiration. In the long term, patent protection through pay for delay could be beneficial to consumer welfare in terms of availability of innovative drugs.⁴⁷

When the originators and the generics have common owners, in order to decide whether to settle or engage in a long and expensive litigation, whose outcome is *ex ante* uncertain, common shareholders may have an incentive to assess the costs for generics to enter the market as opposed to those of the originators to innovate. This exercise is certainly complex and subject to a degree of discretion. This is further complicated by the fact that the approach of competition authorities in scrutinizing patent settlements in the pharmaceutical industry evolves over the years. In the U.S., only in recent years the authorities have opted for the application of the ‘rule of reason’ standard and, as such, for a flexible, *case-by-case* assessments of patent settlements and pay for delay.⁴⁸ In Europe, the approach of the competition

⁴⁷ Y Ding, X Zhao, ‘Pay-for-delay patent settlement, generic entry and welfare, International Journal of Industrial Organization’ (2019) 67.

⁴⁸ In 1984 the Hatch-Waxman Act, that amended the 1938 Federal Food, Drug and Cosmetic Act (FFDCA), legislated market approval for low-cost generic pharmaceuticals by ruling that, at the expiration of the originator’s patent or after having successfully challenged the validity of that patent, the first generic manufacturer filing an abbreviated new drug application was entitled to an exclusive 180-day right to market a new version of the brand medicine. Generic companies had thus an incentive to challenge brand patents because the first could enjoy the benefits of the exclusivity window, but reverse payment settlements have been used as an alternative to patent litigation. These patent settlements have thus called the attention of antitrust enforcers on the basis that they could buy off potential competitors and deprive consumers of the benefits of generics’ low-cost medical products. In this context, the U.S. antitrust enforcers have initially shown a quite rigorous attitude in the assessment of those agreements, but they have recently favoured a more cautious approach. In 2003, rejecting the strict *per se* approach upheld by the Sixth Circuit of the Court of Appeal *In Re Cardizem*, the Eleventh Circuit in *Valley Drug Co. focused on the scope of patent test (Valley Drug Co. v. Geneva Pharm. (2003) Court of Appeals, Eleventh Circuit 344 F.3d 1294)*. In particular, the case concerned a payment made by Abbott to generic companies to delay their entry into the market for drugs containing terazosin hydrochloride, that was used for hypertension diseases. In that case, the Court of Appeal held that patent settlements are valid as long as they remain within the scope of the patent, on the basis that “*exposing settling parties to antitrust liability for the exclusionary effects of a settlement reasonably within the scope of the patent merely because the patent is subsequently declared invalid would undermine the patent incentives*”. This approach was then followed by other

authorities and courts has been rigorous and these agreements are usually qualified as *by object* restrictions of competition, with the consequence that they are deemed to be illegal under antitrust law without engaging in more discretionary *by effect* analyses and hence regardless of evidence of their anticompetitive effects.⁴⁹

With respect to the core topic of this article, both in the U.S. and in Europe the relation between patent settlements and CO by institutional investors has not been assessed so far by antitrust authorities, but should it come on the radar of these enforcers, the presence of common shareholders in the share capital of originators and generic companies should not justify a too rigorous stance. In a scenario in which the originator simply tries to extend the validity of its patents in the absence of further innovation, the patent is weak, and it is likely that a court will uphold its invalidity. As a consequence, patent settlements are not functional to protect incentives to innovate and it is reasonable to assume that generic companies will incur the risk of patent litigation to enter the market. In fact, even if one assumes the presence of common (minority) shareholders in the share capital of originators and generic manufacturers, the majority of the shareholders' base of the generic company will be made up of non-common shareholders with an interest in entering the market immediately. As such, the decision as to whether to enter into a patent settlement does not rest on the presence of common

Appellate Courts, that upheld the legitimacy of reverse payment agreements as long as the patent litigation did not amount to a sham or baseless litigation.

The approach of the FTC was indeed stricter. In the 2010 Staff Study on Pay for Delay agreements, by recalling a Court of Appeal's decision ruling on the invalidity of such agreements under the *per se* category, the FTC highlighted how a strict approach had a deterrent effect on those practices in the period from 1999-2004. In the words of the FTC, since 2005 the less rigorous approach of some Courts of Appeal resulted in the increase of such settlements. Therefore, it should not be welcomed as these practices posed risks to competition.

Then, in 2012, the scope of the patent test was also judicially rejected in the *Re K-Dur Antitrust Litigation*. In that case the Third Circuit expressed a distaste for the presumption of validity of reverse payment settlements when the agreement did not go beyond the patent scope. The Court adopted a "quick look" standard, which had to be applied in light of "*the economic realities of the reverse payment settlement rather than the labels applied by the settling parties*". More precisely, a reverse payment settlement agreement that aim at delaying generics entry into the market amounts to a "prima facie evidence of an unreasonable restraint of trade", that could be rebutted by showing that the payment has not been concluded to delay entry (*In re K-Dur Antitrust Litigation* (2012) U.S. District Court for the Eastern District of Pennsylvania 686 F.3d 197).

The inconsistencies between different Circuits of Court of Appeal were finally composed by the U.S. Supreme Court, that granted *certiorari* in the *Actavis litigation* (*FTC v. Actavis, Inc.* (2013) U.S. Supreme Court 133 S. Ct. 2223). On June 17, 2013, the U.S. Supreme Court, disagreeing with the scope of patent and the quick look tests, upheld a *rule of reason* approach. In the words of the Supreme Court, while presumptive rules (e.g., quick look) are justified when "*an observer with even a rudimentary understanding of economics could conclude that the arrangements in question would have an anticompetitive effect on customers and markets*", reverse payment settlements "*do not ... meet this criterion*". They are complex agreements, and their anticompetitive nature could depend on several factors, including the size of the payment, its value in relation to anticipated litigation costs or the lack of any convincing justification.

⁴⁹ See the recent EU Court of Justice's judgment in *Lundbeck* upholding the European Commission's decision which had fined the originator Lundbeck and various generic companies for having entered into settlements of patent disputes, that had to be qualified as restriction of competition *by object* in violation of Art. 101 TFEU, simply aimed at delaying generics' entry into the market in the absence of any substantiated pro-competitive effect associated with those agreements (Judgment of 25 March 2021, *Lundbeck v Commission*, C-591/16P, ECLI:EU:C:2021:243). See also, Judgment of 12 December 2018, *Servier and Others v Commission*, T-691/14, ECLI:EU:T:2018:922; *Cephalon Inc / Teva Pharmaceutical Industries Ltd* (Case AT.39686) Commission Decision [2020].

shareholders, but rather on non-common owners representing the majority of the shareholder basis of the generics, which should be compensated for the loss they suffer as a result of the delay in entering the market.

If one indeed assumes that the strategies of the generic companies were only defined by common shareholders, even though they hold minority shareholding, one should also consider that the conclusion of patent settlements is unreasonable and irrational: why should originator companies enter into patent settlements and give up to financial resources to compensate generic companies, also (and mainly) to the benefit of non-common shareholders, to block generics from entering the market if they could obtain the same result by simply orienting the commercial strategies of these companies without incurring any cost? The premise upon which that argument rests may be hence erroneous.

It is more logical to think of patent settlements as a means to induce generic companies, subject to control of non-common shareholders, to refrain from entering the market in case of “strong” patents, but which could be still contested in court. Accordingly, even if originator and generic companies have common shareholders, no specific rules are needed to assess the possible anticompetitive effects that patent settlements among these companies may have, with the final aim of balancing IP protection and fair competition.

(ii) CO in the pharmaceutical industry and the boundaries of relevant market definitions.

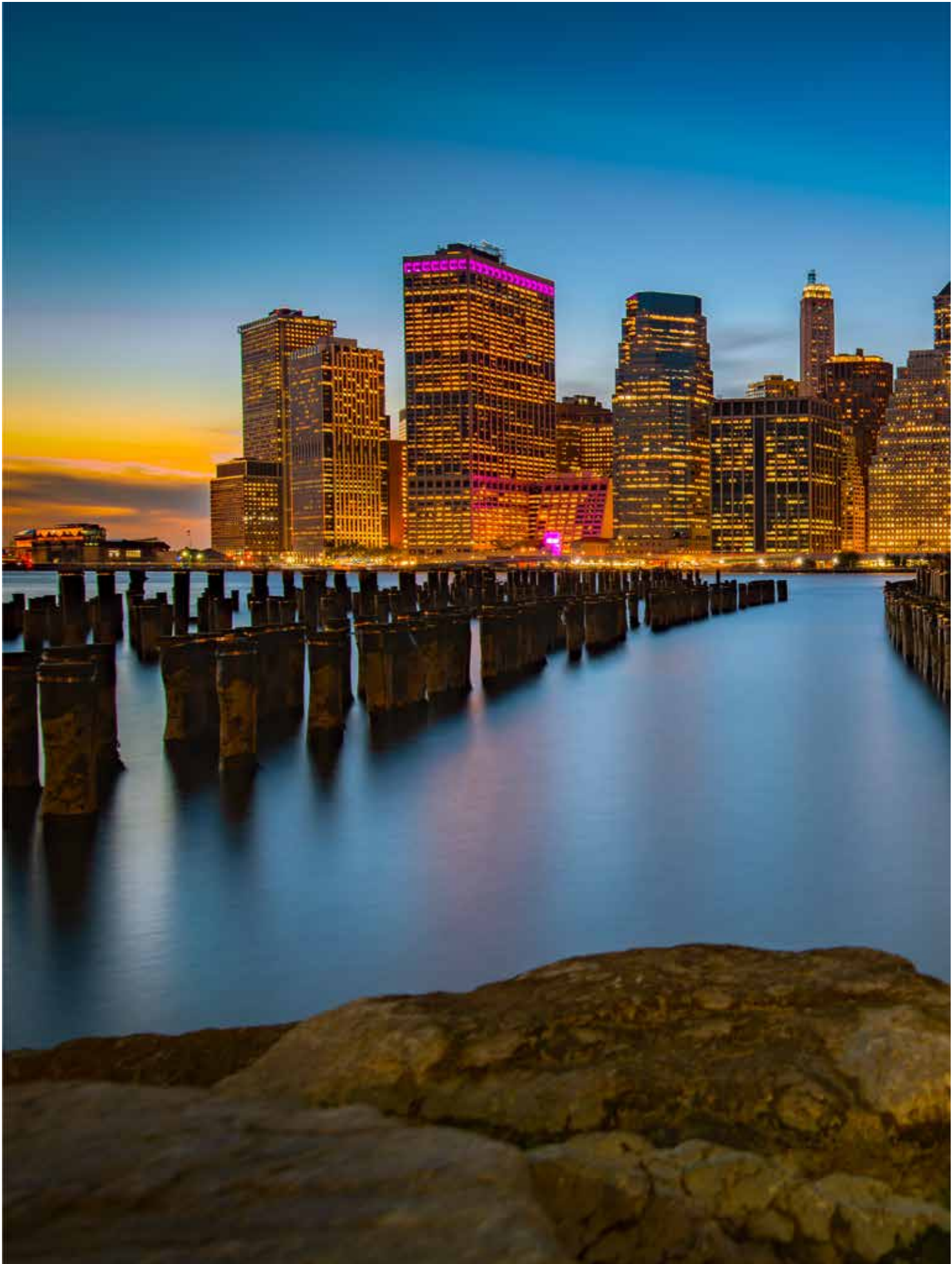
Finding an equilibrium between IP protection and fair competition is not an easy task in the pharmaceutical industry, where the same definition of relevant markets, that is a first step in competition law assessments, is tricky. This is all the more valuable in connection with the CO theory, that looks at competitive dynamics in the *industries* in which portfolio companies of common institutional investors are active, rather than preliminarily defining the relevant markets in which these minority-owned companies compete. The incorrect definition of relevant markets may lead to erroneous antitrust assessments. In addition, in the pharma sector, market definition has traditionally been controversial because of the complexity of identifying substitutable drugs from a demand side standpoint since prices are not necessarily indicative in this respect.

In light of the complexities of this industry and of the fact that prices of medicines may have little to do with industry-wide trends upon which the CO relies, the assessment of the potential anticompetitive effects due to the existence of corporate governance links in the form of common shareholding between originator and generic companies should be conducted on a *case-by-case* basis by preliminarily considering the specific relevant markets – from a competition law standpoint – where pharmaceutical companies are active, instead of relying on wide industry trends.

Conclusions.

In the preceding paragraphs the fascinating CO theory has been tested in industries where the observed increase in prices could have been caused by alternative factors (such as industry concentration) rather than to the presence of common institutional investors in the shareholders' basis of firms active within the same markets. These arguments are even more sound in case of industries, such as the airline and banking, which have been for years on the radar of the antitrust enforcers that so far have not referred to CO as a possible cause of distortive pricing effects. Similarly, there are sectors like the pharmaceutical one in which, in addition to pricing effects, industry innovation is a relevant parameter of competition, and which should be taken into account when assessing the effect of the presence of common shareholders within the share capital of brand vs. generic companies.

The complexities highlighted so far suggest, on the one hand, that the CO theory is fascinating, but it may not be well-founded because of the difficulties of identifying a *causal relation* between the presence of minority common shareholders in the corporate structures of competing firms and the claimed anticompetitive effects, which in turn imply that minority shareholders should have the ability to exercise antitrust control upon these competing firms. On the other hand, because of the inherent weakness of the CO theory and of the adequacy of the existing antitrust framework to cope with the potential competitive concerns raised by corporate structures and by mechanisms that connect independent firms, one might even more question the need to introduce radical changes in antitrust law, such as those suggested by eminent doctrine so far. The rigorous enforcement of antitrust rules against CO may be even more inappropriate if, as said, one considers the potential detrimental effects of such approach on the activities of a plethora of financial institutions, that play a fundamental role in modern economies.



SECTION II
*FOCUS
PAPERS*



The regulation of certain aspects of autonomous driving in the Italian legal system.

MARIA CRISTINA GAETA 

Lecturer in Private Law

Università degli Studi Suor Orsola Benincasa di Napoli

Abstract

The paper focuses on several regulatory issues related to road safety and data protection. Among other things, it discusses the requirements and the role of the driver, the homologation of self-driving cars and the regulation of the different types of data used and produced by autonomous driving systems, considering the different levels of automation identified in the SAE standard J3016.

The recent development of autonomous vehicles asks for regulatory intervention, in relation to road safety and privacy. Therefore, after analyzing the state of the art on road traffic regulation, the contribution proposes the analogical application of some rules relating as well as the introduction of ad hoc legislation for autonomous driving.



Keywords: autonomous vehicles; regulation on autonomous driving; data protection.

Summary: [1. Regulation on autonomous driving and the homologation of self-driving cars in Italy.](#) – [1.1. An overview on the regulation on autonomous driving.](#) – [1.2. Homologation of self-driving cars.](#) – [2. The use of autonomous vehicles.](#) – [2.1. Requirements applicable to the drivers of autonomous vehicles.](#) – [2.2. Conditions permitting activation of the autonomous driving system.](#) – [2.3. Conditions for using driverless vehicles.](#) – [3. Data protection and the processing of personal data by autonomous driving systems.](#) – [3.1. The data collected and processed.](#) – [3.2. Storage and access to the data.](#) – [3.3. Deletion of the personal data.](#) – [4. Other key issues for autonomous driving.](#)

1. Regulation on autonomous driving and the homologation of self-driving cars in Italy.¹

1.1 An overview on the regulation on autonomous driving.

In Italy there is not a regulation on autonomous driving. However, a legislative intervention in this direction is foreseen and it would follow the legislation on the experimentation of autonomous vehicles, which is already in force in Italy since 2018².

Therefore, until the possible introduction of specific legislation for the regulation of autonomous vehicles, the legislation currently applicable to autonomous driving is the following: Civil Code,³ Road Traffic Code,⁴ Consumer Code,⁵ Private Insurance Code,⁶ and Privacy Code,⁷ applied directly or by analogy.

One of the main issues relating to driving, including the case of autonomous driving, is the civil liability for car accident. In this context the main rule on road traffic liability is Art. 2054 of Italian Civil Code. It is the basic provision for civil liability for damages resulting from road traffic. However, this disposition is not sufficient to regulate all the new cases of civil liability in light of the rapid development of onboard vehicle technology.

Article 2054, para 1, of the Italian Civil Code establishes that the driver is responsible for the damage caused by the movement of the vehicle without a

¹ This work is the result of the study carried out for the Swiss Institute of Comparative Law (ISDC) as part of the Legal opinion on the regulation of certain aspects of automated driving (Italy, Spain, Sweden, United Kingdom) of March 2022.

² Smart Road Ministerial Decree 28.02.2018, Smart Road Decree, available at www.normattiva.it.

³ Royal Decree 16.03.1942, n. 262, Italian Civil Code, available at www.normattiva.it.

⁴ Italian Legislative Decree 30.04.1992, n. 285, New Road Traffic Code, available at www.normattiva.it.

⁵ Italian Legislative Decree 6.09.2005, n. 206, Consumer Code, available at www.normattiva.it.

⁶ Italian Legislative Decree 7.09.2005, n. 209, Private Insurance Code, available at www.normattiva.it.

⁷ Italian legislative decree 30.06.2003, n. 196, Code regarding the protection of personal data, containing provisions for the adaptation of national law to regulation (EU) no. 2016/679 of the European Parliament and of the Council, of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46/EC, available at www.normattiva.it.

rail guide, unless he/she proves to have done everything in his/her power to prevent the occurrence of the damage. This is a particular type of civil liability, so-called semi-objective liability, which provides for an inversion of the burden of proof with respect to the ordinary regime of non-contractual civil liability established by Article 2697 of the Italian Civil Code. In fact, pursuant to article 2054, paragraph 1, it is a task of the damaging party proving that he has done everything possible to avoid the damage.⁸

Regarding the special responsibility of the driver, it is first necessary to define his/her role. The driver is who physically controls the vehicle at the time of the occurrence of the damage. To have control means to have the controls of the vehicle, even if at the moment when the damage occurred, they were not used; therefore the driver will answer for damages caused by the vehicle even if this has been, for example, parked without handbrake on a sloping road or has been parked in the middle of a roadway. On the contrary, it is no longer considered as a driver who has given the commands to others, even if temporarily and under his/her control. Between the case in which the vehicle is considered under the control of the driver (traditional vehicles) and the one in which it is not under driver control (autonomous vehicle), there is the case of semi-autonomous vehicles where there is a driver driving the vehicle, but the driving control can be exercised by an ADAS that replaces in whole or in part to the driver in some specific driving activities, carrying out more or less important tasks depending on which it can also be limited or excluded the liability of the driver.⁹ In the case of completely autonomous vehicles,¹⁰ however, it seems logical to compare the person onboard the vehicle to passengers of a train or an airplane: as for the passenger of the train/plane there is no liability in case of an accident, so for the passenger of the driverless car will not be applicable the driver liability in the event of an accident.¹¹

In addition to the liability of the driver, it is necessary to consider that article 2054, para. 3, also provides for the liability of the owner of the vehicle or of persons equivalent to him/her. With a view to progressive automation of vehicles, we are moving further and further away from the figure of the driver while that of the owner is always central. It is a case of joint and several liability with the driver of the owner of the vehicle. The '*ratio*' of this kind of liability of

⁸ It should be noted that the burden of proof of the driver having acted diligently is valid only for damages caused to things or third parties unrelated to road traffic, instead, in the case of collision between two or more vehicles, the driver must also prove the fault of the other driver(s) (so-called presumption of equal co-responsibility, art. 2054, para. 2, Italian Civil Code). Moreover, in order to overcome the presumption of equal co-responsibility, it is also necessary to provide proof of the unpredictability of the conduct of the other driver.

⁹ Bertolini A. (2020). "Artificial Intelligence and Civil Liability", Study Requested by the JURI committee of the European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, PE 621.926.

¹⁰ Bertolini A. (2013). "Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules" 5 (2) LIT: 214 ff., specifies that even fully autonomous vehicles are object and not subject of law. Precisely these are products created by the work of man in order to satisfy certain human needs and, therefore, in the event of a defect, the responsibility would be attributed to the producer of the same.

¹¹ Bertolini A., Palmerini E. (2014). "Regulating robotics: A challenge for Europe", Workshop for the JURI committee of the European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies: 112 ff., they clarify that the problem of liability in road traffic is perhaps the most relevant issue in relation to driverless cars, as it could have a strong technology-chilling effect, delaying their placing on the market.

such subjects must be recognized in the fact that the damage depends on the circulation of the vehicle, which it falls within the sphere of freedom of action of the owner and of the other mentioned subjects who, moreover, are those who can bear the economic loss of the road accident according to strict liability principle. Anyways, the driver, the owner, and the other subjects similar to them, have a right of recourse against the producer if the vehicle accident depended on a vehicle defect.

Another case of strict liability is that sets in paragraph 4 of the same article 2054 which provides, in fact, the objective responsibility of the driver and of the other persons indicated in the same article, in case of a construction defect or maintenance defect.

Concerning the product defect, i.e. the defect of the ADAS or driving software, the strict liability of the driver and of the owner (as well as of the other mentioned subjects) competes with the product liability, according to article 2055 of Italian Civil Code (even if the sources of liability are different: contractual and non-contractual liability). Product Liability was firstly regulated in Italy by the d.P.R., 24.05.1988, n. 224 that, pursuant to art. 15 of the law 16.04.1987, n. 183, implemented the Directive n. 85/374/EEC (so-called Product Liability Directive), relating to the approximation of the laws, regulations and administrative provisions of the Member States regarding liability for damage caused by defective products, and then repealed by d.lgs. 6.09.2005, n. 206, (Italian Consumer Code), which at articles 114 and following, incorporates the provisions of the PLD.

More in details the art. 115, para 1, Italian Consumer Code (art. 2 PLD) defines as a product every movable, even if it is incorporated into another movables or immovables; therefore, fall within this category both the vehicles and the automatic devices installed on them. A product is to be considered defective, under art. 117 Italian Consumer Code (art. 6 PLD), when it does not offer the security that a person is entitled to expect taking into account the presentation of the product, the reasonable use of the product, and the time when the product was put into circulation. In fact, the assessment, to be carried out on a case-by-case basis, will take into account certain parameters which include those indicated by the art. 117 and 118 Italian Consumer Code (art. 6 and 7 PLD).

As can be seen from the definition of a defective product, the concept of defect is strictly connected to the concepts of safety of the person who uses it and of third parties. So, it is important to define if the safety standards represent a minimum or a maximum threshold of producer's liability. In general, in Italy safety standards are intended as minimal requirements, which merely allow the distribution of the product on the market. Indeed, as stated in the art. 118, lett. d), Italian Consumer Code (art. 7, lett. d), PLD), the liability is excluded only if the damage occurred because of the specific feature set by a legal rule. Furthermore, the existence of a higher level of safety standard, which has actually been achieved by other producers (so-called alternative design), may be suitable for configuring producer's liability even though he had respected the safety standards.

Having defined the notion of product and the one of defect, it is now necessary to understand what is meant by producer. About that art. 115, para.

2 *bis*, Italian Consumer Code (art. 3, para. 1 and 2, PDL), defines the producer of the finished product, that of a component part and also the producer of the raw material. Therefore, in the light of the existing EU legislation, a producer of an electronic device onboard the vehicle is a producer, as well as the producer of a vehicle, being it a traditional vehicle or a self-driving car. However, only the professional producer should be considered as a producer, on the basis of the fact that it is opposed to the consumer, the weak part of the relationship, which acts just like a non-professional.

Under art. 114 Italian Consumer Code (art.1 PLD), the producer is liable, regardless of his fault, for damages caused by his defective products (so-called strict liability or no-fault liability). The choice for the producer's strict liability derives from the fact of placing the risk on the subject who can better bear it because in the relationship between the producer and the consumer, the first one is economically stronger and also he can transfer (partially or integrally) the production costs and risks to the end-user, through the product's price.

With regard to the burden of proof, the art. 120, Italian Consumer Code, (art. 4 of the PLD) provides that the same is on the damaged party, which must prove the defect, the damage and the causal link between the defect and the damage, while the producer must prove the exemption of liability. The *ratio* of this rule limiting the liability of the producer is probably the indefectible need to protect also the strong party of the relationship, as it depends on him the innovation in the industrial sector and in particular that of new technologies. In fact, if the liability of the producer was even greater of that provided, he would not choose to introduce new technologies into the market as the same could result in excessive responsibility for him.

Coming to the insurance profile in Italy, mandatory insurance had already been established by article 1 of the law no. 990/1969 (no more in force),¹² for which every vehicle in public areas had to be protected by an insurance policy such as to cover the damages caused to third parties involved in a possible claim, up to a certain threshold. The compulsory insurance coverage fell only when the vehicle was demolished, with consequent radiation from the Public Automotive Registry.

The 1969 law has undergone various updates and modifications and has been definitively replaced by the current Italian Private Insurance Code, repeatedly modified. The Italian Private insurance code, in confirming the compulsory insurance, has also introduced a series of innovations, among which one of the most important is the direct compensation (article 149, Italian Private insurance code).¹³ It provides that, in specific cases, the injured person can go directly to his insurance company to get compensation for damages in case of an accident caused by the other party, without having to request the payment of damages to the company of the damaging party. This direct compensation procedure operates only if: (1) the motor vehicle accident occurred in Italy, in the Republic of San Marino or in the Vatican State;¹⁴ (2) it involved only two vehicles, both identified, insured and registered in Italy; (3)

¹² Law 24.12.1969, n. 990, civil liability insurance for road accidents (not in force).

¹³ Art. 18, Dir 2009/103/EC.

¹⁴ Art 34, par 1, CARD.

and if there has been damage to property and/or persons, but minor value.¹⁵ It seems clear, therefore, that this is an exception to the third party scheme, and that, when applicable, operates according to the scheme of the first-party insurance, even if the requirements are different and far more specific for the direct compensation than the first-party insurance.

In addition, can take advantage of the direct compensation only ones who are insured with an insurance company belonging to the Direct Compensation Agreement (DCA, in Italian CARD), pursuant to art. 13 of the D.P.R. n. 254/2006.^{16 17}

For damages caused by the insured to third parties, the insurance company, after collecting the insurance premium,¹⁸ it replaces the insured by paying the damages caused by him. The damages of which the driver is liable, and possibly also the other subjects expressly provided for in article 2054 of the Italian civil code, are those caused «to people or things». In the formula adopted, no distinction is made between people and things transported or not, but people and things transported are of course included also by Judicial Decisions.¹⁹ Moreover, if the damage derives from the collision with another vehicle, the person transported may also act against the other driver assuming an equal responsibility of the parties pursuant to article 2054, paragraph 2, Italian Civil Code. In addition, the third party is entitled, in the presence of a transport contract, to act against the driver for damages stemming from contractual civil liability, even in the absence of a tort claimed.²⁰

In case of autonomous vehicles, it is clear that the producer can bear the economic risk of damage, even better than the owner of the vehicle, in particular by providing an *ad hoc* professional insurance. In order to not distort the market and frustrate any car manufacturer which wishes to produce automated vehicles, the cost of the manufacturer insurance should be spread between the producer, who get the insurance coverage and the owner of the vehicle who pay the price of the vehicle, which is proportionally augmented covering a part of the insurance policy cost (but the owner effectively buy more performing vehicle even though more expensive).²¹

More concretely, up to level 3, and maybe 4, of driving automation, would operate the traditional insurance scheme, which foresees the insurance policy of the owner of the vehicle. Obviously, all producers have their own

¹⁵ Article. 149 Italian Private insurance code refers to the physical damage suffered by the non-responsible driver if it is contained within the limit set by article 139 Italian Private insurance.

¹⁶ D.P.R., 18.07.2006, n. 254, regulations governing the direct compensation for damages arising from road traffic.

¹⁷ In other words, these companies must establish a specific office, Company Service Reference Conventions Reference (SARC), for the management of the reports relating to the CARD between the member companies. The SARC also manages the relationships that derive from other agreements related to motor vehicle dealings, such as the Third-Party Transports Convention (CTT). Foreign insurance companies, on the other hand, must apply for membership of ANIA (Italian National Association of Insurance Companies) pursuant to Article 2 CARD.

¹⁸ The insurance premium is the amount that the insured corresponds to the insurance company to obtain insurance coverage.

¹⁹ In the past, on the contrary, a restrictive interpretation of the norm was preferred, for which people and goods transported as unrelated to vehicle circulation.

²⁰ In Italy, the transport contract is governed by articles 1678 ff., Italian Civil code.

²¹ According to an authoritative literature we could even talk about 'absolute liability' (which came from the common law legal system) that is even stricter than the objective liability, as there is the only proof that the fact was not unlawful.

professional insurance that is used to compensate the damage, if this derives from a defect of an ADAS or the software of the vehicle (as already happens for the defects of traditional vehicles). With the increasing of automation level and, therefore, of artificial intelligence, liability is more transferred to the producer. This is the case of automation level 4 and 5, where, however, the joint and several liability or the exclusive liability of the owner of the vehicle, called to compensate the damage with his own insurance, can be invoked.

In order to always guarantee damages to the injured person, then, it is necessary to provide for an *ad hoc* fund on which he or she can have recourse in a residual way, when it is not possible to identify the tortfeasor and/or his insurance. This fund should be European, since most vehicle accidents involve subjects or objects belonging to different Member States and are therefore cross-border. Moreover, the fund, so determined, could be increased by a government tax on autonomous vehicles and entrusted to the management of a specific insurance company, as already done for the so-called Guarantee Fund for Victims of the Road.²²

Once the analysis of the existing legislation in Italy on the liability of the driver, the owner and the subjects equivalent to him, as well as that of the liability of the producer is concluded, it appears clear that the same can be applied up to the intermediate automation level (up to level 3 of the SAE standard J3016).²³ However, for the subsequent levels of automation, a modification of the existing legislation or even the introduction of an *ad hoc* one should be provided.

In order to be able to assess which is the right way for regulating autonomous vehicles, it is necessary to test them on the road, as it is not possible to regulate a legal case that is not known.

For this reason, in Italy in 2017 with the introduction of the law of no. 205/2017 (Art 1, para 72), that authorised road testing of 'Smart Road' and connected driving solutions.²⁴ The text of the law called for the introduction of a decree of the Minister of Infrastructure and Transport for the implementation methods and operational tools of the experimentation.

For this reason, in 2018 was published the Ministerial Decree on smart road²⁵ that had a dual purpose. On the one hand, it aims to promote the technological adaptation of the infrastructures according to the 'Smart Roads rules', in line with the European and International requirements. On the other hand, the

²² The Guarantee Fund for Victims of the Road is a compensation body established in implementation of the Strasbourg Convention of 1959 and regulated by the Italian Private Insurance Code in order to compensate: (a) damage caused by an unidentified vehicle or boat; (b) damage caused by a vehicle or a boat identified but not covered by insurance; (c) damage caused by a vehicle or a boat that is insured with an insurance company that at the time of the accident is in a state of compulsory winding up; (d) damage caused by a vehicle placed in circulation against the owner's will (e.g. theft); (e) claims caused by vehicles sent to the territory of the Italian Republic by another State of the European Economic Area; (f) accidents caused by foreign vehicles with a licence plate that does not correspond or no longer corresponds to the same vehicle.

²³ SAE standard J3016, 'Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles' of 2014 (revised in 2016 and then in 2021, but the automation levels are the same). More details are available here: <https://www.sae.org/blog/sae-j3016-update>

²⁴ Italian Law of 27.12.2017, no. 205, available at www.normattiva.it.

²⁵ Ministero delle Infrastrutture e dei Trasporti, Decree of 28.02.2018, on the implementation methods and operational tools of road testing of Smart Road solutions and connected and automatic driving, available on www.gazzettaufficiale.it.

decree had the objective to guarantee and promote the autonomous and connected vehicles tests, in consideration of the possibility that autonomous vehicles will soon be introduced into the market. In particular, the Decree introduces the role of the supervisor (art 1, para 1, let. J and art. 10), starting from the assumption that in the highest automation level there is not a real driver but only a supervisor who must be able to resume the control of the vehicle if requested.²⁶

1.2 Homologation of self-driving cars.

Art. 46 of the Italian New Road Traffic Code qualifies: “*vehicles, all machines which can flow on the roads driven by men*”. Only vehicles that have this characteristic can be homologated according to the ordinary procedure of homologation, provided by art. 75-78, New Italian New Road Traffic Code as well as by Ministerial Decree 28.04.2008.²⁷

However, it should be noted that Italy signed the Vienna Convention of 1968²⁸ and therefore will be called upon to adapt to the new provisions which will be provided by the entering in force of the last amendment of the Vienna Convention, that will regulate the automated driving. In particular art. 46 of the New Italian Road Traffic Act (but in general should be revised part of the New Italian Road Traffic Act) should be modified in order to include the prevision of art. 34 *bis* of the Vienna Convention on the requirement according to which each vehicle must have a driver is considered satisfied when the vehicle uses an automatic driving system compliant with national technical regulations and any applicable international legal instrument and to the national legislation governing the functioning.

The ordinary procedure of homologation provides that the vehicles are subject to the verification of the identification data and their correspondence to the technical prescriptions and to the constructive and functional characteristics foreseen by the New Italian Insurance Code (art. 75, para. 1, New Italian Road Traffic Code). Furthermore, the Minister of Transport establishes with its own decrees specific rules for the national approval of systems, components and technical units, as well as the suitable procedures for their installation as elements of replacement or integration of vehicle parts, on types of cars (art. 75, para. 3 *bis*, New Italian Road Traffic Code). The assessment may concern single vehicles or groups of specimens of the same type of vehicle (art. 75 para. 2, New Italian Road Traffic Code).

In compliance with art 76, New Italian Road Traffic Code, the competent department of the Ministry of Transport after completing the assessment

²⁶ For a more in-depth analysis on the civil liability in relation to self-driving cars allow me to refer to Gaeta M.C. (2019), Liability rules and self-driving cars: the evolution of tort law in the light of new technologies, Napoli, Editoriale Scientifica (ES).

²⁷ Italian Ministerial Decree 28.04.2008, on the transposition of Directive 2007/46/EC of the European Parliament and of the Council of 5.09.2007, relating to the approval of motor vehicles and their trailers, as well as systems, components and technical units intended for such vehicles and repealing the Ministerial Decree 2.05.2001, no. 277, Provisions concerning the homologation procedures for motor vehicles, trailers, agricultural machinery, operating machinery and their systems, components and technical entities, available at www.gazzettaufficiale.it.

²⁸ Vienna Convention of Road Traffic of 8.11.1968

pursuant to art. 75, New Italian Road Traffic Code, issues the approval certificate to the vehicle manufacturer (or groups of the same vehicle).

After the issue of approval certificate certifying the existence of the eligibility requirements for circulation, the vehicles are subject to homologation, carried out on a vehicle prototype, according to the procedures established by Decree of the Ministry of Transport 28.04.2008. The same decree indicates the documentation that the interested party must exhibit in support of the application for approval (Article 75, paragraph 3).

Concerning autonomous vehicles, the possibility to be homologated according to the ordinary procedure, depends on the level of automations as classified by the SAE J3016 Standard of levels of driving automation).²⁹ Until level 2 of automation, the vehicle is driven by the men, so it is clear that traditional homologation rules can be applied to them. Coming to level 3 of automation, this is the first level of automation in which the driving software is driving itself, but the driver has to be able to resume the control of the vehicle if asked by the driving features. For this reason, it is possible to consider that ordinary homologation procedure can be applicable also for level 3 of automation. As a matter of fact, vehicles characterised by this level of automation are already on the market and has been homologated according to the ordinary procedure.

Some doubts about the applicability of the ordinary homologation procedure could arise with reference to level 4 of driving automation, in which the cases of human intervention are significantly reduced or completely eliminated. According to this thesis pedals and steering wheel should be installed, but part of the literature considers that already for level 4 of automation they are not mandatory. This means that the homologation procedure should provide more requirements for homologation, concerning ADAS and, in general, to driving software.

Having reached level 5 of automation, i.e. to completely autonomous vehicles it is not possible to apply the ordinary homologation procedure, because the figure of the human driver disappears.

This means that cannot be applied to fully autonomous vehicles (self-driving cars) in the definition by art. 46 of the new road traffic code, in particular because they are not driven by men. This implies that, currently, the autonomous vehicle cannot be homologated according to ordinary homologation procedure in force in Italy.

However, Italian legislation provides the approval of experimental vehicles, such as the automated vehicles (level 4 ad 5 of driving automation), which are still been tested in Italy, before their introduction on the market. In case of experimentation, the ordinary procedure can be passed by the art. 9, Ministerial Decree n. 277/2001. Indeed, a producer can ask the Italian Ministry of transport to do not applicate the legislation for the homologation “when the exception is required, for experimental reasons” (Art. 9, para 1, let b). The same article defines the homologation for experimental reasons as “temporary homologation” (Art. 9, para 2). Temporary homologation can eventually be

²⁹ SAE standard J3016, ‘Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles’ of 2014 (revised in 2016 and then in 2021, but the automation levels are the same). More details are available here: <https://www.sae.org/blog/sae-j3016-update>

turned in a final homologation if the experimentation gets positive results (art. 75, para 5, Italian Road Traffic Code).

Another way to obtain the homologation of a vehicle in Italy is to ensure that the vehicle gets the ordinary homologation in der country and then that is recognised in Italy, on condition of reciprocity. Therefore, ordinary homologation can be released to autonomous vehicles that gets the homologation in a Country where Italy recognises the homologations on condition of reciprocity (Art. 75, para 5, New Italian Road Traffic Code). However, there is still the issue of the circulation of these vehicles in Italy, when the autonomous driving mode is active, because the Italian legislation allows this mode of driving only for experimental purposes in the Smart Road Decree (D.M. 2802.2018).

Concerning the experimentation phase, according to art. 9, para 3, of the Ministerial Decree of 28.02.2018 (c.d. Smart Road Decree),³⁰ the approval for the experiments could be released only to the vehicles which already gets the homologation in the version without automated systems technology. The application for the authorisation must contain the documents listed in the art. 11, of the same D.M. 28.02.2018. Furthermore, the authorisation is issued for one or more vehicles, with reference to each of which the owner is indicated, belonging to the same class and category pursuant to art. 47 of the New Italian Road Traffic Code, equipped with automatic driving technologies, with similar functional performances and able to guarantee an identical level of safety on the road. Following the authorisation, the vehicles are entered in a special register kept by the authorising subject and are supplied with a special authorisation mark for experimentation (VGA standing for 'Veicolo sperimentale a guida autonoma'), the characteristics of which are set out in Annex B of the Smart Road Decree,³¹ which must be displayed on both the front and rear side of the vehicle, during the experimental activity (art. 9, para. 4, M.D. 28.02.2018).

³⁰ Italian Ministerial Decree 28.02.2018, Implementation methods and operational tools of road testing of Smart Road solutions and connected and automatic driving.

³¹ Annex B of the Ministerial Decree 28.02.2018 is available here: https://www.gazzettaufficiale.it/do/atto/serie_generale/caricaPdf?cdimg=18A0261900200010110001&dqu=2018-04-18&art.dataPubblicazioneGazzetta=2018-04-18&art.codiceRedazionale=18A02619&art.num=1&art.tiposerie=SG

	VEICOLO SPERIMENTALE A GUIDA AUTOMATICA  Ministero delle Infrastrutture e dei Trasporti Dipartimento per i trasporti, la navigazione, gli affari generali e il personale Direzione Generale per la motorizzazione
Contrassegno numero:	
Scadenza:	

Front side of the VGA - Annex B of the Smart Road Decree

Ragione sociale del titolare dell'autorizzazione Autorizzazione n. Del: Numero di telaio del veicolo autorizzato:	Il presente contrassegno certifica che il veicolo è autorizzato a circolare sperimentalmente sulle strade pubbliche italiane, con le limitazioni indicate nell'autorizzazione, ai sensi del decreto del Ministro delle infrastrutture e dei trasporti del 28 febbraio 2018 Durante le prove sperimentali, il presente contrassegno deve essere apposto sia sul lato anteriore che in quello posteriore del veicolo in modo tale che il recto sia chiaramente visibile per i controlli

Back side of the VGA - Annex B of the Smart Road Decree

The vehicles authorised for experimentation circulate, during the experimental activity, with a test licence plate issued pursuant to the decree of the Italian President of the Republic n. 474/2001 (art.9, para 5, M.D. 28.02.2008). The authorisation refers to the execution of experiments on one or more road areas, with the identification the specific road infrastructures indicated by the applicant after having obtained the authorisation from the entity that owns the road (Art. 9, para. 6, M.D. 02.28.2008).

Finally, with regard to the competent authorities for the authorisation of vehicles experimentation and their homologation, the competence has always been of the Ministry of Infrastructure and Transport. However, in the light of the goals of the European Union that aim at the development of sustainable technology, which is particularly important in the field of transport the Ministry of Infrastructure and Transport has become the Ministry of Infrastructure and Sustainable Mobility. (www.mit.gov.it).³² This is currently the competent authority in the homologation and testing of autonomous vehicles.

2. The use of autonomous vehicles.

2.1. Requirements applicable to the drivers of autonomous vehicles.

According to New Road Traffic Code, the requirements for the drivers of the traditional vehicles are stated by New Road Traffic Code and are two: (i) the driver must be suitable for physical and physiological requirements (art. 115, para. 1); (ii) the driver must comply with the age requirements that for driving a traditional car are 18 years old according to certain limits of weight as will see below (art. 115, para. 1, lett. c)).

The driving licence is provided by the New Road Traffic code which states that carl licence B is needed for driving a car whose maximum authorized weight does not exceed 3.500 kg and it is designed and built to carry no more than eight people in addition to the driver (art. 116, par. 3, let. f).

The aforementioned requirements are the main requirements for driving traditional vehicles and it is believed that they can also be applied to semi-autonomous vehicles, up to level 2 of the driving automation level according to the SAE J3016 Standard of levels of driving automation. Indeed, according to SAE J3016 Standard of levels of driving automation the driver has the main lateral and longitudinal driving task and the ADAS constitute valid support for the driving activities. As expressly provided by the SAE International for levels 0, 1 and 2 of driving automation, the driver is driving the vehicle whenever the driver support features are engaged, even if he/her is off the pedals and is not steering. So, it is clear that for this minimum level of automation the driving task remain the same as the traditional vehicles and at the same way the driver requirement remains unchanged.

Reaching an intermediate level of automation, i.e. level 3 of automation the driver is not driving when the automated driving features are engaged, even if he/she is seated in the driving seat. However, in level 3 of automation are limited the cases in which the driving software is driving itself and, in any case, when the driving features request, the driver must drive the car. For this reason, is acceptable that for level 3 of automation the driver requirement remains unchanged, and this is also what is currently happening in the practice as vehicles with level 3 of automation are already on the market in Italy.

Contrariwise, it would be possible to consider an amendment of the driving license requirements for level 4 of vehicle automation in which the main

³² Prime Minister Decree (D.P.C.M.) 23.12.2020, n. 190, art. 6, no. 3, lett b), available at www.normattiva.it

longitudinal and lateral driving functions are entrusted to the vehicle and the driver has more a supervisor role. In level 4 of automation, indeed, the driver/supervisor must be able to understand driving technologies and interact with them according to the principles of the human-machine interface (HMI).

Anyhow, the current driver requirement cannot be applied to vehicles with level 5 of automation (self-driving cars), this kind of vehicles are known for the possibility of transporting people considered passenger of the vehicles not driver. For this reason, it is clear that the requirements for drivers cannot be applied to non-drivers. Furthermore, one of the strengths of autonomous vehicles is precisely that of being able to transport minors or people with physical or physiological disabilities and therefore they do not have the requirements of the driver as provided for by art. 115 of the New Italian Road Traffic Act.

Nevertheless, there are rules applicable by analogy to the vehicles level 5 of automation, such as the provision which requires to display the letter "P" on the rear side of the vehicle (stand as 'beginner') on the vehicle for the new drivers (art. 122, para 4, New Road Traffic Code). The same provision is also provided for the experimental autonomous vehicle which, according to art. 9, para. 4, M.D. 28.02.2018, should display the authorisation mark for experimentation (VGA standing for 'Veicolo sperimentale a guida autonoma') on the rear side of the vehicle.

The *ratio* is to advise other drivers to drive carefully in respect to the beginner. Equally, the automated vehicles should display the mark "AV" to advise other drivers that that vehicle is fully autonomous.

The need to affix the mark AV on the rear side of the vehicle would be necessary only until the complete transition to level 5 automation vehicles as at that level of automation they would communicate with each other via sensors and therefore it would no longer be necessary to affix AV.

Reaching this maximum level of automation also pedestrians would be aware that all vehicles on the road are self-driving and therefore it would not be necessary to indicate them the AV acronym.

2.2 Conditions permitting activation of the autonomous driving system.

The identification of the conditions that allow the activation of the automatic driving system depends on a preliminary analysis of the relationship between the driver and the vehicle, known as the human-machine interface (HMI) or, more precisely, a human-robot interaction (HRI) analysis.³³ This is a behavioural analysis based on the cognitive psychology of the relationship between man and the robot (the autonomous vehicle in the case of this report),

³³ The HRI, sub-category of the human-machine interface (HMI), is fundamental both for the identification of different levels of automation and for vehicle connection levels, since these are directly proportional to the increase in automation. On the basis of these behavioural studies it is possible to evaluate the effectiveness of the legislation and the adequacy of the protections it contains, drawing the necessary conclusions. For a more in-depth study of HMI see D. Sidobre and others, 'Human-Robot Interaction', Siciliano B. (ed.), *Advanced Bimanual Manipulation*, in *Springer Tracts in Advanced Robotics*, LXXX (Springer 2012), 123 ff.. On cognitive law in general and on behavioural study in general see L. Arnaudo, 'Diritto cognitivo. Prolegomeni a una ricerca' (2010) 1 *Politica del diritto* 101 ff.; B. Lurger, 'Empiricism and Private Law: Behavioral Research as Part of a Legal-Empirical Governance Analysis and Form of New Legal Realism' [2014] *Aust Law Jour.* 19 ff..

and is part of the well-known human-machine interface (HMI) analysis. The results obtained by HRI analysis will have to be deepened from a legal point of view.

On the basis of the human-machine relationship (HMI or MRI), automation levels have been classified by several authors and usually all they are based on the level of onboard technologies intervention on human driving. However, in 2014 SAE International published the first international standard J3016 on driving automation, then revised in 2016 and again in 2021, which has defined six different automation levels. The automation levels identified by the SAE international standard are based on the level of driver's intervention in driving activities, which decreases proportionally as the vehicle's automation increases. They are: (L0) no automation, (L1) driver assistance, (L2) partial automation, (L3) conditional automation, (L4) high automation e (L5) full automation.

In the level zero (L0) there is no automation but the driver constantly has the control of the vehicle; however, the vehicle is equipped with 'driver assistance' systems which helps the driver.³⁴ In level one of automation (L1), i.e. 'assisted automation', also called 'hands on', driver continuously perform longitudinal and lateral driving tasks, and the few residual skills are performed by the vehicle.³⁵ In 'partial automation' or 'hands off' (L2) the driver have to monitored the dynamic driving task and the driving environment at all time.³⁶ Level three of automation (L3), is the 'conditional automation' or 'eye off' level, where in time the vehicle system requires the driver to take the control when it is necessary; it means that the driver does not need to monitor the vehicle driving task (e.g. in L3 driver can send a message or eat a meal) and the surrounding environment at all times, but he /she has to be able to resume the control of the vehicle when is asked by the driving.³⁷ 'High automation' (L4) is the immediate development of 'conditional automation' level and follow the same division of driving tasks between the driving system and the driver; the difference lies in the fact that the cases in which the driver must intervene are reduced only to anomalous cases (i.e. in L4 driver can watch a movie and even sleep).³⁸ According to this thesis pedals and steering wheel should be installed, but part of the literature consider that already for level 4 of automation they are not mandatory. Finally, in 'full automation' level (L5) all the tasks are performed by the vehicle and no driver is requested. For this reason, in level five of automation the role of the driver disappears completely.³⁹

³⁴ Examples of 'driver assistance' for level 0 of the SAE Standard J3016 are: automatic emergency breaking, blind-spot warning, lane departure warning, cruise control.

³⁵ Examples of 'assisted automation' for level 1 of the SAE Standard J3016 are: lane centering or adaptive cruise control.

³⁶ Examples of 'partial automation' for level 2 of the SAE Standard J3016 is lane centering and adaptive cruise control at the same time.

³⁷ Example of 'conditional automation' for level 3 of the SAE Standard J3016 is the traffic jam chauffeur. A concrete vehicle characterized by 'conditional automation' is Audi A8 Luxury Sedan. This car is equipped with Traffic Jam Pilot, that takes full control of all aspects of driving in slow-moving traffic at up to 60 kilometres per hour. This driving function works only on highways with a physical barrier separating one stream of traffic from oncoming traffic.

³⁸ Example of 'high automation' for level 4 of the SAE Standard J3016 is local driverless taxi.

³⁹ Example of 'full automation' for level 5 of the SAE Standard J3016 are the same as level 4 but the driving feature can drive everywhere in all conditions.

Thus analysed the relationship between the driver and the vehicle, it is possible to investigate the condition permitting the activation of the automated driving system, as well as the obligations of the driver/supervisor of the autonomous vehicle when the driving system is active, in relation to the high level of automation (i.e. level 4 and 5 of driving automation).

About the condition permitting the activation of the automated driving system, currently the Italian legislation does not provide a specific regulation concerning the activation of driving systems. Indeed, in practice, in Italy is allowed the activation of the automated driving system up to level 2 of automation according to the traditional circulation of vehicles. For level 3 of automation, there are both structural limitations of the vehicle and limitations relating to road characteristics. About the first point, the vehicle can drive in autonomous mode only within 60 km/h; with regard to the second point, the vehicle can drive in this mode only on certain roads. Indeed, the vehicle with level 3 of automation should be compliant with the international standard UN-ECE R-157,⁴⁰ in force since 2021, which for the moment allows vehicles equipped with this technology to drive in automatic mode only on separate carriageways without pedestrians or cyclists, without exceeding 60 km/h. The data stored in the navigators' maps unlock the system when they recognize that they are on an allowable stretch and speed. When these sections end, or in the presence of danger, the ADAS inform the driver to resume the control of the vehicle and, failing that, pull over and stop the vehicle. However, this technology is only permitted if it complies with the laws of the country in which the vehicle is to be used and Italy does not have adequate legislation for level 3 automation.

For the high level of vehicle automation (levels 4 and 5), there is not a regulation on conditions permitting their activation but currently their circulation is admitted only for experimental purposes in specific smart roads equipped with adequate technical infrastructure.

With regard to the obligations of the driver of the autonomous vehicle, a first distinction should be made between the cases in which the vehicle is driven by the driver, and that in which the vehicle is driven by the driving system. In the first cases the driver should comply with the obligation provided for the traditional driving that are stated by Title V of the New Italian Road Traffic Code (art. 140 - 193). Reaching a medium level of automation, i.e. level 3, it is desirable that further obligations are foreseen for the driver in addition to the traditional one, relating to his/her interaction with the ADAS and their understanding. This means that these further obligations should be related to the role of the supervisor that has the function to supervise the driving task performed by the vehicle driving system.

For level 4 of automation and, of course for level 5 of automation, the obligation should change and should be more related to the supervision of the vehicle and to the role of the passenger onboard the vehicle.

Nowadays in Italy a specific regulation on autonomous vehicles is foreseen only as part of the experimentation of the same in testing situations. It is the

⁴⁰ More information on international standard UN-ECE R-157 are available here: <https://unece.org/sustainable-development/press/un-regulation-automated-lane-keeping-systems-alks-extended-trucks>

D.M. 20.02.2018 on the implementation methods and operational tools of the on-road testing of smart road and connected and automatic driving solutions⁴¹ This regulation can be used as a basic prevision to be applied by analogy also in the cases of non-experimentation, obviously with the necessary precautions that differentiate the two cases and that the legislator must consider when will provide for regulation for autonomous vehicles in Italy.

More in detail, concerning the condition permitting the activation of the automated driving system, art. 12 of the Smart Road Decree, states the characteristics of autonomous driving for the admission to testing: (a) guarantee, in all conditions, compliance with the rules referred to in Title V of the New Italian Road Traffic Code and, in general, operate in such a way as to do not constitute a danger or hindrance to traffic; (b) be able to interact safely with all possible road users, including the weakest and most vulnerable users such as people with reduced mobility or disabilities, children, pedestrians, cyclists and motorcyclists; (c) be suitable at all times to allow the switch from the automatic mode to the manual mode, on the action of the supervisor; (d) be equipped with intrinsic safety protections suitable for guarantee data integrity and communication security, as well as to prevent unauthorised access and, in any case, neutralise its harmful or dangerous effects; (e) be able, for the entire duration of the tests, to record detailed data with a frequency of at least ten hertz and such from include at least: (1) time elapsed since the beginning of the recording, coinciding with the beginning of the experimentation; (2) automatic or manual current driving mode; (3) date, time, position in WGS84 coordinates and instantaneous speed; (4) instantaneous acceleration; (5) distance travelled from the start of the trial; (6) activation of commands for the lateral dynamics of the vehicle; (7) activation of commands for the longitudinal dynamics of the vehicle; (8) number of revolutions per minute of the engine, or other indicator equivalent; (9) gear ratio engaged, or other equivalent indicator; (10) current value of the yaw, roll and pitch angle; (11) use of lighting and signalling devices visual and acoustic; (12) data acquired from the sensors forming part of the object system evidence; (13) any V2V and V2I messages received and transmitted.

About the driver/supervisor requirement, art. 10 of the Smart Road Decree provide specific requirements for the role of the supervisor that should be added, if applicable, to the provision of Title V of the New Italian Road Traffic Code. The requirement provided by art. 10 of the Smart Road Decree are: (i) have the driving license for at least 5 years, (ii) has successfully passed a safe driving course or a specific course for self-driving vehicle experimenters at an accredited body in one of the countries of the European Union, (iii) has conducted tests on automated vehicles in a protected site or on a public road, even abroad, as long as in a State where the testing of automated vehicles is regulated, for a mileage of at least one thousand kilometres, and (iv) possesses the necessary knowledge, adequately documented, to take part in the tests as a supervisor (art. 10, para 1, D.M. 20.02.2018). Furthermore, the supervisor must be able to promptly switch between driving in automatic mode to driving in manual mode and vice versa supervisor (art. 10, para 2, D.M. 20.02.2018).

⁴¹ Italian Decree 28.02.2018, Implementation methods and operational tools of the on-road testing of Smart Road and connected and automatic driving solutions

2.3. Conditions for using driverless vehicles.

The conditions for using autonomous vehicles on the public roads are strictly related to the development of adequate driving infrastructures in order to be able to appropriately implement the three types of driving connection currently existing: vehicle to device communication (V2D); vehicle to infrastructure communication (V2I); vehicle to vehicle communication (V2V).

Autonomous vehicles are often defined as connected and automated vehicles to emphasize their ability to connect to the network. In some limited cases the connection can take place via Bluetooth, (e.g. communication between the vehicle and a smartphone), but most of the communications require an Internet connection. In fact, through the internet connection, vehicles can be put in communication with devices (eg. smartphones), with the same infrastructures (eg. traffic lights) and with other (semi) autonomous vehicles. The level of vehicle communication is directly proportional to the level of automation of the vehicles, even though connectivity is just one of the requisites needed to achieve complete automation of vehicles.

Internet development has been greatly enhanced by the extension of this network to the world of objects, a phenomenon known as the Internet of Things (IoT). It is an evolution of the Internet network, thanks to which the objects interact with each other, through sensors and without human intervention, exchanging data and accessing information stored in databases. This information architecture has been defined as a network that connects physical or virtual objects that become recognisable and acquire intelligence through the ability to communicate data about oneself and on the environment around them. For this reason, such objects are defined as intelligent objects. Currently included in this category are incredibly disparate kinds of objects, including ADAS or driving software. Today there are so many smart things that the concept has moved from "Internet of Things" (IoT) to "Internet of Everything" (IoE, that applied to autonomous vehicles domain is Vehicle to Everything - V2X).⁴²

In this regard, on 28.02.2018 has been published the Smart Road Decree⁴³ According to art. 3 the Smart Road Decree aims to promote the enhancement of the existing infrastructural assets, the construction of useful infrastructures, the technological adaptation of the national road network in line with the European and international framework of digitization of road infrastructures, also in support of connected automated vehicles, as well as reducing road accidents and ensuring continuity with the European cooperative intelligent transportation system (C-ITS). This digital transformation process is applied to the road infrastructures of the Trans-European Network - Transport (TEN-T), as well as to new infrastructures connecting elements of the TEN-T network, and progressively to all the infrastructures belonging to the first level of the National Integrated Transport System (SNIT), according to the timing and procedures set out in the Smart Road Decree (art. 4, Smart Road Decree).

⁴² CISCO, 'The Internet of Everything. Global Public Sector Economic Analysis', https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf.

⁴³ Smart Road Ministerial Decree 28.02.2018, Smart Road Decree, available at www.normattiva.it.

More in details on transport infrastructure, art. 6 of the Smart Road Decree provides that the functional specifications of the digital transformation process of the Smart Roads, are identified in paragraph 4, Table 1, of Annex A⁴⁴ and are to be implemented in accordance with Sections A to C, referred to the same Annex A. Moreover, these functional specifications are subject to updates and revisions by decree of the Minister of Transport (Now Ministry of Infrastructure and sustainable mobility), and with the technical support of the Observatory established pursuant to art. 20 of the Smart Road Decree (M.D. 28.02.2018).⁴⁵

ID	Specific Functional Description
1	Road-side presence of communication network with high level of bit-rate (optical fiber).
2	Continuous coverage of the road axis and related appurtenances with connection services for the IoT and routing to the data communication network.
3	Road-Side Unit for V2I communication, located in a way that allows connection to vehicles equipped with On-board-unit V2X that meet industry standards.
4	Presence of a Wi-Fi hot-spot system for the connectivity of personal devices, located at least in the service and parking areas (if any).
5	Traffic detection and enforcement system, as well as detection of outflow conditions, developed on a higher-level detail for type I smart roads, regarding with the descriptions in Section A (detection of traffic and flow conditions): the survey system must have the minimum characteristics of the measurements and comply with the qualification rules described in Section A; the system must be designed in a way that minimizes its ecological and energy impact.
6	Data archiving system from the detection of traffic and flow conditions with archiving functions and historicization, according to the specifications of Section A (detection of traffic and flow conditions), in compliance with the legislation on privacy and data protection.
7	Provision of a modeling system for the forecast of medium-short term flow conditions, as well as for the estimate/forecast for subsequent time periods, regarding with the specifications of Section A detection of traffic and flow conditions).
8	A real-time monitoring system for climatic and rain conditions, as detailed in Section B (Monitoring hydro/weather); the system must be designed in a way that minimizes its ecological and energy impact.

⁴⁴ Annex A of the D.M. 28.02.2018 is available at this link: https://www.gazzettaufficiale.it/do/atto/serie_generale/caricaPdf?cdimg=18A0261900100010110001&dgu=2018-04-18&art.dataPubblicazioneGazzetta=2018-04-18&art.codiceRedazionale=18A02619&art.num=1&art.tiposerie=SG

⁴⁵ According to art. 20 of Smart Road Decree, in order to promote the digital transformation process toward Smart Roads and activities aimed at experimenting and developing connected and automated vehicles, at the General Direction for information and statisticians systems of the Ministry of Infrastructure and Transport (Now Ministry of infrastructure and sustainable mobility) is established the 'Technical Support Observatory for Smart Roads and for the connected and automated vehicle'.

9	Ability, based on traffic detection data and forecasting models, to offer content for advanced travel information services to users, allowing any re-routing actions; the transmission of information can take place using V2I communication systems, if permitted by current standards and equipment, or through web app.
10	Real-time control from a traffic center equipped with management support programs as indicated in section C (ITS advanced services), which include the ability to apply pre-established traffic management scenarios (and object to impact simulation) selected and implemented dynamically based on traffic data and other information received from sources, including heterogeneous ones; scenarios can predict mix of possible measures such as: deviations of flows, in case of serious obstructions; interventions on average speeds, to avoid or solve congestion (speed control); suggestion of trajectories and lanes (lane control); dynamic access management (ramp metering).
11	Ability to provide road users, especially professional drivers and company fleets, on request, with parking management services and refueling (with particular reference to electric charging).
12	Ability to provide, based on the static and dynamic characteristics of the infrastructures, relevant traffic data, medium and short-term estimates of flow conditions, of the hydro/weather monitoring system and of any specific models and algorithms, C-ITS type services according to the specifications referred to in Section C3 (Advanced Services of type C-ITS); in the first instance, the services must be able to be used at least by vehicles service of the management/concessionaire body of the smart-road, as well as by heavy vehicles in transit and equipped on board with V2X communication systems.

General List of the Smart Road functional specification – Annex A of the Smart Road Decree
(English translation)

Furthermore, art. 7 of the Smart Road Decree states that the implementation of functional features applies to all the newly built infrastructures, or those being upgraded for which the preliminary project has not yet been approved at the date of entry into force of the smart road decree and falling within the scope of the application referred to in art. 4 of the same decree. The implementation also applies to infrastructure existing if they are objects of technological innovation interventions.

Finally, it is important to underline that the art. 8 regulates the costs relating to the implementations. These costs are borne by the infrastructure concessionaire, the service concessionaire or, in the absence of the previous figures, the managing body in a different capacity, and are to be considered as investment costs, recognised upon request and according to the regulations and procedures in force. under the relevant conventions, concessions or service concessions.

The Smart Road Decree provisions can be applied by analogy to the general condition for using autonomous vehicles. As a matter of fact, the requirement

provided by the Decree should as basically provisions for the development of road infrastructures, allowing the most adequate growth of autonomous and connected driving. This development of infrastructures is part of the largest phenomenon of the development of smart cities which is increasingly important in contemporary society. We need not only smart mobility but more in general smart roads and smart cities to prepare an appropriate operating environment for AV.

As part of the development of adequate infrastructures to encourage autonomous and connected driving, a significative Italian initiative was the signature of the Memorandum of Understanding between the Ministry for Technological Innovation and Digitization, and the Ministry for Infrastructure and Transport, on May 2020.⁴⁶ The aim of the memorandum of understanding was the development of innovative mobility through research and testing of automated and connected vehicle (CAD). The memorandum, indeed, aims to develop and support applied research, experimentation and prototyping, production and training of new professionals in the field of innovative vehicles, as well as the interest in creating services with a social impact for the Country. The agreement also supports and encourages collaboration and partnership between public institutions, companies, universities and research bodies in these fields.

Following these initiatives, the most recent programme on autonomous driving experimentation has been launched on 17 February 2022 as a result of the collaboration between the Italian Department for Digital Transformation,⁴⁷ the Italian Ministry of Economic Development⁴⁸ and the Italian Ministry of infrastructures and sustainable mobility.⁴⁹

The programme is entitled 'Experimentation Italy'⁵⁰ and its object is the experimentation of a fleet of self-driving shuttles on the road in Turin. The programme represents the regulatory sandbox that allows start-ups, companies, universities, and research centres to experiment with innovative projects through a temporary derogation from current regulations.

'Experimentation Italy' programme aims to make Italy an innovation laboratory by opening the doors to the application of emerging technologies,

⁴⁶ Ministero per l'Innovazione tecnologica e la Digitalizzazione e Ministero delle Infrastrutture e dei Trasporti, Protocollo d'intesa in materia di innovazione per la guida autonoma e connessa in ambito urbano ed extraurbano, available at https://www.mit.gov.it/sites/default/files/media/notizia/2020-05/Guida_Autonoma_MID_MIT_.pdf. Still on the topic of innovation, but not strictly on autonomous vehicles, we report: Working Group on Artificial Intelligence and Blockchain, appointed by the Ministero dello Sviluppo Economico Italiano (MISE), Proposte per una strategia italiana per l'intelligenza artificiale, 2019; Ministro dell'Innovazione tecnologica e della digitalizzazione, Strategia per l'innovazione tecnologica e la digitalizzazione del Paese 2025, 2020.

⁴⁷ The Italian Department for Digital Transformation is the support structure for the Italian Ministry for Technological Innovation and Digital Transition for the promotion and coordination of the Government's actions aimed at defining a unitary strategy in the field of Italian digital transformation and modernisation through digital technologies. Webpage of the Department for Digital transformation: <https://innovazione.gov.it/dipartimento/la-struttura/>

⁴⁸ Website of the Italian Ministry of Economic Development www.mise.gov.it

⁴⁹ Website of the Italian Ministry of infrastructures and sustainable mobility www.mit.gov.it

⁵⁰ The authorisation for the experiment was obtained from the Turin Transport Group (GTT) and takes place within the SHOW project, funded by the European Horizon2020 program, which aims to support the transition to an effective and sustainable self-driving urban transport. More details on the Experimental Italy Programme are available at: <https://www.mit.gov.it/comunicazione/news/innovazione-libera-alla-sperimentazione-di-navette-guida-autonoma-su-strada>

for the benefit of citizens, businesses and public administration. In the event of successful trials, thanks to the data collected, a regulatory change may be proposed to allow the innovations to become replicable throughout the national territory.

3. Data protection and the processing of personal data by autonomous driving systems.

3.1. The data collected and processed.

Personal data are regulated under General Data Protection Regulation (Reg. 2016/679/UE),⁵¹ implemented in Italy by d.lgs. no. 101/2018,⁵² that amended the Italian Privacy Code (D.lgs. no. 196/2003).⁵³ Concerning no personal data, on 23 February 2022 has been published the Regulation Proposal Data Act on fair access to and use of data,⁵⁴ as one of the proposals part of the European strategy for data.⁵⁵ Considering the growing importance of data for society and the economy, the European strategy for data aims at creating a single market for data that will ensure Europe's global competitiveness and data sovereignty protecting individuals.

Coming to soft law acts, it is important to mention the European Data Protection Board (EDPB) Guidelines no. 01/2020 on processing personal data in the context of connected vehicles and mobility-related applications.⁵⁶

Currently, vehicles can process data. Indeed, it is clear that the connectivity of these vehicles results in the collection, processing, and transfer of personal data. More precisely, manufacturers can collect data not only on the performance of their products (which also makes it possible to quickly detect a malfunction and determine liability in case of a car accident) but also users' personal information, who are often unaware of this processing of their personal data.⁵⁷ In addition, this data may be intercepted by third parties who use or sell it for diverse purposes.

⁵¹ Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016/679/UE, (General Data Protection Regulation - GDPR), available at www.eur-lex.europa.eu

⁵² Italian legislative decree 10.08.2018, n. 101, Provisions for the adaptation of national legislation to the provisions of regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and repealing Directive 95/46/EC (General Data Protection Regulation), available at www.normattiva.it.

⁵³ See footnote no. 6.

⁵⁴ Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), 23.02.2022 COM (2022) 68 final

⁵⁵ More details on the European Strategy for data are available on the official web page: <https://digital-strategy.ec.europa.eu/en/policies/strategy-data#:~:text=Strategy%20for%20data-A%20European%20Strategy%20for%20data,and%20societal%20progress%20in%20general>.

⁵⁶ European Data Protection Board (EDPB) Guidelines no. 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, 9.02.2021, available at www.edpb.europa.eu.

⁵⁷ For an analysis on the unawares of the users in relation to the processing of their personal data through new technologies see Gatt L., Montanari R., Caggiano I.A., eds. (2021). Privacy and Consent. A Legal and UX&HMI Approach. Naples, University Suor Orsola Press.

The data processed can be personal data or non-personal data, including data generated directly by the automated and connected vehicles (metadata). A typical example of personal data (art. 4, para. 1, let 1), GDPR) processed are identification and contact data of the driver and passengers onboard the vehicle. The personal data also includes particular categories of data (art. 9 GDPR) such as data relating to the driver's state of health. Moreover, vehicles are able to carry out automated processing of different types of personal data related to the drivers through specific algorithms, creating their detailed profile, i.e. profiling process (art. 22 GDPR), such as driver localisation. Finally, in addition to personal data, non-personal data are also processed, and can also be generated directly by the vehicle itself, such as those relating to the active driving mode and speed of the vehicle.

About the analysis of the data processed by self-driving cars, already before the GDPR, the Article 29 Data Protection Working Party (Article 29 WP)⁵⁸ in 2014 adopted an opinion aimed at finding solutions that enforce privacy protection rules also in the Internet of Things.⁵⁹ Based on a typical Law and economics approach, the Article 29 WP compared citizens' interests to the protection of their personal data and those of companies operating in this sector, who receive significant economic benefits from the spread of IoT, trying to dictate guidelines to extend the existing European legislation on data protection to smart things as well.

Then, in order to define and analyse the IoT phenomenon, the Global Privacy Enforcement Network (GPEN)⁶⁰ has launched Privacy Sweep 2016. It is an international survey to verify respect for privacy and data protection on the IoT field, strengthening cooperation between the Data Protection Authorities of the twenty-six countries of the world who have joined the initiative.⁶¹ The investigation ended on 22 September 2016, with worrying results. In fact, more than 60% of smart things have not passed the GPEN test.

The Italian Data Protection Authority (Garante per la Protezione dei Dati Personali)⁶² is studying the phenomena of the IoT and all the main relevant documents on the topics are available on its dedicated webpage, constantly updated, with an overview on the Italian and European initiatives.⁶³ At the same time the Italian DPA is also monitoring the field of artificial intelligence with particular regard to data protection aspects.⁶⁴

⁵⁸ Article 29 Data Protection Working Party (Art. 29 WP) was established by art. 29, Directive 95/46/CE and currently replaced by European Data Protection Board (EDPB).

⁵⁹ Art. 29 WP, Opinion 8/2014 of 16 September 2014 on the on Recent Developments on the Internet of Things [2014] 10 ff., which refers to Wearable Computing, Quantified Self and demotics, but it appears to be applicable to any area of IoT.

⁶⁰ In 2007, the Council of the Organisation for Economic Co-operation and Development (OECD) adopted the Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. The Recommendation imposed on OECD member states the goal of creating an informal network of Personal Data Protection Authorities, from which the Global Privacy Enforcement Network (GPEN) was born.

⁶¹ For more details on Privacy Sweep 2016, included results www.privacyenforcement.net

⁶² All the information on Garante per la Protezione dei Dati Personali, are available on its official website: www.garanteprivacy.it

⁶³ Webpage on Internet of Things edited by Garante per la Protezione dei Dati Personali <https://www.garanteprivacy.it/temi/iot>

⁶⁴ Webpage on Artificial Intelligence edited by Garante per la Protezione dei Dati Personali: <https://www.garanteprivacy.it/temi/intelligenza-artificiale>

With specific regard to self-driving cars, research commissioned by the Fédération Internationale de l'Automobile (FIA), focusing on the flow of data exchanged between cars and their respective manufacturers, revealed the quantity and quality of data that last-generation vehicles are able to exchange.⁶⁵ Additionally, based on the results of this research, FAI launched the My Car My Data project⁶⁶ to raise awareness about the processing of personal data and the need to introduce specific legislation.

3.2. Storage and access to the data.

Also, for personal data storage the legislation applicable is the GDPR, as well as the EDPB Guidelines 1/2020.⁶⁷ At these two regulations, respectively, the first of Hard Law and the secondo of Soft Law, is added the ePrivacy Directive⁶⁸ which will be replaced by the new ePrivacy Regulation,⁶⁹ when it will enter in force. The ePrivacy Directive has been implemented in Italy by Italian Legislative Decree 28.05.2012, no. 69,⁷⁰ that has amended the Italian Privacy Code art. 121-134.

In particular, the ePrivacy Directive establishes a specific standard for all subjects who intend to store and access information stored in the terminal equipment of a user in the European Economic Area (EEA). Connected and autonomous vehicles (CAD), as well as all intelligent systems connected to them must be considered as terminal equipment and therefore the ePrivacy Directive is applicable to them. Indeed, personal data can be processed by autonomous vehicles and could be stored on the operating systems of the autonomous vehicles themselves or on external software (e.g. cloud computing infrastructures).

Concerning personal data processing, it should be regulated in compliance with GDPR. More in detail this processing is lawful when is compliant with art. 6, 9 and 22 GDPR. As underlined by the EDPB in the Opinion 5/2019 on the interaction between the ePrivacy Directive and the GDPR,⁷¹ the consent of the data subject is required for the storage of data as well as for access to data

⁶⁵ 'FIA Reveals what data is being tracked and how the public reacts to connected cars' (2015) <https://www.fia.com/news/fia-reveals-what-data-being-tracked-and-how-public-reacts-connected-cars>.

⁶⁶ Website of MyCar My Data Project www.mycarmydata.org

⁶⁷ European Data Protection Board (EDPB) Guidelines no. 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, 9.02.2021, available at www.edpb.europa.eu

⁶⁸ Directive of the European Parliament and of the Council of 12.07.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2002/58/EC, available at www.eur-lex.europa.eu

⁶⁹ Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), SWD (2017) 6 final, amended on 10.02.2021.

⁷⁰ Italian Legislative decree 28.05.2012, no. 69, Amendments to the legislative decree 30.06.2003, n. 196, containing the Italian Data Protection Code, in implementation of directives 2009/136/EC, regarding the processing of personal data and privacy protection in the electronic communications sector, and 2009/140/EC in the field of networks and services of electronic communication and of Regulation (EC) no. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection legislation, available at www.normattiva.it

⁷¹ EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities 12.03.2019 1, available at www.edpb.europa.eu.

already stored. Concerning personal data, data subject's consent constitutes the more common lawful basis for processing (Art 6 GDPR), while for personal data that in addition falls into one of the categories listed in art 9 GDPR (i.e. sensitive data), consent is an exception to the general prohibition of processing data of that kind. The same regime of exception is applicable to automated processing according to art. 22 GDPR, which are prohibited as a general rule, and the data subject's consent constitute an exception to the rule. These are the most common but not the only legal bases for lawful processing, for which reference is made to a more in-depth analysis of the data protection legislation.

In any case, the consent must be informed and, therefore, preceded by adequate information on the processing of personal data provided pursuant to art. 13 and 14 GDPR. Data subjects should in fact be informed and enabled to control the way in which their data are collected and processed by the vehicle. The information should be provided in the data subject's language, only strictly necessary data should be processed by default, data should not be transmitted to unauthorised third parties, data must be kept only for the time necessary, the data subject should be able to permanently delete all personal data before the vehicles are put up for sale and should have direct access to the data generated by the applications driving vehicle software. In general, data subjects must be able to exercise all the rights expressly provided for them by the GDPR (art. 12- 21 GDPR).

Furthermore, considering the volume and diversity of personal data processed, the EDPB Guidelines 1/2020 underlines that data controllers must be required to ensure that the technologies used in the context of connected vehicles are configured in compliance with the principles of privacy by design and by default, pursuant to Art. 25 GDPR. In particular, technologies should be designed to minimize the collection of personal data provide default privacy protection settings and ensure that data subjects are well informed and have the ability to easily change associated configurations and their personal data. More in general Data Controllers should adopt the measures to guarantee the security and confidentiality of the data and all the necessary precautions (e.g. encryption).

Concerning the parties authorised to access to personal data of the driver and of the passenger on board the vehicle, they are the Data Controller, the Data Processor and third parties, as well as subjects authorized by them. In particular, the figure of Data Controller includes both the manufacturer of the vehicle and the manufacturer of the intelligent devices of the same as well as the provider of the cloud computing in which the data is saved and in general the provider of the infrastructures through which the vehicles are connected and process personal data.

The data must be stored in compliance with GDPR, guaranteeing access to them only by authorised parties as, for example, the insurance company, public authorities, vehicle dealership or other maintenance person called to perform a technical intervention on the vehicle. These subjects certainly need to access some personal data but under certain conditions and only about data necessary for the performance of a specific task. On the contrary, personal data stored could not be accessible by unauthorised parties, who could unlawfully process these data by entering in the autonomous vehicle and using the onboard

computer. At the same time, the same personal data could be processed unlawfully by third parties capable of hacking the driving system or the external cloud-computing containing personal data.

Therefore, the authorised/legitimated subjects may have access to the data according to GDPR lawful basis. In particular, the insurance company, as well as vehicle dealership or other maintenance person called to perform a technical intervention, are previously authorised by the data subject through express consent (Art. 6, lett. a), GDPR); furthermore, they are also authorised to use and access the data for the performance of the contract of which the interested party is a party (Art. 6, lett. b), GDPR). As for the competent authorities, they can access the data for public interest or in the exercise of official authority (Art. 6, lett. e), GDPR).

Finally, if the data must necessarily be transferred to third parties, it would be advisable to evaluate the possibility of anonymising them where possible, since anonymous data are not considered personal and therefore cannot cause any damage to the individual to whom the data belongs, maintain the benefits and minimise the risks in relation to related vehicles.

When it is not possible to anonymise the data, the possibility of pseudo-anonymisation (art. 25 GDPR) can still be evaluated. In this case, the data is in any case a personal data in which the interested party can be identified and must be governed according to the GDPR, but in any case, it is a greater protection for the data subject.

3.3. Deletion of the personal data.

Also, the deletion of data is regulated under GDPR. However, it does not establish the retention times for the data controller. According to the accountability principle, it is up to the owner to identify and legitimize a period of time deemed compliant, also through references to criteria dictated by sectoral standards or practices.

The important thing is that the principles of data minimization and therefore conservation limitation established in art. 5 of the GDPR are applied.

Furthermore, personal data must be kept in a form that allows the identification of the data subjects for a period of time not exceeding the achievement of the purposes for which they are processed. However, personal data may also be kept for longer periods if they are processed exclusively for archiving purposes in the public interest, for scientific or historical research or for statistical purposes, in compliance with art. 89, para. 1, GDPR. At the same time the so-called 'conservation limitation' provides that the conservations should be made without prejudice to the implementation of technical and organizational measures required by GDPR to protect the rights and freedoms of the data subject

In this regard, Recital 39 GDPR states that it is necessary to define a deadline for the cancellation of personal data stored but also for periodic verification.

The legislator is therefore very clear: the data must be processed for the shortest possible time. This period must consider the reasons why the organization must process the data, as well as any legal obligations for the

retention of the personal data for a specific period (for example national labor, tax or anti-fraud laws).

Moreover, the terms of data retention must be consistent with the contents of the information provided by art. 13 GDPR, which indicates also the retention period of personal data or, if this is not possible, the criteria used to determine this period.

Finally, in any case, the data subject must be able to exercise the right to erasure or the right to be forgotten according to the provision of art. 17 GDPR.

4. Other key issues for autonomous driving.

Regards to the liability rules, Italian administrative and criminal legislation requires personal liability, and no sanction can be imposed on a person for the behaviour of another person. This provision is stated by art. 11, Law 24.11.1981, n. 689⁷², for the administrative sanctions, and art. 40, Italian Criminal Code, for the criminal sanctions⁷³. This means that if there is no driver who has control of the vehicle at least no administrative and criminal provision can be imposed on the driver. However, in a certain condition the owner of the vehicle or its passengers could be held liable.

Instead, it can be assumed that if the vehicle commits an infringement the sanction goes to the owner (and passengers if applicable). Administrative offences applicable by analogy are artt. 140, 142, 143, 146, 147, 148, 149, 152, 189, New Road Traffic Code. With regard to criminal law, this is a much more complex issue that cannot be addressed here considering both the peculiarity of the matter and the complexity of the offence caused by an autonomous vehicle.

Currently, concluding on Civil liability, already analysed in question n. 1, it can be assumed the Civil liability to three different subjects: all people counted of the concept of producer (according to art. 114 of the Italian Consumer Code); the owner of the vehicle for the sole fact that he/she purchased a self-driving cars and therefore is considered responsible for the damage caused by the same (currently according to art. 2015 and 2054, Italian Civil Code, but probably the legislation will have to be changed especially regarding art. 2054 which does not refer only to the owner of the vehicle but mainly regulates the liability of the driver); and to the passenger on board the vehicle (art. 2051, Italian Civil code).

⁷² Law 24.11.1981, n. 689, Changes to the penal system, available at www.normattiva.it.

⁷³ Royal Decree 19.10.1930, no. 1398, Italian Criminal Code, available at www.normattiva.it.



BCI devices and their capacity to express human will having legal value: A model of risk-based classification

LUCILLA GATT 

Full professor of Private Law

ILARIA AMELIA CAGGIANO 

Full professor of Private Law

EMILIANO TROISI 

Ph.D. (c.) in Private Law 'Humanities and Technology'

LIVIA AULINO 

Ph.D. in Private Law 'Humanities and Technology'

DAVIDE SILVIO D'ALOIA 

Ph.D. (s.) in Private Law 'Humanities and Technology'

LUIGI IZZO 

Ph.D. (s.) in Private Law 'Humanities and Technology'

Università degli Studi Suor Orsola Benincasa, Napoli

Abstract

One of the ultimate frontiers in biotechnology is Brain-computer-interface. BCI devices are currently developed for therapeutic purposes (e.g., as assistive tools) but also recreational ones. A BCI system detects brain activity, allowing a decoding of patterns of neural signals, then 'translatable' in commands a computer can understand and even carry out in the external reality. That's why BCI is now becoming more used (or experimented), considering the advantages that could derive from it. Nevertheless, it also raises some questions from a legal perspective. This Paper focuses on BCI-based devices used for assistive and augmented communication of users, and wonders what legal regime should be accorded to the personal will expressed through those tools. Once the risks have been identified, the parameters and requirements a BCI device must meet, for the human will expressed through it having legal value, are outlined. The Paper proposes, in conclusion, a self-assessment strategy to operationalize BCI technologies applicable to the context of legal relations, implementing methods of risk evaluation and management. A risk-based classification model is also suggested.



Keywords: BCI, Brain-Computer Interface; Regulatory perspectives; Vulnerable people; Human enhancement; Legal capacity; Legal relations; Contracting; Risks; Classification; Impact.

Summary: [1. Introduction](#) - [2. Transhumanism and BCI experimentation: legal context and new challenges](#) - [3. BCI and the new \(possible\) frontiers of contractual capacity](#) - [4. Brain-computer interfaces \(BCI\) to create legal relations. The frontiers of contracting abound with doubts](#) - [4.1. BCI-induced restoration of legal capacity](#) - [4.2. BCI-mediated intention to create legal relations](#) - [4.3. A legal standpoint: the need for accuracy. Critical issues and key requirements](#) - [4.4. A risk-based classification model and approach](#)

1. Introduction.*

For generations, humans have imagined communicating and interacting with machines through thought and creating devices that can analyze a person's thoughts.

In fact, the cyberpunk movement, especially in the figure of W. Gibson, brought forward the idea of 'jacking in', understood as the possibility of hooking the human or animal mind into software capable of reproducing brain impulses. Outside of the myth, for the last 30 years or so, science has been progressing more and more in the field of 'bioengineering', understood as a medical field that uses methodologies and technologies specific to engineering to solve problems in medicine, biology and the life sciences in general. This medical-scientific field is the result of a mixture of tools of various kinds, relating to chemistry and molecular biology, applied mathematics, mechanics, electronics, computer science, etc., as well as combinations of these disciplines.

This contribution focuses on the use of electromyographic bio-signals derived from neural activity. These signals are used today to construct and 'educate' brain-machine interfaces (BCIs). One of the major fields of application of BCI technology today concerns tetraplegic patients, who, by means of robotic arms, are able to command their thoughts to grasp objects and, conversely, receive sensory stimuli in the brain.

It is generally possible to distinguish three types of BCI:

Invasive BCI, where a connection takes place at the neural level. The invasive

* The paper is the result of the work of a selected team of researchers of the Research Centre of European Private Law (ReCEPL) at Università degli Studi Suor Orsola Benincasa, coordinated by the ReCEPL Director Prof. Lucilla Gatt and the ReCEPL Vice-Director Prof. Ilaria A. Caggiano.

The work was presented at the IEEE International Conference 'Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering' (MetroXRINE), National Research Council, Rome, October 26-28, 2022, and published in the IEEE MetroXRINE 2022 Proceedings, 557. awarded as 'Best Paper on Service Innovation' from MetroXRINE scientific committee.

The author of paragraph 1 is Dr. Davide Silvio d'Aloia, ReCEPL Young Researcher and Ph.D. (s.) in Private Law 'Humanities and Technologies'; the author of paragraph 2 is Dr. Livia Aulino, ReCEPL Young Researcher and Ph.D. in Private Law 'Humanities and Technologies'; the author of paragraph 3 is Luigi Izzo, ReCEPL Young Researcher and Ph.D. (s.) in Private Law 'Humanities and Technologies'; the author of paragraphs 4, 4.1, 4.2, 4.3 e 4.4 is Dr. Emiliano Troisi, ReCEPL Young Researcher and Ph.D. (c.) in Private Law 'Humanities and Technologies'.

BCIs used today are used to repair damaged vision and provide new functionality to paralysed people. But they are subject to the accumulation of scar tissue that causes weakening and loss of signal as the body reacts to a foreign object in the brain.

Partially invasive BCIs are implanted inside the skull, but are placed outside the brain. The signals produced have better resolution than non-invasive BCIs and have a lower risk of forming scar tissue in the brain than the former.

Non-invasive BCIs allow muscle implants to be powered in order to restore movement as close as possible to natural motion. These implants are based on connections totally outside the cranial box and, although they are easy to wear, have the lowest signal resolution of the three types of BCIs, as they scatter and blur the electromagnetic waves created by neurons. The subject must undergo rehabilitation to bring the body to 'fuse' with the BCI but they are suitable for temporary and limited needs, as well as being low cost.

The paragraph II deals with the relationship between Transhumanism and BCI and the application of Italian and European legislation in this field.

Paragraph III deals with the possibility of expressing a contractually valid consent through the bci taking into account the characteristics and vulnerabilities of the bci, in a perspective of the application of the concept of error and violence as vices of the will.

The paragraph IV deals with the legal aspects of BCI used for assisted or augmented communication of will to create legal relations and proposes a risk-based classification model and approach to the use of their applications.

2. Transhumanism and BCI experimentation: legal context and new challenges.

The development of the BCI has increased the closeness between man and technology. Transhumanism is a cultural movement that supports the use of scientific and technological discoveries to increase physical and cognitive abilities and improve the human condition¹. Such technologies can be a support for vulnerable people, such as people with disabilities². The use of such technologies raises some legal issues.

With BCIs, an artificial communication system is created that, using special sensors, allows the reception of data from the brain and their transfer to a computer. So, the question arises whether technological tools can be considered suitable for effective communication directly from the brain. And consequently, whether the will expressed through technology can be considered attributable to the subject. This problem is even more important when the person to whom the technology is applied is physically disabled³.

This entails the need to identify "neurorights", which protect human rights

¹ AP Karanasiou, 'On being trans-human: commercial Bcis and the quest for autonomy, The Cambridge Handbook of the Law of Algorithms' (CUP 2020).

² Ministero della salute – Commissione per lo studio delle problematiche concernenti la diagnosi, la cura e l'assistenza dei pazienti affetti da sclerosi laterale amiotrofica, 'Rapporto di Lavoro' (13/12/2004, https://www.salute.gov.it/imgs/C_17_pubblicazioni_450_allegato.pdf, 3).

³ S Amato, 'Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie' (Torino 2020, 120). P Perlingieri, 'Note sul "potenziamento cognitivo', Comparazione e diritto civile (1 2021, 209 ff).

within the mental and neurocognitive sphere of the individual. In this regard, it is noted that, also in the context of cognitive technologies, some articles of the Italian Constitution are applied.

Art. 13, in fact, recognizes freedom as an inviolable right, even when it is denied by physical impediments. The second paragraph of the article states that no form of restriction of personal freedom is permitted, except by a reasoned act of the judicial authority (Art. 111, c. 1, 2) and only in the cases and ways provided for by law (Art. 25, c. 3). This principle also extends to freedom of expression.

In addition, Article 32, co. 2 establishes respect for the human person as a limit to compulsory medical treatment, and Article 21 recognizes freedom of expression by all available means.

The right to physical and mental integrity is also protected at the European level. Article 3 of the Charter of Fundamental Rights states that "every person has the right to his or her physical and mental integrity", and Article 8 of the European Convention on Human Rights, according to which "every person has the right to respect for his or her private and family life, home and correspondence".

The contamination between the human body and technology could mean that the acts of will of a subject are vitiated by a highly technological element that is even grafted into the physicality of the human being, that is why it is essential that the right to continue to operate, observing reality and finding solutions through new imputation criteria.

If the BCI is used as a tool to test the will of the subject used as evidence during a study, a neuroscientific test implies a physical and psychological intrusion, so that in this case, too, personal freedom is taken into account and balanced with the constitutional principles that stipulate that every individual has the right of defense and the proof of the right to a fair trial governed by law.

In this field, it is important that the legal research combines skills and technical knowledge with ethical principles and at the same time as the reference regulatory framework to protect the fundamental rights of the persons involved.

Therefore, a proactive approach in research is appropriate, which also consists in examining, from the design, the legal aspects, the acquisition of informed consent, the cost/benefit ratio for the people involved, which also take into account the protection of their rights.

3. BCI and the new (possible) frontiers of contractual capacity.

BCIs, in view of the characteristics outlined in the introductory paragraph, are able to play a role as true game changers in the contractual landscape and, more specifically, in the context of subjects who might not be able to express a valid consent for contractual purposes.

In fact, through these aids they could:

- obtain information on the contractual relationship in which one is interested;

- express consent or even a counter-proposal.

To exemplify the matter, consider a person in a state of paralysis, such as that of Amyotrophic Lateral Sclerosis, a neurodegenerative disease affecting the motor neurons of the spinal cord, brain stem and motor cortex⁴. Again, suppose a person suffers a particularly violent stroke that renders him or her almost paralysed and unable to communicate⁵.

In such cases, it would be impossible to communicate any consent for the purpose of assuming obligations.

However, with the use of BCIs to assist affected individuals, it would be possible to enable them to regain the communicative capabilities necessary to express a valid consent for contractual purposes, perhaps by operating a brain link between a tablet/pc and a brainwave conversion system or other equally efficient BCIs, in the same way that the use of BCIs for non-therapeutic purposes is being experimented with⁶, or even to perform 'biometric' authentication via EEG⁷. Similarly, with devices such as cochlear implants or systems to compensate for vision loss, it becomes possible to be aware of the characteristics of the contract⁸.

This is not a new scenario for national judges, since a tutelary judge has decided that an ALS sufferer, respecting precise conditions, can avoid being subject to support administration and use BCIs to express his or her wishes⁹. Yet, it is not clear whether this can actually lead to the expression of an effective consent¹⁰.

This is for two reasons.

Firstly, the 'information acquisition' phase is relevant where the subject is forced to use implants that allow for a recovery of hearing and/or visual capabilities. Since these implants do not all guarantee first-class quality of sensory information (think of cochlear implants, which in any case do not cover

⁴ Ministero della Salute - Commissione per lo studio delle problematiche concernenti la diagnosi, la cura e l'assistenza dei pazienti affetti da sclerosi laterale amiotrofica, 'Rapporto di Lavoro', p. 3, 13/12/2004, https://www.salute.gov.it/imgs/C_17_pubblicazioni_450_allegato.pdf.

⁵ M. Poloni, E. Vitelli, S. Fumagalli, A. Valente, Ictus: cause, tipi e sintomi dell'ictus cerebrale, <https://www.marionegri.it/magazine/ictus-cerebrale>.

⁶ P. Nuyujukian, J. Albites Sanabria, J. Saab, C. Pandarinath, B. Jarosiewicz, CH. Blabe, et al. (2018) 'Cortical control of a tablet computer by people with paralysis'. PLoS ONE 13(11): e0204566. <https://doi.org/10.1371/journal.pone.0204566>.

A. Al-Hamadani, M. Al-Faiz, "Inverse Kinematic Based Brain Computer Interface to Control Humanoid Robotic Arm", International Journal of Mechanical & Mechatronics Engineering IJMME-IJENS Vol:20, No:01, 2020, Available at SSRN: <https://ssrn.com/abstract=3566851>. M. Blankertz, C. Tangermann, Vidaurre, Siamac Fazli, C. Sannelli, S. Haufe, C. Maeder, L. Ramsey, I. Sturm, G. Curio, K.R. Müller, 'The Berlin brain-computer interface: non-medical uses of BCI technology', Frontiers in neuroscience, 2010, doi: 10.3389/fnins.2010.00198.

⁷ A. Mosslah, R.H. Mahdi, Shokhan M. Al-Barzinji, 'Brain Computer Interface for Biometric Authentication by Recording Signa', The International Journal of Multimedia & Its Applications (IJMA) Vol.11, No.03, 2019, available at SSRN: <https://ssrn.com/abstract=3438143> or <http://dx.doi.org/10.2139/ssrn.3438143>.

⁸ See <https://www.amplifon.com/it/news/tipologie-impianto-cocleare>; Nitish Kumar, 'BRAIN COMPUTER INTERFACE - A SEMINAR REPORT', 2008, p. 3, https://www.academia.edu/35433827/BRAIN_COMPUTER_INTERFACE_A_SEMINAR_REPORT. <https://support.apple.com/en-gb/HT201466>

⁹ F. G. Pizzetti (2011), 'Libertà di autodeterminazione e protezione del malato nel «Brain-Computer interfacing»: un nuovo ruolo per l'amministratore di sostegno?', Rivista Critica del Diritto Privato, Jovene Editore, disponibile su https://www.academia.edu/12219908/Libert%C3%A0_di_autodeterminazione_e_protezione_del_malato_nel_Brain_Computer_interfacing_un_nuovo_ruolo_per_l'amministratore_di_sostegno.

¹⁰ R. Sacco e G. De Nova, Il contratto, t. I, Illed., in R. Sacco (dir.), Trattato di diritto civile, (Torino, 2004) 134 ss.

the entire spectrum of sound frequencies), it may well be the case that the potential contracting party is misled by exploiting the limitations of the BCI and does not understand all the contractual conditions. In that case, there would be a misled consent and the aggrieved contracting party would be able to request the annulment of the contract under Art. 1427 of the Civil Code.

The same problem arises with BCIs designed to express consent, i.e. tablets or even an electronically controlled arm, since the user may not be able to fully coordinate the movements and functions of the BCI, perhaps having not yet completed the rehabilitation process in order to use it properly.

It is true that here one would not have an error resulting from the conduct of others, but it is difficult to admit the validity of such a consent.

To this must be added the computer vulnerability of the BCIs themselves, which are now hyper-connected and can also be used via smartphone apps, leading to the creation of sensitive 'spots' through which computer intrusions can be conducted¹¹.

These attacks can first and foremost harm the privacy of the user and even evolve into veritable 'brain spyware', aimed at granting the counterparty an undue informational advantage over the BCI user, as it could abstractly be assumed that the counterparty understands the objections that he is about to make to the contract proposal, thus being able to prepare answers 'in advance'.

Again, the BCIs themselves could be manipulated as tablets and electronic arms, making them perform movements not ordered by the user but favourable to the manipulator. Certainly, in such a hypothesis, there would be cases of consent extorted with malice or violence and this would lead to the annulment of the contract that may have been 'concluded'.

It follows that, as long as secure standards for the protection of BCIs from external intrusion are not established and in the absence of a discipline to ascertain whether or not there is a validly given consent, BCIs may be useful for communicating with the outside world but certainly not for expressing a position for contractual purposes.

4. Brain-computer interfaces (BCI) to create legal relations. The frontiers of contracting abound with doubts.

4.1. BCI-induced restoration of legal capacity.

Brain-Computer-Interfaces can successfully allow people suffering from severe medical conditions, such as complete paralysis or locked-in-syndrome,

¹¹ Q. Li, D. Ding, M. Conti, 'Brain-Computer Interface Applications: Security and Privacy Challenges' (2015) 10.1109/CNS.2015.7346884; A. Krausová, "Legal aspects of brain-computer interfaces" (2014) Masaryk University Journal of Law and Technology 8. 199-208. T. Bonaci, R. Calo, H. Chizeck, "App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces", May 23, 2014. IEEE International Symposium on Ethics in Science, Technology and Engineering, pp. 1-7, 2014, IEEE Technology & Society Magazine, Vol. 34, No. 2, pp. 32-39, 2015, University of Washington School of Law Research Paper No. 2788104, Available at SSRN: <https://ssrn.com/abstract=2788104>. B.J. Maiseli, L.V. Massawe, M. Mbise, K. Mkocho, N. Ally, M. Ismail, J. Michael, S. Kimambo, "Brain Computer Interface: Future, Challenges, and Potential Threats". BSPC-D-22-00311, Available at SSRN: <https://ssrn.com/abstract=4073630> or <http://dx.doi.org/10.2139/ssrn.4073630>

to autonomously communicate and physically interact with the environment around them. Without any doubt, this is a medical-engineering achievement that marks a life-changing milestone for so many people who have ended up paralyzed due to accidents or illness.

Indeed, BCI systems have been proven able to help patients to perform handwriting or to typewrite, despite the inability to move, simply by decoding the patient's imagined handwriting or spelling from recorded signals of neuronal activity¹². It results in better living conditions and the restoration of relational possibilities for them, including of relevant legal nature. Through these systems, it becomes indeed possible to establish a communication with subjects otherwise unable to express themselves; to determine whether they are conscious and able to voluntarily respond and make relevant decisions (e.g., informed consent in health care or making end-of-life decisions).

Such particular use of BCI devices raises some legal questions; namely, whether, under what conditions and to what extent, the individual's will, expressed through brain-computer interface communication methods, might or might not have legal value. The answer to this question is far from irrelevant and challenges the current notion of legal capacity: as mentioned in the previous paragraph, the subject who possesses intact mental competence, hitherto considered legally incapacitated just because physically unable to express their will, would regain (and be legally granted) the full right to self-determination in all relevant matters affecting them¹³.

4.2. BCI-mediated intention to create legal relations.

The personal will of an individual, for it to be accorded legal value, must be manifested - i.e., externalized - to reveal the purpose pursued or the arrangement of interests intended to be realized and regulated. A typical example is that of the manifestation of consensus for the conclusion of a contract. Normally, the intention of a subject to create some juridic consequences (e.g. the acceptance of an offer) must be expressed by way of declaration of intent (and meet all legal requirements) to have legal effects (and for the contract to be binding). This declaration can be expressed, manifesting the intention, e.g., through language - whether written or spoken - (as is normally the case), or implied by a behavior, that is a conduct that unambiguously makes tacitly manifest a specific intention (e.g., mouse click on a 'purchase' button).

Whereas this manifestation of will traditionally occurs through bodily and muscle movements, activated by neural activity, in the case of BCI-mediated declarations, that occurs by means of artificial systems, devices, or mechanical

¹² J. Xue, "Handwriting with brain computer interface" in J. Phys. (2021) Conf. Ser. 1865 042026; K. T. Huang, Z. B. Moses, J. H. Chi, "Advances in implanted brain-computer interfaces allow for independent communication in a locked-in patient, in *Neurosurgery* 80 (2017) 5, 30-31; P. Chaudharya, R. Agrawalb, "Emerging threats to security and privacy in brain computer interface", in *IJASSR*, Special Issue based on proceedings of 4th International Conference on Cyber Security, (2018).

¹³ R. Folgieri, "Brain computer interface and transcranial magnetic stimulation in legal practice and regulations", in A. D'Aloia, M. C. Errigo (eds.), "Neuroscience and Law. Complicated crossings and new perspectives" (Springer, 2020), 273; F. G. Pizzetti, "Brain-computer interfaces and the protection of the fundamental rights of the vulnerable persons", in A. D'Aloia, M. C. Errigo (2020), 291

prostheses on the impulse of executable commands resulting from a translation of those very same neural signals.

On a strictly phenomenological level, these BCI-mediated actions are, of course, suitable to express a legally binding will, as long as it is not equivocal; what raises some questions, however, is the artificial translation of patient's mental decisions into control signals and the level of accuracy of the analysis and decoding of their bioelectrical brain activity.

4.3. A legal standpoint: the need for accuracy. Critical issues and key requirements.

In BCI operation, of any kind, 4 stages can be outlined¹⁴:

- 1) brain signal acquisition;
- 2) feature extraction;
- 3) feature translation;
- 4) device output;

Each of these steps involves a margin of error. Initially, a recording interface (e.g., electrodes) tracks neural signals reflecting the subject's intent embedded in the on-going brain activity (EEG, etc.); therefore, this information is automatically processed twice: first, an algorithm analyzes the data to map and classify electrophysiological features and filter those having strongest correlations with the user's intent that will be used to control the BCI (thus eliminating 'noise' and irrelevant activity); then, a second algorithm translates the extracted signal features into executable device commands. These commands eventually activate a device that will produce a certain output: letter writing, movement of a cursor¹⁵, operation of a prosthetic arm, etc. Errors could occur at each of these stages; the neural information collected could be not sufficiently accurate or complete (e.g., because of the obsolescence of an implanted interface that has been in place for some time) and thus result in a crucially flawed automatic processing as a consequence; the algorithms may not be properly trained or be biased; the device could end up responding to neural activity accidentally (and not willfully) produced or misinterpreted.

Not only that, on an ethical level, a high level of accuracy is particularly important in situations where the system could directly impact human lives, potentially causing harm; accuracy, but also traceability and transparency at every stage of BCI model construction (especially when AI is involved) are also very relevant on a legal level. If, indeed, a certain level of reliability about the consistency between the subject's will and its BCI-mediated manifestation cannot be demonstrated, it is very difficult for a will or consent that are so manifested to be considered legally valid (and the paralyzed person, therefore, legally capable). In a not-so-different case, for example, the Italian

¹⁴ S. S. Borikar, S. R. Kochre, Y. D. Zade, "Brain computer interface", in NCETMS (2014), 1-4

¹⁵ P. Nuyujukian et al., "Cortical control of a tablet computer by people with paralysis", PLoS ONE 13(2018)11

Guardianship Judge of Sassari declared able to legally self-determinate a patient suffering from Amyotrophic Lateral Sclerosis (ALS) who was using an eye-controlled device to communicate, basing their decision on a technical assessment of 'consistency' between the tool-mediated manifestation of will and what the patient wanted to express. As Pizzetti (2020) states¹⁶, according to this ruling, a biotechnological communication device, as the BCI-based ones, may be considered legally reproducing a person's will only where, after a proper evaluation, it can be considered technically 'suitable' to realize an effective and reliable directly-from-the-brain communication, which can be considered surely 'attributable' to the subject.

To meet this requirement, more accurate systems can be developed implementing adaptive algorithms, which are also capable of detecting patterns related to response errors and conflicts in decision making, thus acting as an automatic decision controller in real time, improving BCI performance. In any case, it is important, when occasionally inaccurate algorithmic processing cannot be avoided, to ensure that at least the system is able to indicate the probability of these errors.

It should be acknowledged, actually, that many of the published trial results report rather encouraging average error rates; even significantly better where auto-correct mechanisms are provided¹⁷; however, it has to be considered that these experimentations took place in a controlled environment and applying systems trained on the specifics of each individual selected tester: it is entirely unpredictable what might happen in a normal setting, under presence of more disturbing factors, and in case of broad unsupervised use.

Lastly, BCI systems are exposed to possible misuse and cyberattacks, which can easily result in intentional or unintentional alteration of their functioning¹⁸.

The assessment of this risks' impact on fundamental human rights, is finally essential. In fact, even the use of an assistive or augmentative communication device capable of expressing a perfectly reliable individual's will must in fact be evaluated – for it to be granted a legal value - by balancing all the benefits (e.g, the right to communicate and self-determine) and risks (for the fundamental rights involved). This will be addressed in the following section.

4.4. A risk-based classification model and approach.

Based on the critical issues and key requirements as set out in the previous sections, this section proposes a self-assessment strategy to operationalize BCI technologies applied or potentially applicable to the context of legal relations

¹⁶ F. G. Pizzetti, "Brain-computer interfaces and the protection of the fundamental rights of the vulnerable persons", in A. D'Aloia, M. C. Errigo (2020), 291

¹⁷ J. Xue, "Handwriting with brain computer interface" in J. Phys. (2021) Conf. Ser. 1865 042026; K. T. Huang, Z. B. Moses, J. H. Chi, "Advances in implanted brain-computer interfaces allow for independent communication in a locked-in patient, in Neurosurgery 80 (2017) 5, 30-31; P. Nuyujukian et al., "Cortical control of a tablet computer by people with paralysis", PLoS ONE 13(2018)11

¹⁸ I. Olaronke et al., "Prospects and problems of brain computer interface in healthcare", CJAST, 29(2018)6, 1-17; Chaudharya, R. Agrawalb, "Emerging threats to security and privacy in brain computer interface", in IJASSR, Special Issue based on proceedings of 4th International Conference on Cyber Security, (2018).

and juridic self-determination, implementing methods of technology risk evaluation and management.

The proposal - standing at this stage as a work-in-progress developing approach - consists, in particular, in a risk-based BCIs classification model, which provides - for each item given (i.e., a critical issue) - the attribution of a progressive score (1;2;3.) according to increasing level of associated potential risk, where risk means the misalignment between the user's negotiating will and its BCI-mediated manifestation. The highest misalignment item-associated risk will be assigned a value of 3; the lowest will be assigned a value of 1 (TABLE I).

TABLE I.

ITEM	- Risk ^a Level score +		
	1 (low risk)	2	3(high risk)
Technique used and accuracy of brain signal acquisition	<Accurate> ^b	<Acceptable>	<Inaccurate>
Feature extraction method/s	< >	< >	< >
Machine-learning algorithm accuracy and traceability	<Sufficient>	<Acceptable>	<Insufficient>
Adaptive model and auto-correct method/s implementation and responsiveness	<Adequate>	<Acceptable>	<Inadequate>
Scalability and resistance to disturbing /interfering factors in uncontrolled setting	<High>	<Medium>	<Low>
Propensity to misuse	<Low>	<Medium>	<High>
Resilience to attack and security	<High>	<Medium>	<Low>

^a. The risk is represented by the misalignment between the user's will and its BCI-mediated manifestation.

^b. The words in brackets <...> represent the to-be-defined technical-legal parameter of reference by which to make the classification.

The model is addressed to developers and users of contracting BCIs, so that it can be of guidance in the design of these systems or in the adoption of appropriate-to-the-case mitigation measures or documentation practices. The model is also believed to be a useful tool for policy-makers to consider where they intend to intervene with an ad hoc regulatory framework guided by a balanced and proportionate horizontal approach that is limited to the minimum requirements necessary to address BCI-related risks, without unreasonably hindering or making excessively costly their technological development.

The research will proceed by defining for each level of risk related to a given item, a precise technical-legal parameter of reference by which to make the classification. A search and analysis of the principal scientific publications and

studies related to the design and testing of BCI applications that are eligible for the proposed model will be conducted.

A different, but interconnected classification model might instead consider the level of impact of BCI applications on human rights and from an ethical and social sustainability perspective.

TABLE II.

Impact area	- Ethical/Human rights impact score +		
	1(<i>low impact</i>)	2	3(<i>high imp.</i>)
Application /domain	<therapy> ^d	<recreational>	<human enhancement>
User Safety	<high>	<medium>	<low>
Interface invasiveness	Non-invasive	Semi-invasive	Invasive
Potential harm (fundamental rights impact)	<low risk>	<acceptable risk>	<high risk>
Propensity to misuse	<low>	<medium>	<high>

^c. The score represents the level of impact of a given BCI tool (from low to high) on the human rights involved as defined in each relative impact area.

^d. The words in brackets <...> represent the to-be-defined technical-legal parameter of reference by which to make the classification.

The model proposed here (TABLE II) involves, in particular, an increasing scoring scheme (from 1 to 3) in proportion to the level of impact (from minor to major) on the human rights involved¹⁹ and certain ethically critical areas²⁰. The purpose of the model is to facilitate a risk-benefit analysis in the context of the human rights framework that can orient possible judicial decisions and policy choices aimed at balancing them fairly.

Indeed, the benefit/risk ratio is the ultimate prerequisite for BCI-communicative applications to be compatible with the legal system and for the individual's will expressed through their use to be considered of legal value. In fact, in general, the assessment and possible acceptability the risk represented is determined in relation to the possible benefits²¹.

The research will proceed with the definition of all relevant "impact areas," meaning the fundamental rights and principles exposed to be either fulfilled or threatened by the use of BCIs.

To this end, for example, the right to self-determination and communication, as well as the right to mental and physical health and well-being or privacy and

¹⁹ A. D'Aloia, M. C. Errigo (eds.), "Neuroscience and Law. Complicated crossings and new perspectives" (Springer, 2020)

²⁰ I. Olaronke et al., "Prospects and problems of brain computer interface in healthcare", CJUST, 29(2018)6, 1-17; A. Coin, M. Mulder, V. Dubljevic, "Ethical aspects of BCI technology: what is the state of the art?", Philosophies, 5 (2020)31

²¹ M. C. Errigo, "Neuroenhancement and law", in A. D'Aloia, M. C. Errigo (2020), 189

data protection, will be considered, now as justification, now as a limitation on the use of tools. Newly created rights and principles proposed by some scholars in response to the emerging issues of neurotechnologies will also be considered²².

For each level of impact related to a given area, a precise technical-legal parameter of reference will be then defined to guide the classification. Example of such a parameter is, e.g., the definition, reconstructed on the basis of the prevalent scientific literature, of the difference between therapy (that could be defined, for example, according to some²³ as the use of BCI for treatment of individuals affected by diseases, disabilities or other impairments to restore their natural health status) and enhancement (which could be defined, on the contrary, as the use of BCI beyond what it is necessary to maintain or restore their natural health status).

²²M. Ienca, R. Andorno, "Towards new human rights in the age of neuroscience and neurotechnology", *Life Sciences, society and Policy*, [2017]

²³ M. C. Errigo, "Neuroenhancement and law", in A. D'Aloia, M. C. Errigo (2020), 189



Keywords: BCI regulatory perspectives; security; privacy; cybersecurity.

Summary: [1. Introduction and background of the research study.](#) – [2. Methodology of the research.](#) - [3. Critical analysis of the legal issues related to BCI applications and presentation of the tool prototype.](#) - [3.1. First part of the tool prototype: Liability rules and BCI, with particular regard to user's safety.](#) – [3.2. Second part of the tool prototype: The processing of neural and mental data.](#) – [3.3. Third part of the tool prototype: BCI technologies and cybersecurity profiles.](#) – [4. Conclusion and future work.](#)

1. Introduction and background of the research study.¹

In medical and educational fields, in workplaces, as well as more generally, in interpersonal relationships, the Brain Computer Interface (BCI) had an ever wider and faster development thanks to the implementation of the AI system². This occurred, for example, in the case of the neural interfaces that are able to monitor the stress conditions or other negative and positive human emotions, or the technologies used in the medical rehabilitation field (therapeutic BCI), also using wearable technologies. The neurotechnology used in verifying the level of involvement and understanding of the teaching contents by the learners, or those used by individuals to express their will in relationships between private individuals, are also very relevant.

The BCI can be very useful for assisting and protecting people in different environments, but an evaluation of BCI applications appears necessary to define the legal consequences of the individual's behaviours using BCI devices.

¹ The paper is the result of the work of a selected team of researchers of the Research Centre of European Private Law (ReCEPL) at Università degli Studi Suor Orsola Benincasa, coordinated by the ReCEPL Director Prof. Lucilla Gatt and the ReCEPL Vice-Director Prof. Ilaria A. Caggiano.

The work was presented at the IEEE International Conference 'Metrology for eXtended Reality, Artificial Intelligence, and Neural Engineering' (MetroXRINE), National Research Council, Rome, October 26-28, 2022, and published in the IEEE MetroXRINE 2022 Proceedings, 551-556; awarded as 'Best paper presented by a young researcher' from MetroXRINE scientific committee, thanks to the support of Micron.

The author of paragraphs 1, 2, 3.1, and 3.3 is Dr. Maria Cristina Gaeta, ReCEPL Senior Researcher and Scientific Secretary, Lecturer in Private Law at Università degli Studi Suor Orsola Benincasa; the author of paragraphs 3.2. and 4 is Dr. Anna Anita Mollo, ReCEPL Senior Researcher and Postdoctoral Research Fellow at Scuola Superiore Meridionale.

² N Liv, 'Neurolaw: Brain-Computer Interfaces' (2021) 15 (1) U. St. Thomas J.L. & Pub. Pol'y, 328-355.

This evaluation will help to verify the risk for individuals interacting with these technologies, to guarantee consequent adequate protection.

Indeed, the considerable potential of BCI is evident but, at the same time, the rapid spread of these neural technologies requires the analysis of multiple issues that can arise from the application of BCI devices or their software, to verify and measure the risks that can arise from these new technologies, and guarantee the compliance by design of the BCI application under an anthropocentric point of view. In this regard, legals have the role to verify the functioning of BCI technologies and regulate them to protect human beings in the digital environment, alias artificial, since this environment places ontologically the former in a position of vulnerability. The category of "vulnerable individuals" includes, in fact, all natural persons, who, acting in a digital environment, are exposed to the risk of damages for various reasons (minor/old age, asymmetry of contractual power or information, patients with serious diseases). This vulnerability of individuals, strictly related to the development and application of new technologies can be defined as technological vulnerability.

2. Methodology of the research.

The research activities in the field of BCI have been carried out at the Research Centre of European Private Law - ReCEPL,³ based at Università degli Studi Suor Orsola Benincasa (Italy).

In the perspective of uniform regulation, also considering the opportunities for its effective implementation in specific sectors, ReCEPL develops research itineraries on the relationship between law and new technologies, working in close collaboration with the Living Lab Utopia, of the Interdepartmental Research Center 'Scienza Nuova',⁴ also based at Università degli Studi Suor Orsola Benincasa (Italy).

The equipment of the most modern technological instruments of the 'Scienza Nuova' Center, allows ReCEPL researchers to adopt innovative research and study methodologies (empirical studies, behavioral analyses), conducted jointly with researchers (engineering, psychologists, communication sciences, statisticians), that belong to 'Scienza Nuova' Research Center and are fundamental for the application of mixed methodologies applied for the design and implementation of the tool prototype.

More in detail, starting from a critical analysis of the state of the art (legislation, case law, literature and research studeis), the research team has identified, mapped, and evaluated the possible risks related to BCI applications and their legal regulation, to then create the tool prototype that aims to verify the compliance by design.

Furthermore, the research method adopted has been hybrid (hybridization of knowledge), using not only the traditional legal methods but also the

³ For more details on the Research Centre of European Private Law see <https://www.unisob.na.it/ateneo/c008.htm?vr=1&lg=en>

⁴ For more details about Scienza nuova see www.centroscienzanuova.it

human-machine-interface and user experience approach (HMI&UX), as well as empirical legal studies method (ELS). Indeed, to carry out an impact assessment, it is important to really understand how new technologies work. In this light, it has been essential to resort to the behavioural sciences, and technical science, starting with practical applications of BCI.

In the 21st century, the level of an in-depth study of the new technology law is so high and complex that legal must work in synergy with experts from other sectors of science (e.g. engineers, computer scientists, psychologists and philosophers). As a matter of fact, on one side, legal science needs technical science to understand technologies and provide specific regulations based on their functioning. On the other side, technical science needs the legal and social one for putting in place the principles of techno-regulation based on current law, first of all, hard law, but also soft law, which in this context plays a fundamental role of guidance and orientation, as well as technical regulation (e.g. standards).

3. Critical analysis of the legal issues related to BCI applications and presentation of the tool prototype.

To verify and measure the possible risks related to the use of BCI technologies the research team has realised a prototype tool on the legal assessment of BCI applications, that serves as an operational tool for manufacturers to enable them to assess the level of product safety and reliability before they are put on the market. As a matter of fact, all BCI applications must be structured according to the principle of legal compliance by design, submitting BCI applications to the evaluation tool in advance, before making them available to the public and, even earlier, during the production phase.

In this light the prototype of the evaluation and measurement tool has been divided into the following parts that correspond to the main risks for the individuals using BCI application: the first part on BCI safety; the second part on BCI privacy, third part on cybersecurity, representing the main types of risks associated with the use of BCI technologies.

Figure 1 – Scheme of the prototype of evaluation and measurement tool of BCI applications

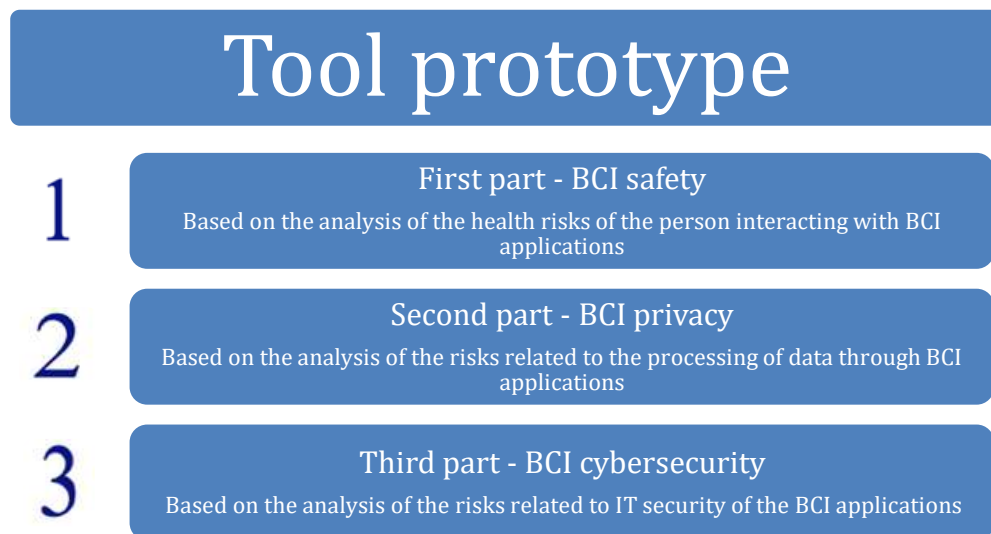


Figure 1 – Scheme of the prototype of evaluation and measurement tool of BCI applications

The paper critically analyses these risks explaining the choices made in identifying the matters of the prototype tool, that consists in an interactive questionnaire made by digital software, whose results are visible in real-time at the end of the questionnaire.

3.1. First part of the tool prototype: Liability rules and BCI, with particular regard to user's safety.

From a legal perspective, the possibility of damage (mainly of a non-pecuniary nature) for the user interacting with BCI technologies or other human beings who interact with the user using BCI, is high. Among the possible risks associated with the use of BCI, there is a high possibility of injury to the user's safety, who could suffer physical or psychological injury related to the incorrect use of neural technologies.⁵ At the same time, it is also possible that damages to surrounding objects are caused. In these cases, it is foreseeable also a pecuniary damage.

Under the perspective of private law, the configurable typologies of civil liability are the following: civil liability for non-pecuniary damage and civil liability for pecuniary damage. Artt. 2043 and ff. of the Italian Civil Code, regulate the civil liability for pecuniary damage. These legal provisions also include art. 2059 of the Italian Civil Code, that governs the case of non-pecuniary civil liability, which can be compensated only in cases determined by law.

When the relationship is between the producer of the BCI application and the user (the physical person who uses these technologies) the applicable regulation is that of the Consumer Code (Italian Legislative Decree 6

⁵ Q Li, D Ding, M Conti, 'Brain-Computer Interface applications: Security and privacy challenges' (2015) IEEE Conference on Communications and Network Security (CNS), 663-666.

September 2005, no. 206), which currently implement in Italy the European Directive 85/374 /EEC on liability for damage from defective products (so-called Product Liability Directive, acronym PLD), after the repealing of the previous national regulation (d.P.R. n. 224/1988).

Article 114 cons. Code (art. 1 PLD) establishes that the manufacturer is responsible for the damage caused by defects in his product, while art. 115 cons. Code (art. 2 PLD) states that by product we mean any movable property, even if incorporated into another movable or immovable property and that electricity is also a product. It is therefore evident that BCI applications can fall within the notion of product, for which the producer is responsible, in relation to the consumer. The manufacturer is the physical person or legal person who designs and manufactures BCI technologies, as well as who informs about the permitted uses of such applications (art. 2, para bis, cons. Code, in compliance with art. 3 PLD).

Unlike the general discipline of the civil code, the consumer code, as well as the PLD, provides for the strict liability of the producer.⁶ This is a type of liability for which the producer is liable if the consumer proves the damage, the product defect and the causal link between defect and damage. The product is defined as defective when it does not offer the security that can be expected considering all the circumstances and in particular those indicated in art. 117 cons. Code (art. 6 PLD). To mitigate the producer's strict liability there are the causes of exclusion of liability referred to in art. 118 cons code (art. 7 PLD), but these are mandatory hypotheses subjected to the burden of proof by the manufacturer.

It is therefore evident that the producer's strict liability is directly related to the safety of the product and provides for compensation for damage under favorable conditions for the consumer, compared to the ordinary discipline of civil liability, in consideration of the weak position of the consumer. In order to avoid the producer liability, it is important to carry out an *ex ante* verification of product safety, before putting it on the market.

For this reason, the first part of the tool is focused on BCI safety. More specifically, in the section 1.1. are analysed the possible physical or psychological injury for the individuals who use BCI application (e.g. individuals who use the BCI because they have disabilities that can be overcome using BCI technologies, as well as individuals who undergo some tests such as those to check the level of knowledge and understanding or monitor the stress conditions or other negative and positive human emotions). In the section 1.2. are analysed the possible injuries caused to another human being and surrounding environment that interacts with individuals using BCI applications (e.g. relationships with a people whose cognitive and movement abilities are supported by BCI devices with particular regard to the consequences of their action).

⁶ C Bublitza, A Wolkensteinb, RJ Joxc, O a Friedrichd, 'Legal liabilities of BCI-users: Responsibility gaps at the intersection of mind and machine?' (2019) 65 International Journal of Law and Psychiatry, 101-399.

First part of the tool prototype

- Individuals using BCI applications
- Other human beings and surrounding environment in the interaction with individuals using BCI applications

Figure 2 – Scheme of the first part of the prototype tool for the evaluation and measurement of BCI applications

In the context of the physical or psychological injury of the individuals, two possible specific risks are outlined: the first concerns the unlawful processing of personal data through brain computer interface technologies, and mainly concerns non-pecuniary damages, while the second concerns the cybersecurity breach of brain computer technologies, which can result in both pecuniary and non-pecuniary damages.

3.2. Second part of the tool prototype: the processing of neural and mental data.

A central point in the analysis of the risks that BCI systems may cause relates to the exact identification of the type of data they are able to detect by recording and decoding the user's brain activity.

In this regard, it is necessary to make a brief premise on the functioning of BCI interfaces, which is articulated in four phases: after the generation of an initial input (first phase), i.e. a brain activity by the user in response to a stimulus, this is first recorded and then decoded by the interface (second phase); in this way, the initial input is transformed by the interface into an output (third phase), i.e. in the execution of a precise function that the individual will be able to perform autonomously thanks to the BCI device (fourth phase). In the clinical field, think of the control of a robotic limb or of

an electronic wheelchair; expression of one's will in full autonomy thanks to the help of the interface).⁷

In this process, the third phase appears central as the data measured in the previous phase are classified and selected in order to identify the most appropriate output for the proper functioning of the BCI interface.

Such data can be distinguished into neural data and mental data. Neural data or "human brain data"⁸ pertain to the structure and functioning of the brain and can reveal information on the clinical condition and, therefore, on a person's health - think of BCI used in clinical fields- understood in a broad sense, i.e. also including a condition of well-being and not pathological.

Mental data, on the other hand, are additional and distinct data from neural data, pertaining to the more intimate sphere of the subject. This category therefore includes any data that can be organized and processed to infer a person's mental states⁹, including their cognitive and affective states such as inner speech,¹⁰ memories,¹¹ emotions¹² and intentions.¹³

In neural interfaces, mental data are derived from the analysis of neural data by means of the so-called 'reverse inference' procedure,¹⁴ which does not show the semantic content of a thought or memory but allows a correspondence to be established between the neural correlates of a certain brain activity and information about certain mental states.

For the purposes here, the distinction between neural data and mental data appears necessary in order to identify the legal nature of the data that BCI devices are able to detect in function of an analysis that extends to the privacy protection profile also in relation to the domain of the mind.

Neural data, referring to the functioning and structure of the brain, make it possible to identify the subject they refer to, suggesting, therefore, a first legal

⁷ U Chaudhary, I Vlachos, JB Zimmermann, et al., 'Spelling interface using intracortical signals in a completely locked-in patient enabled via auditory neurofeedback training' (2022) 13 (1236) *Nature Communications*, 1-9.

⁸ M Ienca, *Common Human rights challenges raised by different applications of neurotechnologies in the biomedical fields*, (SPDP, Council of Europe, 2021).

⁹ M Ienca, G Malgieri, 'Mental data protection and the GDPR' (2022) 9 *Journal of Law and the Biosciences*, 1-19.

¹⁰ DA Moses, M.K. Leonard, JG Makin, EF Chang, 'Real-time decoding of question-and-answer speech dialogue using human cortical activity' (2019) 10 (3096) *Nature Communications*, 1-14.

¹¹ J Chen, YC Leong, CJ Honey, CH Yong, KA Norman, U Hasson U, 'Shared memories reveal shared structure in neural activity across individuals' (2017) 20 *Nature neuroscience*, 115-125.

¹² A Tambini, U Rimmele, EA Phelps, L Davachi, 'Emotional brain states carry over and enhance future memory formation' (2017) 20 *Nature Neuroscience*, 271-278.

¹³ M Bles, JD Haynes, 'Detecting concealed information using brain-imaging technology' (2008) 14 *Neurocase*, 82-92.

¹⁴ RA Poldrack, 'Inferring mental states from neuroimaging data: from reverse inference to large-scale decoding' (2011) 72 *Neuron*, 692-697.

qualification of the same as personal data within the meaning of Article 4(1) of the GDPR.¹⁵

However, as such, neural data are also an expression of a clinical condition of the data subject, the latter not necessarily understood as a condition of a pathological nature but also expressive of a situation of physical and mental well-being.¹⁶

Therefore, neural data are not merely personal identification data but 'health-related data' within the meaning of Article 4(15) GDPR. From this it follows that the legal basis of the processing is to be found in Art. 9 GDPR for that 'special category of personal data' for which there is enhanced protection, which takes the form of the 'explicit consent' of the data subject.

The qualification in terms of personal data, on the other hand, is not peaceful in relation to mental data. The latter, in fact, if linked to other data allowing the certain identification of the data subject (as in the case of neural data), may qualify as personal data (neural interfaces used in the clinical field).

In this first case, the close link between the neural data and the mental data suggests a qualification of the latter as personal data, since the joint reading with the neural data is capable of allowing the identification of the data subject.

The doubt as to the qualification of mental data arises with greater force in hypotheses in which it is acquired outside the clinical sphere, as in the case of consumer neurotechnologies, which could detect mental data even though they do not directly access the functioning of the brain understood as a biological complex. In this second case, a valid normative reference seems to be found in Article 4(1) GDPR, which also considers as suitable for identifying the subject 'one or more elements characteristic of his or her psychic identity', although the same provision does not clarify what is meant by psychic identity. Therefore, only by way of interpretation can mental data be qualified as personal data at present, i.e. where it is possible to consider that an emotion or a memory is data that can unambiguously identify a subject, even without referring to his or her neural data.

As to the possible legal basis for processing mental data where these are not read in conjunction with neural data, as in the case of consumer neurotechnologies, it must be noted that in this case mental data cannot be qualified as health data since they cannot by themselves show the state of health (albeit physiological and not pathological) of the person concerned.

There would therefore remain the possibility of access to the greater protection of Article 9 GDPR only where the mental data are also capable of revealing the racial or ethnic origin, political opinions, religious or philosophical beliefs or sexual orientation of the person with a disability.

¹⁵ S Raiuney, K McGillivray, S Akintoye, T Fothergrill, C Bublitz, B Stahl, 'Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?' (2021) 7, *Journal of Law and Biosciences*, 1-19.

¹⁶ G Malgieri, G Comandé, 'Sensitive-by-Distance: Quasi-Health Data in the Algorithmic Era' (2017) *Inf. Commun. Technol. Law*, 229-249.

This case, i.e. mental data that is not linked to neural data and, therefore, qualifies as health data, is not envisaged in our GDPR, which is characterised by an obvious lacuna in that it does not define. In this regard, some authors believe that the lacuna is due to the failure to include in the regulatory provision of Article 9 GDPR data relating to thoughts, emotions and other mental states that are not connected with or cannot be attributed to health or other areas covered by the provision.¹⁷ According to a different approach, on the other hand, it is necessary to start from the consideration that the special data referred to in Article 9 GDPR are such in light of the purpose of the processing; therefore, it is considered that if the purpose of the processing of mental data initially declared is not related to health, or to other purposes contemplated by the norm, the same cannot be considered sensitive data.¹⁸

In any case, the element that emerges is that the legal basis of the processing can currently only be found in Article 6 GDPR, which indicates in which cases non sensitive data can be the subject of lawful processing if certain conditions indicated by the norm (consent, performance of a contract, compliance with a legal obligation, protect the vital interests of the data subject or of another natural person, public interest, legitimate interests pursued by the controller or by a third party) are met.

In conclusion, the considerable implications in the protection of mental privacy¹⁹ call for adequate ethical and legal reflection aimed at assessing the concrete functioning of such devices. This would seem to be possible on the basis of an evaluation questionnaire intended to measure not only the security and reliability of current BCI devices, but also the level of risk awareness on the part of the user.

¹⁷ M Ienca, G Malgieri, 'Mental data protection and the GDPR' (2022) 9 Journal of Law and the Biosciences, 1-19.

¹⁸ S Raiuney, K. McGillivray, S Akintoye, T Fothergrill, C Bublitz, B Stahl, 'Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?' (2021) 7 Journal of Law and Biosciences, 1-19

¹⁹ M Ienca, 'Common Human rights challenges raised by different applications of neurotechnologies in the biomedical fields', 1-82.

Second part of the tool prototype

- Data subject and data qualification
- Data protection qualification
- Scope of the processing

Figure 3 – Scheme of the second part of the prototype tool for the evaluation and measurement of BCI applications.

In this regard, the second part of the prototype of the evaluation tool will focus on privacy issues in relation to BCI applications. This should comprise an overview of all planned data collection and processing operations in order to develop secure data management practices and share and process data in compliance with GDPR and best security standards

Particular attention will be paid to understand if BCI system assuring effective transparency in information through suitable forms and devices; and on the verification of the level of user awareness of the possible risks of BCI systems.

In particular, the second part of the questionnaire is divided into three sections. Section 2.1. on data qualification is focused on: data subjects (vulnerable people, people who have not given their explicit consent etc.) and types of data for the legal qualification of the data processed by BCI applications, to understand whether or not data related to brain activity - neural data and mental data – are qualified as personal data.

Section 2.2. is based on data protection qualification, also through the application of the principles of data protection by design and by default. In this part of the questionnaire, the processing techniques of neural and mental data is identified. In this section the focus is on; identification of the type of IT tool used in the processing; any automated decision-making processes; the pseudonymization or anonymization of personal data; data minimization.

Finally, in section 2.3. is deepened the scope of the processing. The questions are structured so as to understand the purpose of the processing of the data recorded by BCI's applications in order to: identify the correct legal basis for the processing; assess whether the processing is lawful or not.

3.3. Third part of the tool prototype: BCI technologies and cybersecurity profiles.

In relation to BCI application is also very relevant to analyse the possible injuries that could result to the user in the case of a violation of the IT security of BCI technologies.²⁰ This case can occur for the malfunctioning of IT security systems (section 3.1.) or for the hacking of the IT security systems (section 3.2.),²¹ resulting in consequent physical or psychological damage to the user, including the unlawful processing of the personal data stored or transferred for software to another software (interoperability).

Currently, there is no unitary and complete regulation on IT security but the EU Directive 2016/1148 (Directive on the Security of network and information systems, acronym NIS, implemented in Italy with the Italian Legislative Decree of May 18, 2018, n. 65), was an important landing place. The regulation aims at improving national cybersecurity capabilities and provides for cooperation at the EU level. It also envisaged the establishment of the Cyber Security Incident Response Teams (CSIRT), to deal with incidents and risks, as well as the NIS Toolkit which provides practical information to member states. Furthermore, a culture of safety and risk management in all sectors which are vital to the economy and society has been straightened. Sectors that strongly depends on Information and communication technologies (ICT) include the healthcare, digital infrastructure and cloud computing sector.

Furthermore, among the regulation recently adopted for cybersecurity, the Cybersecurity Act (Reg. 2019/881/EU) is of fundamental importance. Indeed, the Regulation aimed at creating a European framework for the certification of the cybersecurity of ICT products and digital services, and at strengthening the role of the European Union Agency for the Cybersecurity (ENISA). At the national level, in 2019, the competent NIS Authorities in the Ministries have developed the national Guidelines for risk management and accident prevention and mitigation, which have a significant impact on the continuity and provision of essential services.

Therefore, the European and national attention on cybersecurity is evident, considering the increasing possibility of risks for individuals. This is why the tool also takes into consideration aspects concerning IT Security also in the light to provide a cybersecurity certification. In this regard, the third part of the tool prototype is focused on cybersecurity and is divided into a section 3.1. on malfunctioning of IT security systems and a section 3.2. on the hacking of the IT security system.

²⁰ Ajrawi, R Rao, M Sarkar, 'Cybersecurity in Brain-Computer Interfaces: RFID-based design-theoretical framework' (2021) 22 Informatics in Medicine Unlocked, 1 - 9.

²¹ S López Bernal, A Huertas Celdrá, G Martínez Pérez, M Taynnan Barros, S Balasubramaniam, 'Security in Brain-Computer Interfaces: State-Of-The-Art, Opportunities, and Future Challenges' (2020) J. ACM, 1-35.

Third part of the tool prototype

- malfunctioning of IT security systems
- hacking of the IT security systems

Figure 4 – Scheme of the third part of the prototype tool for the evaluation and measurement of BCI applications

4. Conclusion and future work.

The current legal framework does not provide for specific regulation of neurotechnology in relation to the distinct profiles mentioned above: security, privacy and cybersecurity.

It is clear that the preventive legal analysis of BCI devices and related risks is necessary in order to avoid situations of 'technological vulnerability' against which the legal system is unable to guarantee adequate protection for the individuals.

The creation of the tool prototype described in the paper appears, therefore, to be an innovative but necessary approach to the proper techno-regulation in order to guarantee the legal compliance of BCI products.

The production of BCI devices that is genuinely human-centred will be possible only if technical evaluations are flanked by legal ones, which must be founded on an analysis method that does not stop at theoretical reflection but opens up to a phase of integrated juridical thought in bioengineering testing, in which the design of prototypes, products, or services is inspired by a set of minimum standards (legal and ethical), so that major tech companies bring to market products according to the existing regulatory framework.

The aim is to prevent a possible 'abuse of technology' to the detriment of the progress and the benefits it can bring to vulnerable people.

Therefore, a new approach is needed to be able to offer the most appropriate protection for all interests involved: the protection of vulnerable people, especially in the clinical field, by stimulating clinical research with BCI devices for the diagnosis and treatment of severe neurodegenerative diseases, thus improving the quality of life of the patients involved; maximising the level of reliability of BCI systems, making them safe and increasing the level of confidence of users (including consumers); supporting manufacturers by providing them with precise ethical and legal standards to make products compliant with both binding European and international legislation on the protection of human rights and vulnerable consumers, and with the most appropriate soft law instruments.

All this requires a highly interdisciplinary work, in which the skills of experts from various fields of knowledge dialogue together in order to achieve the same goal: the psychophysical integrity of the human person even in the technological context.



New machine behavior's evolutionary approaches between AI learning, control and ethics promoting cooperative Human-Machine Intelligence

SERGIO GUIDA ^{ID}

Independent Scholar, Data Gov. & Privacy(Sr Mgr), eHealth, Behavioral AI

Abstract

The technological revolution in the fields of robotics and artificial intelligence seems to indicate a future shift in our human-centered social paradigm towards a greater inclusion of artificial cognitive agents in our everyday environments. Understanding AI agents goes beyond the interpretation of a specific algorithm and requires analyzing the interactions between agents and with their surroundings. Combining AI and behavioral science is then seen in its true potential, as an ethical way to improve people's lives, where end users can feel safe when sharing personal data for transparent and relevant services.

La rivoluzione tecnologica nei campi della robotica e dell'intelligenza artificiale indicare un cambiamento futuro nel nostro paradigma sociale centrato sull'uomo verso una maggiore inclusione di agenti cognitivi artificiali nei nostri ambienti quotidiani. La loro comprensione va oltre l'interpretazione di un algoritmo specifico e richiede l'analisi delle interazioni tra gli agenti e con l'ambiente circostante. La combinazione di intelligenza artificiale e scienza comportamentale va quindi vista nel suo vero potenziale, come un modo etico per migliorare la vita delle persone, che possono sentirsi al sicuro quando condividono i dati personali per servizi trasparenti e pertinenti.



Keywords: Artificial agents, evolutionary robotics, machine behavior, hybrid intelligence, saliency maps, adaptive robots, neuroevolution, collaborative behavior.

Summary: [1. Introduction.](#) – [2. The behavior of the machines.](#) – [3. New evolutionary approaches.](#) – [4. The most recent developments.](#) – [5. Conclusions.](#)

1. Introduction.

The technological revolution taking place in the fields of robotics and artificial intelligence seems to indicate a future shift in our human-centered social paradigm towards a greater inclusion of artificial cognitive agents in our everyday environments. Collaborative scenarios between humans and robots will become more frequent and have a deeper impact on everyday life.¹

In one of the best examples of the evolutionary robotics' potential, the authors² used physical robots equipped with motors and sensors to conduct various evolutionary models and fitness goals. They concluded that 'these examples of experimental evolution with robots verify the power of evolution by mutation, recombination and natural selection. In all cases, the robots initially exhibited completely uncoordinated behavior because their genomes had random values'.³ In summary, the study concluded that 'a few hundred generations of random mutations and selective reproduction were sufficient to promote the evolution of efficient behaviors in a wide range of environmental conditions'.⁴

This kind of evolution is also illustrated by Alphabet's recent release of over 100 daily robot prototypes in Google's offices, which is still under development.⁵

¹ Cf. S Vinanzi, M Patacchiola, A Chella, A Cangelosi, 'Would a robot trust you? Developmental robotics model of trust and theory of mind' (2019) Phil. Trans. R. Soc. B 374: 20180032, in <https://royalsocietypublishing.org/doi/pdf/10.1098/rstb.2018.0032>, 1.

² Cf. D Floreano, L Keller, 'Evolution of Adaptive Behavior in Robots by Means of Darwinian Selection' (2010) PLoS Biol 8 (1): e1000292, in <https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.1000292>.

³ *Ibid.*

⁴ *Ibid.*

⁵ 'Google's parent company Alphabet announced today that its *Everyday Robots Project* — a team within its experimental X labs dedicated to creating 'a general-purpose learning robot' — has moved some of its prototype machines out of the lab and into Google's Bay Area campuses to carry out some light custodial tasks. 'We are now operating a fleet of more than 100 robot prototypes that are autonomously performing a range of useful tasks around our offices' said Everyday Robot's chief robot officer HP Brøndmo in a blog post (<https://x.company/blog/posts/everyday-robots>). (..) The big promise that's being made by the company is that machine learning will finally enable robots to operate in 'unstructured' environments like homes and offices. (..) Think about it: you may have seen robots from Boston Dynamics performing backflips and dancing to The Rolling Stones, but have you ever seen one take out the trash? It's because getting a machine to manipulate never-before-seen objects in a novel setting (something humans do every day) is extremely difficult. This is the problem Alphabet wants to solve', in J Vincent, 'Alphabet is putting its prototype robots to work cleaning up around Google's offices' (2021) The Verge, Nov 19, in <https://www.theverge.com/2021/11/19/22791267/alphabet-google-everyday-robot-project-cleaning-office-prototype> accessed 4 February 2022.

In truth, evolutionary robotics is not a new concept⁶, but the tools needed to put the concept into action have become available with technological innovations that have grown exponentially in recent years.

For the first time in modern history, we have all the building blocks needed to facilitate evolutionary robotics: rapid prototyping and physical reproduction using 3D printing, neural networks for learning and training, improved battery life, cheaper materials, and much more other.

NASA has already used artificial evolution to develop antennas for satellites⁷, for example. For their part, scientists from the University of Vermont and Tufts University in 2020 unveiled '*xenobots*', which are 'small biological machines first designed in computer simulations using evolutionary robotics techniques'⁸. These self-healing biological machines were built using frog stem cells and have shown the ability to move and push payloads; one purpose is that these *nanobots* could one day be used to deliver drugs after being injected into the bloodstream.

Indeed, evolutionary robotics is the only way to create robots capable of complex and autonomous interactions in the real world. The benefits of such robots are too long to list, but use cases can range from robotic firefighters and search and rescue robots to nuclear waste cleaning robots, home care robots and more (see *infra*).

We may also gain a better understanding of organic evolution. A more nuanced understanding of evolution could have such broad applications that it is difficult to understand. We could gain incredible insights into the best ways to cure disease and build immunity, improve our lifespan, reduce our impact on the ecological world, and otherwise gain a better understanding of our future on this planet.

Recognizing the growing need to effectively identify and manage artificial intelligence risks, COSO published '*Realize the Full Potential of Artificial Intelligence*'⁹: this new guide exploits the principles of Enterprise Risk Management(ERM) and serves as a guide to help organizations align risk management with the strategy and execution of their artificial intelligence (AI) initiatives and to realize the potential of humans who collaborate with AI.¹⁰

In 2019, a group of 23 researchers from MIT's Media Lab announced on their blog the urgent need for a new scientific discipline to study the behavior of

⁶ 'The first pioneering attempt to design adaptive robots were carried by cyberneticists in the 50s, before the digital computers era and before the development of the deliberative approach. The first systematic studies, instead, were carried in the 90s after the development of evolutionary, reinforcement learning, and regression learning algorithms' in S Nolfi, *Behavioral and Cognitive Robotics: An Adaptive Perspective*. (Institute of Cognitive Sciences and Technologies, National Research Council 2021, ISBN 9791220082372) in <https://bacrobotics.com/Behavioral%20and%20Cognitive%20Robotics%20An%20Adaptive%20Perspective%20-%20Stefano%20Nolfi.pdf>, 15.

⁷ See GS Hornby and Al Globus, 'Automated Antenna Design with Evolutionary Algorithms', American Institute of Aeronautics and Astronautics, in <https://ti.arc.nasa.gov/m/pub-archive/1244h/1244%20%28Hornby%29.pdf> accessed 4 February 2022.

⁸ See J Brown, 'Scientists Create the Next Generation of Living Robots', March 31, 2021, in <https://www.uvm.edu/news/story/scientists-create-next-generation-living-robots> accessed 4 February 2022.

⁹ Committee of Sponsoring Organizations of the Treadway Commission (COSO), 'Realize the Full Potential of Artificial Intelligence', 9/15/2021, in <https://www.coso.org/Documents/COSO-News-Release-Realize-the-Full-Potential-of-Artificial-Intelligence.pdf> accessed 4 February 2022.

¹⁰ As reported in the Press release, *ibid*.

machines. Iyad Rahwan, Director and Principal Investigator of the Media Lab's Scalable Cooperation Group, wrote: 'We are seeing the rise of *agency*¹¹ machines, machines that are actors who make decisions and take action on their own. This requires a new field of scientific studies that look at them not only as products of engineering and computer science, but also as a new class of actors with their own behavioral models and ecology'.¹²

The day after, the group published the seminal article 'Machine Behavior'¹³, which describes a broad scientific research agenda to study the behavior of machines in order to integrate computer science and the sciences that study the behavior of biological agents. The researchers point out that just as animal and human behavior cannot be understood without the context in which they occur, the behavior of machines also requires a coordinated study of algorithms and the social environments in which they frequently occur.

Moreover, the current prevalence of different algorithms in society is unprecedented (Fig. 1).

¹¹ 'In very general terms, an agent is a being with the capacity to act, and *agency* denotes the exercise or manifestation of this capacity. The philosophy of action provides us with a standard conception and a standard theory of action. The former construes action in terms of intentionality, the latter explains the intentionality of action in terms of causation by the agent's mental states and events. From this, we obtain a standard conception and a standard theory of agency. (.) Examples of human action include instances of habitual actions, such as actions taken while driving a car, and instances in which the agent is engaged in a reactive flow of interaction, such as in jazz improvisation or verbal exchanges. Examples from robotics include skills such as coordination of limb movements and the ability to navigate through new environments', in M Schlosser, 'Agency', *The Stanford Encyclopedia of Philosophy* (Winter 2019 Edition), <https://plato.stanford.edu/archives/win2019/entries/agency/> accessed 8 March 2022.

¹² See M Castelluccio, 'Understanding machine behavior', May 8, 2019, in <https://sfmagazine.com/technotes/may-2019-understanding-machine-behavior/> accessed 5 February 2022.

¹³ I Rahwan, M Cebrian, N Obradovich et al., 'Machine behavior' (2019) *Nature* 568, 477–486 in <https://www.nature.com/articles/s41586-019-1138-y.pdf>.

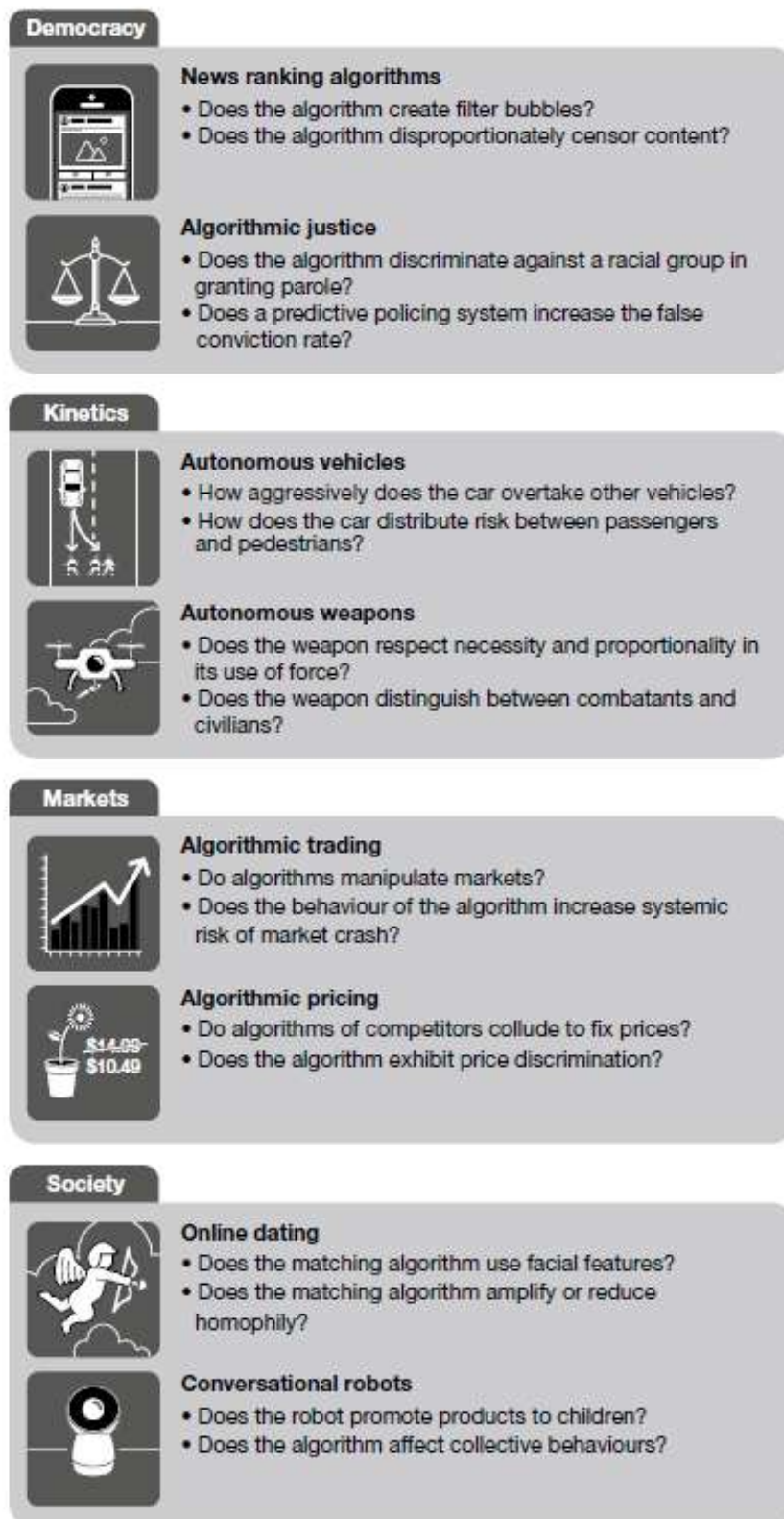


Figure 1 - Issues affecting the behavior of machines span a wide variety of scientific disciplines and topics. (Source: 'Machine Behavior', MIT Media Lab, cit.).

2. The behavior of the machines.

Understanding the behavior of AI agents is clearly one of the crucial challenges of the next decade of AI. *Interpretability* or *explainability* are some of the terms often used to describe methods that provide insights into the behavior of AI programs, although most have focused on exploring the internal structure of deep neural networks.

Recently, a group of artificial intelligence researchers from the Massachusetts Institute of Technology (MIT) are exploring a radical approach that attempts to explain the behavior of artificial intelligence by observing them in the same way we study human or animal behavior. They group ideas in this area under the captivating name of *machine behavior* which promises to be one of the most interesting fields of AI in the coming years.

The ideas behind the machine's behavior may be transformative, but its principles are relatively simple. The behavior of machines relies more on observations than engineering knowledge to understand the behavior of artificial intelligence agents. Think about how we observe and draw conclusions from the behavior of animals in a natural environment: most of the conclusions we get from observations are not related to our knowledge of biology, but rather to our understanding of social interactions. Understanding AI agents goes beyond the interpretation of a specific algorithm and requires analyzing the interactions between agents and with their surroundings. To achieve this, *behavioral analysis*¹⁴ using simple observations can be a powerful tool.

So *machine behavior* is a field that leverages behavioral sciences to understand the behavior of artificial intelligence agents: experimental methodology, population-based statistics and sampling paradigms, observational causal inference, neuroscience, collective behavior, or social theory.

From this point of view, the behavior of machines places itself at the intersection of computer science and engineering and behavioral sciences in order to obtain a *holistic* (see also *infra*) understanding¹⁵ of the behavior of artificial intelligence agents (fig. 2).

¹⁴ Behavioral analysis 'is a natural science that seeks to understand the behavior of individuals. That is, behavior analysts study how biological, pharmacological, and experiential factors influence the behavior of humans and nonhuman animals. Recognizing that behavior is something that individuals do, behavior analysts place special emphasis on studying factors that reliably influence the behavior of individuals, an emphasis that works well when the goal is to acquire adaptive behavior or ameliorate problem behavior', in The Association for Behavior Analysis International, 'What Is Behavior Analysis?' in <https://www.abainternational.org/about-us/behavior-analysis.aspx>, Copyright 2022 accessed 10 February 2022.

¹⁵ "In terms of psychology, the holistic view suggests that it is important to view the mind as a unit, rather than trying to break it down into its individual parts. Each individual part plays its own important role, but it also works within an integrated system. Essentially, holism suggests that people are more than simply the sum of their parts. In order to understand how people think, the holistic perspective stresses that you need to do more than simply focus on how each individual component functions in isolation. Instead, psychologists who take this approach believe that it is more important to look at how all the parts work together. (...) One key phrase that summarizes the key idea behind the holistic approach is that 'the whole is more than the sum of its parts.' The field of holistic medicine, for example, focuses on treating all aspects of a person's health including physical symptoms, psychological factors, and societal influences. One reason why it is so important to consider the entire being is that the whole may possess emergent properties. These are qualities or characteristics that are present in the whole but cannot be observed by looking at the individual pieces", as we read in K Cherry, A Morin, 'What Is Holism? How psychologists use holism to

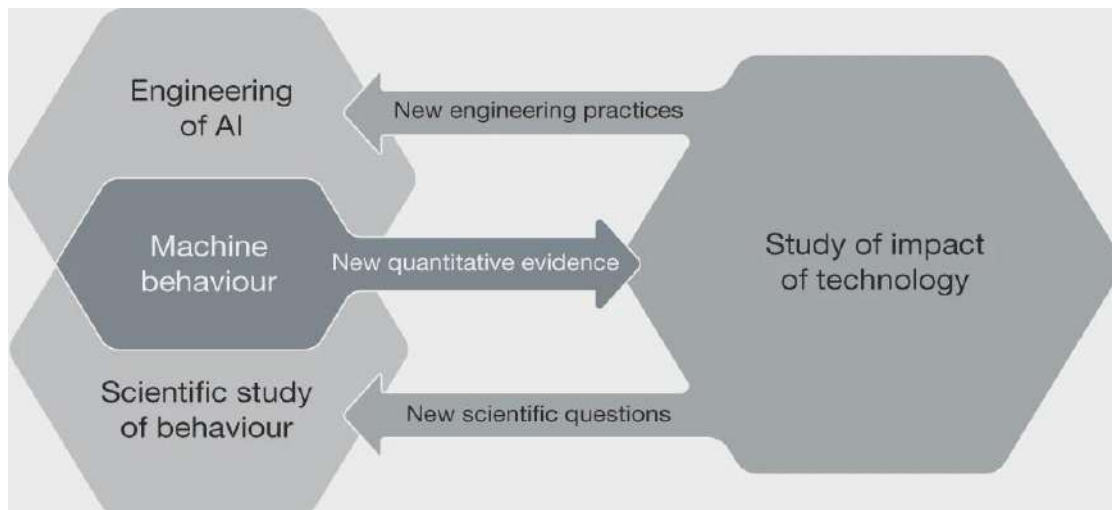


Figure 2 - The interdisciplinary nature of the machine behavior. The behavior of machines lies at the intersection between the fields that design and engineer artificial intelligence systems and the fields that traditionally use scientific methods to study the behavior of biological agents. Insights from machine behavior studies provide quantitative evidence that can help inform those fields studying the potential effects of technology on social and technological systems. In turn, these fields can provide useful engineering practices and scientific questions to fields examining the behaviors of machines. Finally, the scientific study of behavior helps AI scholars make more accurate claims about what AI systems can and cannot do. (Source: 'Machine Behavior', MIT Media Lab, cit.).

As AI agents become more sophisticated, analyzing their behavior will be a combination of understanding their internal architecture and their interaction with other agents and their environment. While the former will be a function of deep learning optimization techniques, the latter will rely in part on behavioral sciences.

Ethology is the field of biology that focuses on the study of animal behavior under natural conditions and as a result of evolutionary traits. One of the fathers of ethology was Nikolaas Tinbergen, who in 1973 won the Nobel Prize in Physiology or Medicine for his work identifying key dimensions of animal behavior. Tinbergen's thesis was that there were four complementary dimensions to understanding animal and human behavior: function, mechanism, development, and evolutionary history.

Despite the fundamental differences between artificial intelligence and animals, machine behavior borrows some of Tinbergen's ideas to delineate major behavior blocks in AI agents. Machines have mechanisms that produce behavior, undergo development that integrates environmental information into behavior, produce functional consequences that cause specific machines to become more or less common in specific environments, and embody evolutionary histories through which past environments and human decisions continue to influence the behavior of machines. An adaptation of the Tinbergen framework to the behavior of the machine can be seen in the following figure:

understand behavior', updated on April 19, 2020, in <https://www.verywellmind.com/what-is-holism-4685432> accessed 10 February 2022.

Scale of inquiry		
Hybrid		
Collective		
Individual		
Type of question	Object of study	
	Dynamic view Explanation of current form in terms of a historical sequence	Static view Explanation of the current behaviour of a machine
Proximate view How a particular type of machine functions	Development (ontogeny) Developmental explanations of how a type of machine acquires its behaviour, from deliberate engineering and supervised learning based on specific benchmarks, to online learning and reinforcement learning in a particular environment.	Mechanism (causation) Mechanistic explanations for what the behaviour is, and how it is constructed, including computational mechanisms or external stimuli that trigger it.
Ultimate (evolutionary) view Why a type of machine evolved the behaviours it has	Evolution (phylogeny) Incentives and market forces that describe why the behaviour evolved and spread, whether by programming or learning, subject to computational and institutional constraints.	Function (adaptive value) The consequences of the machine's behaviour in the current environment that cause it to persist, either by appeal for particular stakeholders (such as users or companies) or fit to some other aspect of the environment.

Figure 3 - The four categories proposed by Tinbergen for the study of animal behavior can be adapted to the study of the behavior of machines. Tinbergen's framework proposes two types of question, as well as two points of view of these questions. Each question can be examined on three scales of investigation: individual machines, collective machines and hybrid human-machine systems. (Source: 'Machine Behavior', MIT Media Lab, cit.).

In this framework, the study of the behavior of the machine focuses on four fundamental areas:

1. **Mechanism:** the mechanisms for generating the behavior of AI agents are based on its algorithms and on the characteristics of the execution environment. At its most basic level, machine behavior exploits interpretability techniques to understand the specific mechanisms underlying a given behavioral model.

2. **Development:** The behavior of AI agents is not something that happens in one fell swoop, but rather evolves over time. *Machine behavior* studies how machines acquire (develop) a specific individual or collective behavior. Behavioral development could be the result of engineering choices as well as the agent's experiences.

3. **Function:** An interesting aspect of behavioral analysis is understanding how a specific behavior affects the life function of an AI agent and how those functions can be copied or optimized on other AI agents.

4. **Evolution:** In addition to functions, AI agents are also vulnerable to evolutionary history and interactions with other agents. In the course of its evolution, aspects of the algorithms of artificial intelligence agents are reused in new contexts, both by constraining future behavior and by making further innovations possible. From this point of view, the behavior of the machine also studies the evolutionary aspects of artificial intelligence agents.

The four aspects provide a *holistic* model for understanding the behavior of AI agents.

However, these four elements do not apply equally when we are evaluating a single agent classification model versus a self-driving car environment with hundreds of vehicles. In this sense, the behavior of the machine applies the four previous aspects on three different scales (fig. 4):

- 1) **Individual Machine Behavior:** there are two general approaches to studying the behavior of individual machines. The first focuses on profiling the set of behaviors of any specific machine agent using an *in-machine* approach, comparing the behavior of a particular machine under different conditions. The second, an *inter-machine* approach, examines how a variety of individual machine agents behave in the same condition.
- 2) **Collective behavior of the machine:** unlike the individual dimension, this area seeks to understand the behavior of AI agents by studying the interactions in a group. The collective dimension attempts to identify behaviors that do not emerge at the individual level.
- 3) **Hybrid Human-Machine Behavior:** there are many scenarios where the behavioral patterns in AI agents are triggered by interacting with humans.

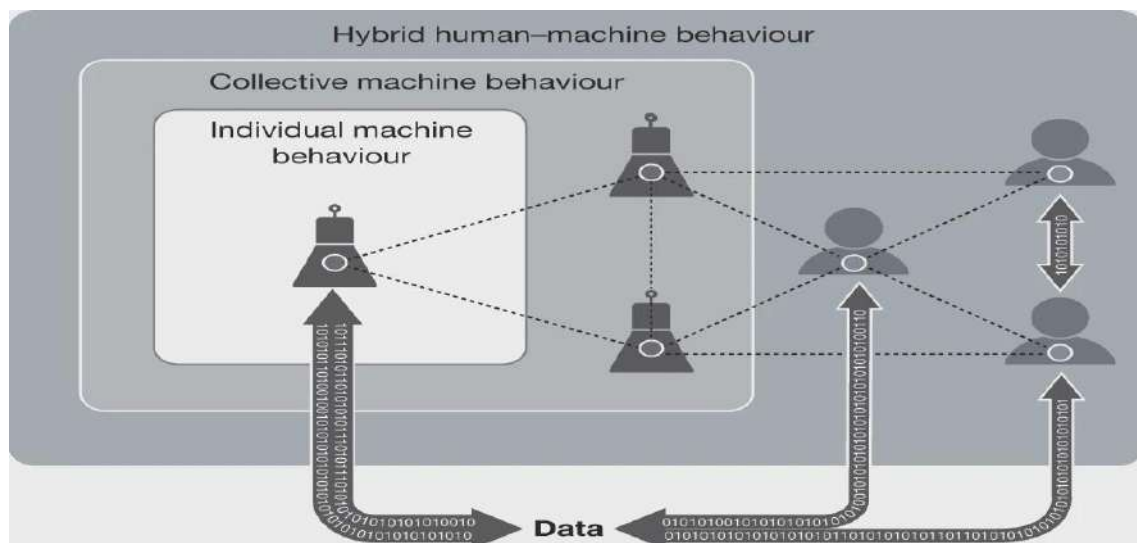


Figure 4 - Scale of investigation in the ecosystem of the machine behavior. Artificial intelligence systems represent the amalgamation of human beings, data and algorithms. Each of these domains influences the other in ways both well understood and unknown. The data, filtered through man-made algorithms, influence the individual and collective behavior of machines. AI systems are trained on data, which in turn affects how humans generate data. AI intelligence systems interact and influence each other. Human interactions can be altered by the introduction of these systems. (Source: 'Machine Behavior', MIT Media Lab, cit.).

Indeed, as interactions between humans and artificial intelligence become more sophisticated, the behavior of machines plays a critical role in enabling

the next level of ‘hybrid’ intelligence. This is why machine behavior is one of the most intriguing and nascent fields of behavioral sciences.

3. New evolutionary approaches.

Interpretability remains one of the greatest challenges of modern AI applications. Recent advances in computational models and deep learning research have enabled the creation of highly sophisticated models that can include thousands of hidden layers and tens of millions of neurons. While it is relatively simple to create incredibly advanced deep neural network models, understanding how such models create and use knowledge remains a challenge.

Recently, researchers from the Google Brain team published a paper proposing a new method called *Concept Activation Vectors* (CAVs)¹⁶ that opens a new perspective to the interpretability of AI models.¹⁷

In the current generation of technologies the friction between *interpretability* and *accuracy* is the friction between being able to perform complex knowledge tasks and understanding how those tasks were performed: in essence, knowledge vs. control, performance vs. responsibility, efficiency vs. simplicity, all these antinomies can be explained by balancing the trade-offs between accuracy and interpretability.

Are you interested in getting the best results or are you interested in understanding how those results were produced? This is a question data scientists must answer in any deep learning scenario. Many techniques are complex in nature and, although they are very accurate in many scenarios, they can become incredibly difficult to get interpreted (Fig. 5).

¹⁶ ‘The interpretation of deep learning models is a challenge due to their size, complexity, and often opaque internal state. In addition, many systems, such as image classifiers, operate on low-level features rather than high-level concepts. To address these challenges, we introduce Concept Activation Vectors (CAVs), which provide an interpretation of a neural net’s internal state in terms of human-friendly concepts. The key idea is to view the high-dimensional internal state of a neural net as an aid, not an obstacle. We show how to use CAVs as part of a technique, *Testing with CAVs* (TCAV), that uses directional derivatives to quantify the degree to which a user-defined concept is important to a classification result—for example, how sensitive a prediction of zebra is to the presence of stripes. Using the domain of image classification as a testing ground, we describe how CAVs may be used to explore hypotheses and generate insights for a standard image classification network as well as a medical application’ in B Kim, M Wattenberg, J Gilmer, C Cai, J Wexler, F Viegas, ‘Interpretability beyond feature attribution: Quantitative testing with concept activation vectors (tcav)’ in International conference on machine learning (2018) PMLR 2668-2677, in <https://arxiv.org/pdf/1711.11279.pdf>, 1.

¹⁷ See J Rodriguez, ‘This New Google Technique Help Us Understand How Neural Networks are Thinking’, 24 Jul 2019, in <https://www.kdnuggets.com/2019/07/google-technique-understand-neural-networks-thinking.html> accessed 15 February 2022.

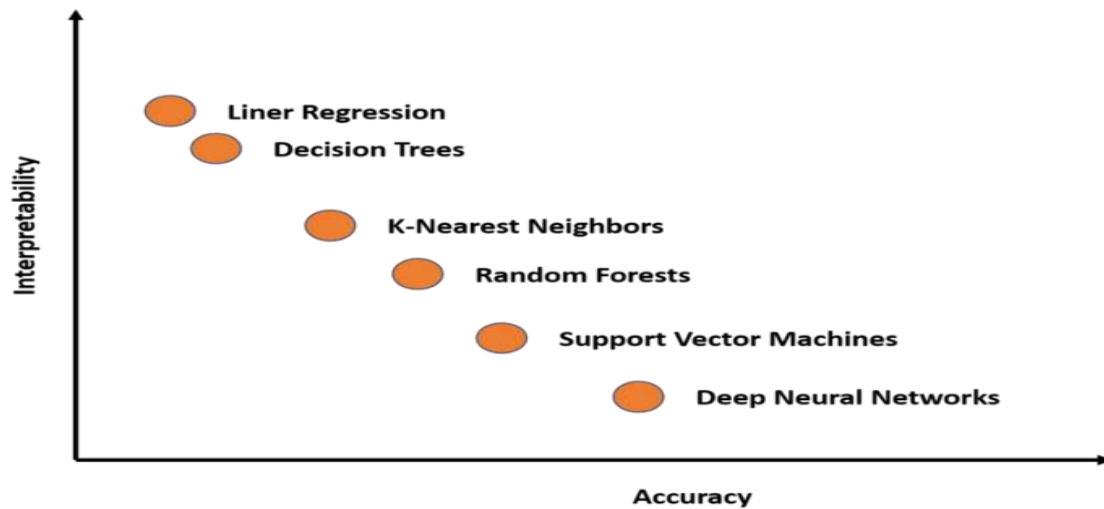


Figure 5 - The main deep learning models in a graph correlating accuracy and interpretability. (Source: 'This New Google Technique Help Us Understand How Neural Networks are Thinking Machine Behavior', cit.).

Furthermore, interpretability in such models is not a single concept and can be seen on multiple levels (fig. 6).

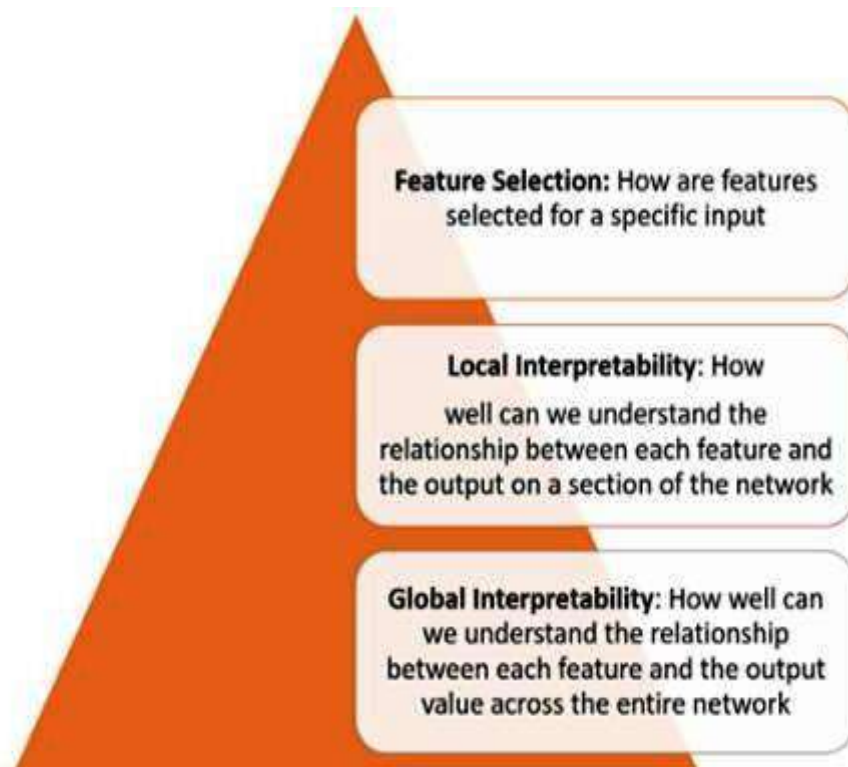


Figure 6 - The levels of interpretability in deep learning models. (Source: 'This New Google Technique Help Us Understand How Neural Networks are Thinking Machine Behavior', cit.).

Achieving interpretability through each of the levels defined in the previous figure requires several fundamental building blocks¹⁸:

✓ Understanding What Hidden Layers Do: most of the knowledge in a DL model is formed in the hidden layers, so understanding the functionality of the different hidden layers at the macro level is essential to be able to interpret the model.

✓ Understanding How Nodes Are Activated: the key to interpretability is not understanding the functionality of individual neurons in a network, but rather groups of interconnected neurons firing together in the same spatial location. Segmentation of a network by groups of interconnected neurons will provide a simpler level of abstraction to understand its functionality.

✓ Understanding How Concepts Are Formed: understanding how the deep neural network forms individual concepts that can then be assembled into the final output is another key element.

These principles are the theoretical foundation behind Google's new CAV technique, based on *saliency maps*¹⁹, to measure the relevance of a concept in the model's outputs (fig. 7).

¹⁸ Cf. C Olah, et al., 'The Building Blocks of Interpretability', Distill, 2018. Doi: 10.23915/distill.00010, in <https://distill.pub/2018/building-blocks/> accessed 15 February 2022.

¹⁹ Deep learning saliency maps were first seen in the article 'Deep Inside Convolutional Networks: Visualizing Image Classification Models and Saliency Maps' (<https://arxiv.org/pdf/1312.6034.pdf>). The paper presented by researchers from the *Visual Geometry Group* at the University of Oxford highlighted visualization techniques for calculating images, including saliency maps. (..) Saliency refers to unique characteristics (pixels, resolution, etc.) of the image in the context of visual processing. These unique features describe the visually alluring positions in an image. The saliency map is a topographical representation of this. These maps, first proposed by neuroscientists Itti and Koch in their study on image feature extraction ('*A saliency-based search mechanism for overt and covert shifts of visual attention*' (2000) *Vision Research* 40 1489-1506, in http://ilab.usc.edu/publications/doc/Itti_Koch00vr.pdf), give a detailed description: 'The purpose of the saliency map is to represent the conspicuity—or 'saliency'—at every location in the visual field by a scalar quantity and to guide the selection of attended locations, based on the spatial distribution of saliency. A combination of the feature maps provides bottom-up input to the saliency map, modelled as a dynamical neural network. Saliency maps process images to differentiate visual features in images. For example, coloured images are converted to black-and-white images in order to analyse the strongest colours present in them. Other instances would be using infrared to detect temperature (red colour is hot and blue is cold) and night vision to detect light sources (green is bright and black is dark). (..) The aggressive developments in saliency detection have almost achieved a human-like precision when it comes to recognising features. Be it with respect to datasets, learning models or with performance, saliency maps is the next big thing for computer vision and image processing projects.', as reported in A Sharma, 'What Are Saliency Maps In Deep Learning?', July 11, 2018, in <https://analyticsindiamag.com/what-are-saliency-maps-in-deep-learning/> accessed 16 February 2022.

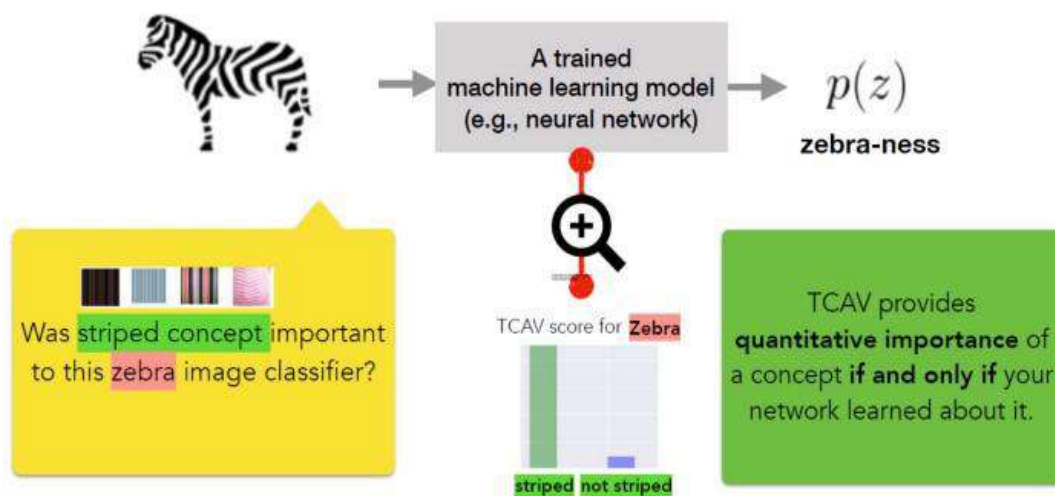


Figure 7 - TCAV measures the relevance of a concept in the model's outputs (Source: 'This New Google Technique Help Us Understand How Neural Networks are Thinking Machine Behavior', cit.).

A CAV for a concept is simply a vector in the direction of the values (e.g. activations) of the set of examples of that concept. In its article, Google's research team outlines a new linear interpretability method called '*Testing with CAV* (TCAV) that uses directional derivatives to quantify the sensitivity of the model's prediction to a learned, high-level underlying concept from a CAV.

The methodology is defined in three basic steps (fig. 8):

1) Define concepts relevant to a model.

TCAV achieves this by simply choosing a set of examples that represent this concept or find an independent dataset with the concept labeled. CAVs are learned by training a linear classifier to distinguish between the activations produced by examples of a concept and by examples at any level.

2) Understand the sensitivity of the forecast to those concepts.

The second step is to generate a TCAV score that quantifies the sensitivity of the predictions to a specific concept. TCAV achieves this by using directional derivatives that measure the sensitivity of ML predictions to changes in inputs towards the direction of a concept, at the level of neural activation.

3) Extract an overall quantitative explanation of the relative importance of each concept for each prediction class of the model.

The final step seeks to assess the overall relevance of learned CAVs to avoid relying on irrelevant CAVs. To address this challenge, TCAV introduces a statistical significance test that evaluates a CAV against a random number of training sessions (typically 500), because a meaningful concept should lead to TCAV scores that behave consistently throughout training sessions.

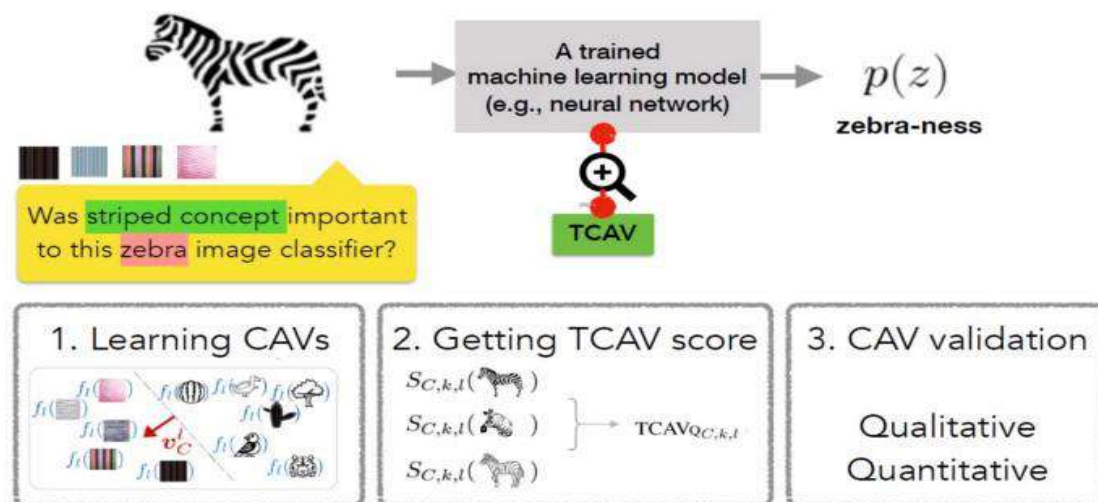


Figure 8 - The three fundamental steps of the TCAV methodology (Source: 'This New Google Technique Help Us Understand How Neural Networks are Thinking Machine Behavior', cit.).

The Google Brain team conducted several experiments to evaluate the efficiency of TCAV compared to other methods of interpretability. In one of the most extraordinary tests, the team used a salience map that attempts to predict the relevance of a caption or image to understand the concept of a taxi (fig.9).

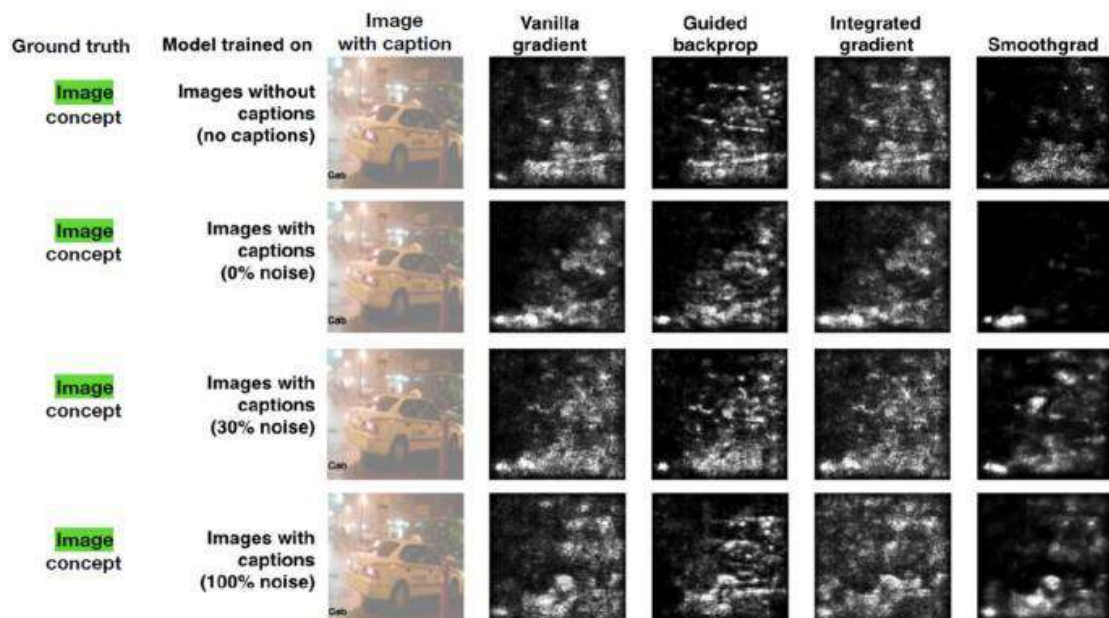


Figure 9 - Results of the salience map with approximated truth: models trained on datasets with different noise parameters p (rows) and different methods of salience map (columns) are presented. (Source: 'Interpretability Beyond Feature Attribution: Quantitative Testing with Concept Activation Vectors (TCAV)', cit.).

The fundamental truth of the experiment was that the concept of an image was more relevant than the concept of a caption. However, when examining salience maps, humans perceived the concept of caption as more important (model with 0% noise) or did not notice any differences (model with 100% noise). On the contrary, the TCAV results correctly show that the concept of image was more important.

TCAV is one of the most innovative evolutionary approaches of neural networks in recent years and open to interesting developments: it is a step towards the creation of a human-scale linear interpretation of the internal state of a deep learning model, in a way that model decision questions can be solved in terms of high-level natural concepts.²⁰

4. The most recent developments.

The discovery of expressive features constitutes a critical pre-requisite for the development of effective control policies. In the case of robots, *feature learning* can be especially challenging as it involves the generation of features describing the state of the agent and of the environment from raw and noisy sensor measurements that provide only part of the required information.²¹

Recent works in evolutionary (Salimans et al., 2017; Pagliuca et al., 2020) and reinforcement learning methods (Duan et al., 2016; Andrychowicz et al., 2019) demonstrated how *adaptive robots*²² can successfully learn effective policies directly from observation on the basis of reward signals that only rate the performance of the agent. In other words, these methods can discover the features required to realize effective control policies automatically without the need of additional dedicated mechanisms or processes. These approaches are usually referred to as *end-to-end learning*.²³

This is a type of deep learning process where all parameters are trained jointly, rather than step by step.²⁴ It is particularly prevalent in the self-driving car industry, as the benefits of this process fit neatly into the car's *convolutional neural networks* (CNNs).²⁵

²⁰ See Kim, Wattenberg et al., 'Interpretability beyond feature attribution: Quantitative testing with concept activation vectors (tcav)' (n 16) 8.

²¹ Cf. N Milano, S Nolfi, 'Autonomous Learning of Features for Control: Experiments with Embodied and Situated Agents' (2020) arXiv 2009.07132, in <https://arxiv.org/ftp/arxiv/papers/2009/2009.07132.pdf>, 1.

²² Cf. "the adaptive robot Rizon is the first applied product of the 3rd generation robotic technology. It combines high-performance force control, computer vision and advanced AI technologies, which enables the robot to adapt to the complicated environments and accomplish better 'hand-eye' coordination like human does. There are three key features which differentiate adaptive robots from others: high tolerance of position variance, great disturbance rejection and transferrable intelligence", as we read in 'Adaptive Robots', Contributed by Flexiv, 10/22/19, Robotics Tomorrow - Online Robotics Trade Magazine Industrial Automation, in <https://www.roboticstomorrow.com/article/2019/10/adaptive-robots/14305> accessed 18 February 2022.

²³ Cf. N Milano, S Nolfi, 'Autonomous Learning of Features for Control: Experiments with Embodied and Situated Agents' (n 21) 1.

²⁴ Cf. Computer Science Wiki contributors, 'End-to-end learning', Computer Science Wiki, , 6 April 2018, https://computersciencewiki.org/index.php?title=End-to-end_learning&oldid=8019 accessed 18 February 2022.

²⁵ "CNNs are a collection of neurons that are organized in interconnected layers, with convolutional, pooling, and fully connected layers. As a mathematical construct that processes data of multiple dimensions, CNNs are designed to adaptively learn simpler patterns at lower depths while transitioning to more complicated

Since the autonomous self jointly receives multiple parameters through CNNs, it is useful to use an end-to-end learning process that can train or infer the parameters. An example could be: 'the autonomous car has to turn right towards the civil area from a highway', as there is a certain speed limit the car has to adjust its speed accordingly, while at the same time the car must also turn to the right. In this situation, end-to-end learning allows the car to perform the correct inference based on multiple reception parameters (fig. 10).

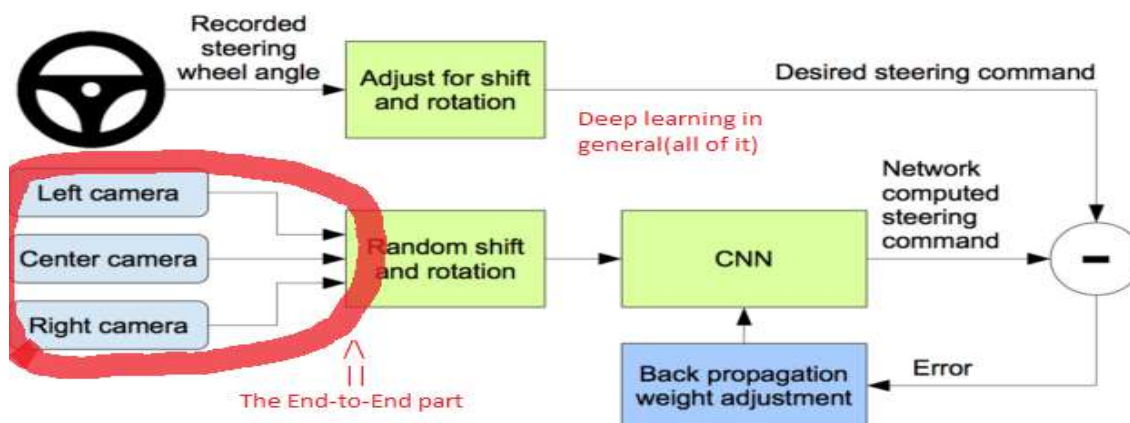


Figure 10 - The circled parameters are evaluated jointly (at the same time) within this Deep learning process, so that it too can be classified as an *end-to-end learning process* (source https://computersciencewiki.org/index.php/End-to-end_learning, cit.).

On the other hand, extensive methods that incorporate mechanisms or processes dedicated to extracting useful features can potentially accelerate learning and better adapt to complex problems. *Feature learning* is a general domain that aims to extract features that can be used to characterize data.

Recently, this area has achieved remarkable results in the context of learning neural networks for classification and regression problems. For example, feature learning with deep convolutional neural networks is an excellent solution to image classification problems. Self-learning feature learning for control is a special area of feature learning where input vectors (observations) are influenced by output vectors (actions) and where observations and actions vary throughout the process learning (Bohmer et al., 2015; Lesort et al., 2018). The term *autonomous* refers to the fact that characteristics are extracted through a self-supervised learning process, i.e. a learning process in which supervision is provided directly by the data available as input.

A first goal of feature learning is to generate a *compact* representation of high-dimensional sensory data which, in the case of robotic problems, could include 50 or more joint angles and velocities, hundreds of sensors encoding tactile information, and thousands or millions of pixels that form camera images.

patterns as we dive deeper. Deep neural networks overcome the use of exponentially large parameters by the addition of multiple hidden layers", as reported in JM Vaz, S Balaji, 'Convolutional neural networks (CNNs): concepts and applications in pharmacogenomics' (2021) Molecular diversity, 25(3), 1569–1584, in https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8342355/pdf/11030_2021_Article_10225.pdf, 1570.

A second goal is to generate *useful* features, that is, more informative characteristics of the observation states from which they can be extracted.

Therefore Milano & Nolfi (2020) analyze whether features extracted through self-supervised learning methods facilitate the development of effective solutions in 'embedded and situated' robots trained through an evolutionary algorithm. They consider experimental scenarios in which robots have access to egocentric perceptual information²⁶: the results demonstrate how the use of features extracted through *sequence-to-sequence learning model*²⁷(Srivastava et al. 2015, Sutskever et al. 2014, Cho et al. 2014) allows to obtain better solutions with respect to the *end-to-end control* condition, provided that the self-supervised learning process (which determines the extracted features) continues throughout the evolutionary process.

In summary, 'the effectiveness of adaptive methods can be enhanced by combining a control network, trained with an evolutionary or reinforcement learning algorithm, with one or more feature extraction networks trained through self-supervised learning (Lange, Riedmiller & VoigtHinder, 2012; Mattner, Lange & Riedmiller, 2012; Ha & Schmidhuber, 2018; Milano & Nolfi, 2020). While the feature extraction networks are used to extract useful features from the observations, the control network is used to map the features extracted from the previous network(s) into appropriate actions'.²⁸

For its part, '*neuroevolution*' (Lehman and Miikkulaian, 2013) is a widely used method to evolve embodied and situated agents.²⁹ Clearly, the conditions

²⁶ Cf. "The very notion of a position in space requires a reference frame, and one of the primary distinctions made among possible reference frames has been between egocentric and allocentric (a.k.a. geocentric, exocentric, environment-centered) reference frames (e.g., Burgess, 2006; Feigenbaum & Rolls, 1991; Howard, 1991; McNamara, Rump, & Werner, 2003; Nardini, Burgess, Breckenridge, & Atkinson, 2006; Neggers, Van der Lubbe, Ramsey, & Postma, 2006; Wang & Spelke, 2000). As the terms suggest, egocentric reference frames code location with respect to the observer, whereas allocentric reference frames code location with respect to something external to the observer (room axes, distal cues, cardinal directions, etc.). There is substantial evidence for both egocentric and allocentric information coded in the brain from neurophysiology and neuropsychology. In different subregions of the parietal cortex, neurons respond to the stimuli in retina-centered, head-centered, and even hand-centered coordinate systems (e.g., Colby & Goldberg, 1999), supporting a system for representing space egocentrically. However, place cells in the medial temporal lobes have been shown to code location with respect to the environmental reference frame (e.g., Burgess, Jeffery, & O'Keefe, 1999)", in N Burgess, 'Egocentric and allocentric information in spatial memory', in https://ebruary.net/155480/psychology/egocentric_allocentric_spatial_memory accessed 18 February 2022.

²⁷ Cf. "Sequence to Sequence (often abbreviated to seq2seq) models is a special class of Recurrent Neural Network architectures that we typically use (but not restricted) to solve complex Language problems like Machine Translation, Question Answering, creating Chatbots, Text Summarization, etc.(..) This model can be used as a solution to any sequence-based problem, especially those where inputs and outputs have different dimensions and categories. (..) The most common architecture used to create Seq2Seq models is the *Encoder-Decoder architecture*. Both the *encoder* and the *decoder* are LSTM models", in P Singh, 'A Simple Introduction to Sequence to Sequence Models', August 31, 2020, in <https://www.analyticsvidhya.com/blog/2020/08/a-simple-introduction-to-sequence-to-sequence-models> accessed 19 February 2022.

²⁸ Cf. S Nolfi, 'Behavioral and Cognitive Robotics: An Adaptive Perspective' (n 6) 159-160.

²⁹ Cf. "Much of recent machine learning has focused on deep learning, in which neural network weights are trained through variants of stochastic gradient descent. An alternative approach comes from the field of neuroevolution, which harnesses evolutionary algorithms to optimize neural networks, inspired by the fact that natural brains themselves are the products of an evolutionary process. Neuroevolution enables important capabilities that are typically unavailable to gradient-based approaches, including learning neural network building blocks (for example activation functions), hyperparameters, architectures and even the algorithms for learning themselves. Neuroevolution also differs from deep learning (and deep reinforcement learning) by maintaining a population of solutions during search, enabling extreme exploration and massive parallelization" in K Stanley, J Clune, J Lehman, R Miikkulainen, 'Designing neural

under which agents are evaluated influence the course of the evolutionary process.³⁰ Ideally, the environmental conditions should match the skill level of the evolving agents, that is, they should be difficult enough to elicit adequate selective pressure and simple enough to ensure that random variations can occasionally produce progress. This can be achieved by varying the evaluation conditions during the evolutionary process, i.e. by increasing the complexity of environmental conditions across generations and by selecting conditions that are challenging for current evolving agents.

There are three possible methods:

1) incremental evolution: the use of an evolutionary process divided into successive phases of increasing complexity. For example, the evolution of the ability to visually track target objects can be accomplished by exposing evolving agents first to large immobile targets, then to small immobile targets, and finally to small moving targets (Harvey, Husband & Cliff, 1994). Similarly, the evolution of agents evolved for the ability to capture fleeing prey can be organized in a series of successive phases in which the speed of the prey and the delay in pursuit are progressively increased (Gomez & Miikkulainen, 1997). However, these approaches assume that the tasks can be sorted by difficulty, when in fact they might vary along multiple difficulty axes. In general, incremental approaches can be effective but introduce hyperparameters that are difficult to tune and require the use of domain-dependent knowledge.³¹

2) Competitive co - evolution: the evolution of agents that compete with other evolving agents. For example, the co-evolution of two populations of predators and robot prey selected respectively for their ability to capture prey and escape predators (Rosin & Belew, 1997; Nolfi & Floreano, 1998; De Jong, 2005; Chong, Tiño & Yao, 2009; Miconi, 2009; Samothrakis et. al., 2013). However, if on the one hand the exploitation of their weaknesses has an adaptive value for the opposing population, on the other it does not necessarily lead to a progressive complexification of the adaptive problem. Furthermore, it can only be applied to problems that can be formulated competitively.³²

3) A third possible method, (Milano & Nolfi, 2021) consists in enhancing the evolutionary algorithm with a process capable of selecting the environmental conditions that have the right level of difficulty for the current evolving agents and that challenge the weaknesses of the agents in current evolution. This class of methods is referred to as *curriculum learning*.³³ Its usefulness for supervised

networks through neuroevolution' (2019) Nature Machine Intelligence. 1. 10.1038 in https://www.researchgate.net/publication/330203191_Designing_neural_networks_through_neuroevolution, 1.

³⁰ See N Milano, S Nolfi, 'Automated curriculum learning for embodied agents a neuroevolutionary approach' (2021) Sci Rep 11, 8985, in <https://www.nature.com/articles/s41598-021-88464-5.pdf>, 1.

³¹ *Ibid.*

³² *Ibid.*, 2.

³³ Cf. "Humans need about two decades to be trained as fully functional adults of our society. That training is highly organized, based on an education system and a curriculum which introduces different concepts at different times, exploiting previously learned concepts to ease the learning of new abstractions. By choosing which examples to present and in which order to present them to the learning system, one can guide training and remarkably increase the speed at which learning can occur. This idea is routinely exploited

learning has been widely demonstrated and constitutes an active research field (Bengio et al., Cit; Sutskever & Zaremba, 2014; Graves et al., 2016 and 2017; Held et al., 2017). Wang et al. (2019) proposed an algorithm that evolves a population of increasingly complex agent-environment pairs. Progressive complexity is achieved by:

- (i) optimizing agents in their associated environments,
- (ii) generating new environments by creating varying copies of existing environments, and
- (iii) attempting to transfer copies of current agents to another pair of environmental agents.

As demonstrated by the authors, this method allows to produce agents capable of operating effectively in remarkably complex conditions and to generate solutions for environmental conditions that are too difficult for a conventional evolutionary method. Conversely, however, this method produces tailor-made solutions for specific environmental conditions that do not necessarily generalize to other conditions.

Milano and Nolfi then propose a curricular learning method that automatically selects the environmental conditions in which the evolving agents are evaluated.³⁴ More specifically, it allows evolutionary algorithms to select the environmental conditions that facilitate the evolution of effective solutions. This is accomplished by adding a curricular learning component that estimates the level of difficulty of environmental conditions from the point of view of evolving agents and selects conditions with different levels of difficulty in which the frequency of difficult cases is greater than the frequency of easier cases.

The estimation of the level of difficulty of the environmental conditions is carried out on the basis of the suitability obtained in those conditions (*fitness*) by recently evaluated agents. The selection of suitable environmental conditions is achieved by selecting h environmental conditions from h corresponding subsets characterized by different levels of difficulty, where h is the number of evaluation episodes.

Finally, the preferential selection of difficult conditions is achieved by increasing the probability of selecting difficult environmental conditions, that is, by determining the intervals of the subsets with a power function. Using this method also reduces the stochasticity of the *fitness measure* as it ensures that agents are exposed to environmental conditions that have similar levels of difficulty.³⁵

in animal training where it is called shaping (Skinner, 1958; Peterson, 2004; Krueger & Dayan, 2009). (..) The basic idea is to start small, learn easier aspects of the task or easier subtasks, and then gradually increase the difficulty level" in Y Bengio, J Louradour, R Collobert, J Weston, 'Curriculum Learning', in Proceedings of the 26th International Conference on Machine Learning, Montreal, Canada, 2009, in <http://machinelearning.org/archive/icml2009/papers/119.pdf>, 2-3 accessed 20 February 2022.

³⁴ See N Milano, S Nolfi, 'Automated curriculum learning for embodied agents a neuroevolutionary approach' (n 30) 2.

³⁵ *Ibid*, 12.

The curricular learning component proposed is general and can be combined with any evolutionary algorithm. Its effectiveness has been verified in combination with the 'Open-AI neurodevelopmental strategy'³⁶, one of the best state-of-the-art algorithms available.

5. Conclusions.

AI is described by the 'Regulation on a European approach to artificial intelligence' Commission's draft as 'a rapidly evolving family of technologies that can contribute to a wide range of economic and social benefits'.³⁷

The use of AI makes it possible to infer complex and non-linear relationships from the data that the software analyzes, to achieve a specific objective by identifying and, if necessary, automatically perfecting the operations of a system.

However, if ethical challenges are not addressed sufficiently, a lack of public trust can hinder the adoption of such systems which, in turn, would lead to significant social opportunity costs through the under-use of available and well-designed technologies: the ethical challenges posed is therefore becoming a prerequisite for good governance in hi-tech societies.³⁸

From an ethical perspective, this shifts the focus of ethical deliberation from specific decision-making situations to the ways in which algorithms are designed and implemented.³⁹

Since the use of artificial intelligence systems proliferates, being able to explain how a certain model or system works is essential, especially for those used by governments or public sector agencies, to avoid talking about *AI black boxes*.⁴⁰

³⁶ "The OpenAI-ES method proposed by Salimans et al. (2017) is a form of natural evolutionary strategy that estimates the gradient of the expected fitness. (..) It is a variation of the batch normalization method commonly used in supervised learning adapted to problems in which the stimuli experienced by the network are not fixed (see also Salimans et al., 2016). This is the case of embodied agents in which the stimuli that are experienced depend on the actions executed by the agents previously. The problem is solved by calculating the average and the variance of the activation of the sensors incrementally on the basis of the distribution of the activation of the sensors of agents of successive generations. This technique is particularly useful in problems in which the range of activation of the sensors vary widely during the course of the evolutionary process", as specified in P Pagliuca, N Milano, S Nolfi, 'Efficacy of Modern Neuro-Evolutionary Strategies for Continuous Control Optimization' (2020) Front. Robot. AI 7:98. doi: 10.3389/frobt.2020.00098, in <https://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC7805676&blobtype=pdf>, 2-3.

³⁷ Cf. Proposal for a Regulation of the European Parliament and of the Council establishing harmonized rules on Artificial Intelligence (Law on Artificial Intelligence) and amending some legislative acts of the Union-COM / 2021/206 final, Brussels, [2021] in <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206>, 2.

³⁸ Cf. J Mökander, J Morley, M Taddeo, L Floridi, 'Ethics - Based Auditing of Automated Decision - Making Systems: Nature, Scope, and Limitations'(2021) Science and Engineering Ethics, in <https://link.springer.com/content/pdf/10.1007/s11948-021-00319-4.pdf>, 43.

³⁹ *Ibid*, 44.

⁴⁰ "At its core, black boxes are algorithms that humans cannot survey, that is, they are epistemically opaque systems that no human or group of humans can closely examine in order to determine its inner states. Typically, black box algorithms do not follow well understood rules (as, for instance, a Boolean Decision Rules algorithm does), but can be 'trained' with labelled data to recognise patterns or correlations in data, and as such can classify new data. In medicine, such self-learning algorithms can fulfil several roles and purposes: they are used to detect illnesses in image materials such as X-rays, they can prioritise information or patient files and can provide recommendations for medical decision-making. (..) The reflection on the

So 'there are challenges of blending AI with behavioral science for behavior change, such as:

- Building trust with end users to gather sufficient user data.
- Designing scalable personalized and engaging interactions to retain users.

To build trust with end users, the business use case must be a win-win instead of only benefiting the company. Besides, the underlying technology must be reliable, trustworthy and ensure privacy. The emerging field of ethical AI explicitly takes into account fairness, explainability and robustness during algorithm design'.⁴¹

In this regard, it is worth citing here an example of artificial cognitive architecture for trust, ToM (Theory of Mind)⁴², and episodic memory in an HRI (human-robot interactions) scenario that can improve the performance of artificial agents in contexts of shared objectives.

To conclude *à la* Munro⁴³, 'human beings have always been part of Machine Intelligence systems: they create unstructured data, load them into systems, develop statistical models, interpret the results. Adaptive learning optimizes people's time and effort by making machines smarter to make people smarter. In reality, it is a question of making the most of human intelligence'.

limitations of algorithms offers, indeed, insight into ways to improve their use. To our mind, being aware of the epistemic limitations of medical AI is a condition for entrenching responsible use and interaction with such systems. For these reasons, we believe that the debate needs to be widened by not solely focusing on the technological aspect of medical AI, but also on the interaction of humans with such technological systems" in JM Durán, KR Jongsma, 'Who is afraid of black box algorithms? On the epistemological and ethical basis of trust in medical AI', Journal of Medical Ethics, 18 March 2021 in <http://dx.doi.org/10.1136/medethics-2020-106820>, 329, 334.

⁴¹ Cf. B Fontaine, 'The Advent Of Trustworthy Behavioral AI', Forbes Technology Council, Jun 4, 2021 in <https://www.forbes.com/sites/forbestechcouncil/2021/06/04/the-advent-of-trustworthy-behavioral-ai/> accessed 22 February 2022.

⁴² See "A complementary approach to simulated social interaction is cognitive simulation, which seeks to develop artificial representations of neurocognitive mechanisms such as imitation and perception of self, simulate them in artificial agents such as humanlike robots, and assess their functioning in enabling ToM inferences in human-agent interactions (Breazeal and Scassellati, 2002; Scassellati, 2002; Michel et al., 2004). Building on simulation theory (Gallese and Goldman, 1998), cognitive simulation involves the robot establishing and maintaining representations of the mental states of its human counterparts by tracking and matching their states with resonant states of its own. These representations enable the robot to take the perspective of its human counterparts, make inferences about the human's goals, and learn from their actions", in LJ Byom, B Mutlu, 'Theory of mind: mechanisms, methods, and new directions' (2013) Frontiers in human neuroscience, 7, 413, in <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3737477/pdf/fnhum-07-00413.pdf>, 6.

⁴³ Cf. R Munro, 'The fourth generation of machine learning: Adaptive learning', September, 2015, in <http://www.junglightspeed.com/the-fourth-generation-of-machine-learning-adaptive-learning/> accessed 22 February 2022.



Digital surveillance technologies. Ethical, anthropological and political issues.

MARIA GIORGIA CARACENI

Research Fellow of Fondazione Magna Carta of Rome
Doctor in Philosophy of Law

Abstract

The article aims to show how, over the decades, the noble ideals underlying the technological revolution began in the last century have been betrayed. The peculiar characteristics of that system defined as 'surveillance capitalism' by Shoshana Zuboff are first described, and then the historical and cultural framework allowing it to establish itself is reconstructed. Next, the consequences on human beings, such as the lack of privacy and the restriction of fundamental rights and liberties, are analyzed and discussed. Finally, the phenomenon of mass surveillance conducted through digital tools is addressed from a political and juridical point of view. In this regard, the risks that this represents for democratic political systems and the consequent legislative response that the European Union is trying to give are debated. Finally, conclusions are drawn.



Keywords: Capitalism; Surveillance; Privacy; Democracy.

Summary: [Introduction](#) – [1. The Surveillance Capitalism.](#) – [2. The historical context.](#) – [3. New frontiers of surveillance.](#) – [4. The expropriation of the self.](#) – [5. Can we talk about digital totalitarianism?](#) – [6. The risks for democracy.](#) – [6.1 The case of social credit.](#) – [7. The European legislative response.](#) – [Conclusions.](#)

Introduction.

Having to describe the so-called *technological revolution* that began in the last century, we might say that technological instruments appeared at their dawn as formidable tools that seemed to allow the human being to test a degree of freedom never experienced before: e. g., through the Web and storage devices, he has got ‘the privilege of forgetting the various things he does not need to have immediately at hand, with some assurance that he can find them again if they prove important’.¹ In a more and more complex and wealthy of information society, man inevitably struggles, because his memory is transient, so according to the theoretical conceptions, ideals, and motives underlying this evolution, technology would have made his life easier. Furthermore, it would have let him be able to weave personal relationships with extreme ease as well;² and finally, thanks to the total and indiscriminate availability of information and the negligence of costs,³ it would have pushed in the direction of an increasingly radical democratization of society.⁴

1. The Surveillance Capitalism.

In someone’s opinion, the dream of a fairer and more democratic digital future was shattered when the capitalist economic system realized the possibility that digital offered it. According to one of the most authoritative scholars of the subject, Shoshana Zuboff, to have discovered, put into practice, and spread that new form of capitalism that is defined as *surveillance*, was *Google*, a company founded in 1988 by Larry Page and Sergey Brin: users, guided by the ideal of information capitalism as a liberating and democratic force, immediately started using the search engine. These activities thus initiated to produce *new behavioral data*, which were initially randomly archived. Google engineers soon began to understand that this incessant flow

1 V Bush, ‘As We May Think’, *Atlantic* (Jul. 1954), 15, <<https://mondodomani.org/eticaeinformatica/media/filelist/etistoinfa/1-%20Vannevar%20Bush%2C%20As%20We%20May%20Think%20%28completo%29.pdf>> accessed 01 February 2022.

2 A similar idea is, e.g., expressed in the text of the presentation of *Community Memory*, the first kind of bulletin board considered the ancestor of modern forums, created in 1972 at the University of Barkley. See *Community Memory Message Base*, 1972, <<https://web.archive.org/web/20130307110833/http://www.well.com/~szpak/cm/cmflyer.html>> accessed 01 February 2022.

3 See V Bush, ‘As We May Think’, 8.

4 See G Salmeri, ‘Il senso politico dell’informatica. Due esempi dalle sue origini’, in A.T. Calogero Caltagirone (edited by), *Tecnologie della comunicazione e forme della politica*, Morcelliana, Brescia 2020, 237-40.

of collateral behaviors – or *behavioral surplus* –⁵ was able to improve search engine performance; nonetheless, it is essential to emphasize that initially ‘behavioral data were used for the benefit of the user, they offered value at no cost, and that value was reinvested in the user experience by improving services’;⁶ therefore, the raw material provided in data by users was collected and used to improve the speed and accuracy of searches and/or to contribute to the creation of secondary products such as the translator.⁷

Things have started to change as the new millennium dawned when extraordinary events occurred, modifying the nature of digital forever. First of all, the crisis that Google experienced in 2000 should be pointed out, when the company began to come under pressure from investors who were not satisfied enough with the revenues obtained through their financing. As in politics, the declaration of a state of emergency allows the implementation of exceptional measures that otherwise would not be justifiable, so, at the end of 2000, the state of emergency became a mantra for Google. It was the pretext for its founders to abandon any hostility towards *advertising* and cancel any spirit of reciprocity regarding the relationship with users. Brin e Page then hired the AdWords team to look for new ways to ‘make money’.⁸ From that moment on, Google began to work differently on and with the data collected in its immense archive, which from a technical point of view means that the *ads* would no longer be linked only to the *query* but *targeted* for the single individual. Google, therefore, opened its doors to advertising, but just to that *relevant* to users. However, this new rhetoric omitted a decisive aspect: Google would have entered a territory hitherto unexplored, exploiting the sensitive data revealed by its users. That raw material previously used to exclusively improve the quality of user navigation was therefore put at the service of targeted advertising. Thus, if Google had considered people as a goal in the first phase of its existence, now it was starting to consider them as a *means* to achieve a different purpose.

Hence, the *state of emergency* is the background on which the so-called *surveillance capitalism* took its roots. Google registered several patents in those years; particularly relevant is, for this discussion, the one recorded in 2003 and published two years later, called *Generating User Information for Use in Target Advertising*. The authors of the patent explicitly stated that their work was animated by a *profit-oriented logic*.⁹ Here is Zuboff’s comment about it:

The techniques described in the patent imply that for each search conducted through the Google search engine, the system simultaneously presents a specific configuration of a particular ad and all of this in the fraction of time it takes to type the query. The data used to implement this instant translation of the query into the ad, a predictive analysis called

5 See S Zuboff, *Il capitalismo della sorveglianza. Il futuro dell’umanità nell’era dei nuovi poteri*, Luiss University Press, Rome 2019, 73-108.

6 Ibid 79 (translation mine).

7 See *ibid*.

8 K Swisher, ‘Dot-Com Bubble Has Burst; Will Things Worsen in 2001?’, *The Wall Street Journal* (Dec. 18th, 2000), <<https://www.wsj.com/articles/SB97709118336535099>> accessed 01 February 2022.

9 See K Barath, S Lawrence, M Sahami, *Generating User Information for Use in Target Advertising* (Jun. 16th, 2005), 1-2, pdf available at <<https://patentimages.storage.googleapis.com/7c/39/51/a52b212d281f11/US20050131762A1.pdf>> accessed 01 February 2022.

matching, went far beyond simply denoting search terms. New data sets, called user profile information or UPI, capable of drastically increasing the accuracy of these predictions, were compiled. They would no longer have to guess, and there would be no more waste in the advertising budget. Mathematical certainty would take care of it.¹⁰

The system was gradually perfected thanks to the development of a series of mechanisms ranging from cookies to analysis methods up to predictive algorithms, according to a logic of expropriation of behavioral data as the basis of a new form of market that soon became dominant. Social networks – first of all, Facebook – certainly played a decisive role in this process, too, as they could rely on data voluntarily posted by users. ‘We have better data than anyone else. We know the gender, age, location, and these are all actual data, not just inferred’,¹¹ said Sheryl Sandberg – one of the top managers of Facebook and former creator of AdWords. Another fundamental invention in this sense is, for obvious reasons, represented by the *like* button.

While it is true that an economic system always produces specific social relationships,¹² *surveillance capitalism* embodies the asymmetry between knowledge and power that exists between a close circle of data experts operating in the dark, ‘of which Google is the *Übermensch*’,¹³ and the rest of the individuals. If classical capitalism was born first from the expropriation of the land and then of the means of production,¹⁴ that of surveillance was generated by an act of *digital expropriation*¹⁵ in which *behavior* has become a *commodity*; however, users are unaware of the mechanisms of operation of this market because their consciousness is not just not necessary, but above all, it is not desirable. Surveillance capitalists, therefore, work to ensure that the protection of online privacy is cancelled and that any attempt at law that favors it is blocked, as it would pose a threat to their very existence.¹⁶

2. The historical context.

A question that seems legitimate to ask is: how did all this happen? At the beginning of the previous paragraph, mention was made of the circumstances that made it possible to implement and improve the system. However, the crisis that Google went through at the beginning of the new millennium cannot be sufficient to answer the question just posed. This business need was undoubtedly the trigger for an epochal change, but this could also happen thanks to particular cultural and historical conditions. First of all, the role that *neoliberal ideology* has historically played in the United States cannot be ignored: a study carried out by Jodi Short, law expert and academic at the University of California, aims to demonstrate how in the victorious defense –

10 S Zuboff, *Il capitalismo della sorveglianza*, 88-9 (translation mine).

11 See ibid 103 (translation mine).

12 See K Marx, *Il Capitale. Critica dell'economia politica*, Newton Compton, Rome 2015, 85-90.

13 S Zuboff, *Il capitalismo della sorveglianza*, 92 (translation mine, german original).

14 See K Marx, *Il Capitale*, 85-90.

15 See S Zuboff, *Il capitalismo della sorveglianza*, 110.

16 See J Brodtkin, ‘Google and Facebook lobbyists try to stop new online privacy protections’, *Ars technica* (May 24th, 2017), <<https://arstechnica.com/tech-policy/2017/05/google-and-facebook-lobbyists-try-to-stop-new-online-privacy-protections/>> accessed 01 February 2022.

by Google and the other digital giants – of a territory within which being able to act outside the law, a liberal matrix can be identified; a particular convergence is then traced to the concept of *self-regulation*, according to which a company can independently decide its standards, check that they are respected and even issue a judgment on its conduct by applying ‘the law to themselves, determine whether it has been violated, and voluntarily report and remediate legal violations’:¹⁷ it is in this context that the surveillance capitalists have developed a strong ‘cyberlibertarian’¹⁸ ideology.

The other historical condition that allowed surveillance capitalism to assert itself can be identified in the sudden reorientation of government security policies that occurred in America as a consequence of the 9/11 attacks.¹⁹ After the 9/11 attacks, the political agenda changed abruptly, and the priority became security over privacy. Both the European Parliament and the US Congress presented bills expanding surveillance activities. ‘The United States Congress passed the Patriot Act, devised the Terroristic Screening Program, and instituted a series of additional measures that vastly expanded the collection of personal information’.²⁰ There were then the institutions themselves that broke down every wall because they needed to draw on the information collected by the various digital agencies making user profiling activities.²¹

3. New frontiers of surveillance.

It is not just through online activities that users can be profiled. Intelligent appliances, now present in several homes, are, for surveillance capitalists, a precious means of collecting data (in many cases, users are forced to share data and grant permissions without which functionality is limited).²² Digital assistants such as Cortana or Alexa can acquire complete data on people's lifestyle habits, being *conversation* the medium of interaction between the user and the device.²³ They are even able to modulate their responses by basing them on the inflection of the interlocutor's voice, interpreting the more or less acute tone as a manifestation of a specific emotional state. However, smartphones provide the best data: most smartphone apps require user positioning even if it is not necessary for its operation, just as it is often necessary to grant access to the archive of files, photos, and videos. In particular, the apps that can extract the most sensitive data are those for health and fitness: they can monitor biometric data – such as heart rate, body temperature, sweating, blood pressure, calorie consumption – and require the

17 JL Short, ‘The Paranoid Style in Regulatory Reform’, *Hastings Law Journal* 63 (Jan. 12th, 2011), 667, pdf available at

<https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1242&context=hastings_law_journal> accessed 01 February 2022.

18 S Zuboff, *Il capitalismo della sorveglianza*, 118 (translation mine).

19 See D Lyon, *Surveillance After September 11. Themes for the 21st century*, Polity, 2003, 7.

20 S Zuboff, *Il capitalismo della sorveglianza*, 124 (translation mine).

21 See § 6.

22 See S Zuboff, *Il capitalismo della sorveglianza*, 249-50.

23 See *ibid* 274.

user to reveal precise information in order to effectively develop customized plans that he can follow – for example, a diet.²⁴

In 2016, more than ‘100,000 apps dedicated to mobile health for Android and iOS (iPhone) operating systems [were available], which doubled over the last two years’.²⁵ Furthermore, ‘In the United States, most health and fitness apps were not subject to health privacy laws’.²⁶ In response to this, also in 2016, the Federal Trade Commission (FTC) issued guidelines that mobile app developers should follow in order to increase transparency, privacy, and security;²⁷ however, they can be easily circumvented, possessing only a *vis directiva* and not a *vis coactiva*. Many studies are revealing how health-related mobile apps sell users’ data to advertising companies without their permission;²⁸ in particular, a survey on Android apps for diabetes appeared in the *Journal of American Medicine* in 2016 demonstrated that, ‘Permissions, which users must accept to download an app, [automatically] authorized collection and modification of sensitive information’,²⁹ even those not voluntarily released by users: the apps, in fact, also accessed information regarding identity, call log, archive, contacts, wi-fi connections.³⁰

Besides the various wearable devices and apps dedicated to health, social networks are also a mine to extract biometric data. For example, in 2017, Facebook declared that it had about two billion profiles – now five – through which 350 million photos were uploaded per day, and in 2018 it announced that it had achieved a face recognition capacity that reached a level of 97.35 percent accuracy,³¹ identifying facial recognition as a further possibility to improve ad targeting.

In 2015, the National Telecommunications and Information Administration (NTIA), under the patronage of the United States Department of Commerce, attempted to establish general guidelines for the creation and use of biometric information. After weeks of negotiations, NTIA had to ascertain; the impossibility of reaching an agreement due to the hard-line held by the technology companies – especially regarding the consent. So, in 2016 it had to

24 Biometric data can even be interpreted by digital technologies as a manifestation of a particular mood, such as detecting an increase in a heartbeat when a subject is exposed to viewing specific contents. See *ibid* 260-1.

25 G Addonizio, ‘The privacy Risks Surrounding Consumer Health and Fitness Apps with HIPAA’s Limitations and the FTC’s Guidance’, *Health Law Outlook* 9 (n 1, 2016), <<https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1015&context=health-law-outlook>> accessed 01 February 2022.

26 S Zuboff, *Il capitalismo della sorveglianza*, 263 (translation mine).

27 See Federal Trade Commission, *Mobile Health App Developers: FTC Best Practices* (Apr. 2016), <<https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices>> accessed 01 February 2022.

28 A long series of studies proves this. See e.g.: Privacy Rights Clearinghouse, *Mobile Health and Fitness Apps: What are the Privacy risks?* (Jul. 1st, 2013); pdf available at <<https://privacyrights.org/consumer-guides/mobile-health-and-fitness-apps-what-are-privacy-risks>> accessed 01 February 2022. For further bibliographical information see: S. Zuboff, *Il capitalismo della sorveglianza*, 586 (nt. 50).

29 SR Blenner and others, ‘Privacy Policy of Android Diabets App and Sharing of Health Information’, *JAMA* 315 (n 10 2016), 1051; pdf available at <[file:///C:/Users/User/Downloads/Jld150059%20\(1\).pdf](file:///C:/Users/User/Downloads/Jld150059%20(1).pdf)> accessed 01 February 2022.

30 See *ibid*.

31 See Y Taigman and others, ‘DeepFace: Closing the Gap to Human-Level Performance in Face Verification’, *Facebook Research* (Apr. 14th, 2018) 7; pdf available at <https://www.cs.toronto.edu/~ranzato/publications/taigman_cvpr14.pdf> accessed 01 February 2022.

limit itself to presenting *recommendations*.³² However, the problem with this kind of document is that lacking regulatory value; they are not binding and can be ignored.

4. The expropriation of the self.

Digital surveillance is often justified by those who practice it with the rhetoric of *inevitability*: it is necessary to be constantly monitored as this increases social security. After all, those who have nothing to hide have nothing to fear: it was Google CEO Eric Schmidt who was the first to become the spokesperson for this concept.³³ Faced with the incessant repetition, many people have come to accept it. In *Nothing to Hide. The False Tradeoff between Privacy and Security*, Daniel Solove reports some of the most common arguments given by people who were asked if they cared about their privacy and worried about the increasing use of digital devices for mass surveillance. Among the most common responses are:

I don't have anything to hide from the government. I don't think I had much hidden from the government in the first place. I don't think they care if I talk about my ornery neighbor.

Do I care if the FBI monitors my phone calls? I have nothing to hide. Neither does 99.99 percent of the population. If the wiretapping stops one of these Sep. 11 incidents, thousands of lives are saved.

Like I said, I have nothing to hide. The majority of American people have nothing to hide. And those that have something to hide should be found out, and get what they have coming to them.³⁴

Actually, the *nothing to hide argument* not only proves to be logically inconsistent as 'arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying that you don't care about free speech because you have nothing to say',³⁵ not only it does infringe a "right"³⁶. It hides a contradiction since those who invoke it are ready to make an exception for themselves since surveillance practices are almost unknown

³² See S Zuboff, *Il capitalismo della sorveglianza*, 267-8.

³³ 'If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place': these are the words pronounced by Schmidt in an interview with Class CNBC on December 9th, 2009. The partial video of the interview is available on YouTube at the address <<https://www.youtube.com/watch?v=A6e7wFDHzew>> accessed 01 February 2022, while some of Schmidt's statements have been reported by the most important newspapers in the country; please refer, e.g., to the article published the next day by the *Huffington Post*, 'Google CEO On Privacy: "If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It"' (Dec. 10th, 2009), <https://www.huffpost.com/entry/google-ceo-on-privacy-if_n_383105> accessed 01 February 2022.

³⁴ DJ Solove, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, London 2011, 22.

³⁵ This is the famous counter-argument formulated by Edward Snowden in response to that of "Nothing to hide". Part of the video of the first interview in which Snowden expressed his argument was published by A Rusdrigger, J Gibson, E MacAskill, 'Edward Snowden: NSA reform in the US is only the beginning', *The Guardian* (May 22nd, 2015), <<https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video>> accessed 01 February 2022. We will return to Snowden in § 6.

³⁶ The term "right" has been placed in quotation marks because it must be specified that there is no natural right to privacy in the American Constitution; however, jurists include it in the IV amendment. The same applies to articles 13, 14, and 15 of the Italian Constitution. The GDPR of the European Union talks about the right to the protection of personal data. For further information regarding the GDPR, see § 7.

to the most, but it is also patently *false*. In reality, privacy is a desire common to all as it is essential – and not an accessory – for the human being. The private sphere is where everyone feels free to act, think, speak as they prefer since they are away from the judgmental gaze of others. ‘Privacy is a fundamental condition of being a free person’.³⁷ The restriction of privacy limits the freedom of choice because when people know they are being watched, they change their behavior and try to do what others expect from them to avoid shame and condemnation. All oppressive political and religious authorities rely on the idea that the awareness of being observed induces a subject to comply with what is required: the re-educational method formulated by Jeremy Bentham in the *Panopticon* is its emblem. The occupants of the Panopticon were not necessarily under constant surveillance, but not being able to know for sure was enough.³⁸ The same principle underlies the surveillance system described by George Orwell in *1984*.³⁹ Michel Foucault in *Discipline and Punish*, commenting on the panoptic method, came to argue that omnipresent surveillance even pushes individuals to internalize their supervisors and therefore to do what is expected of them without realizing or not being controlled.⁴⁰ Several studies show how awareness of being observed alters behaviors.⁴¹

Privacy is relational; it depends on whom you are dealing with: for example, having a job but looking for a better one is certainly not illegal or condemnable. However, it is understandable to have the desire that your employer does not come to know it. It could be said – provocatively – that *everyone has something to hide*.⁴² When an economic system such as the one described up to now is affirmed, which is based on the expropriation of sensitive data in order to profile each user and predict their behavior by showing them content that they will *indeed* consider relevant, it follows that the personal boundaries that protect the inner life are considered an obstacle to business. It is then the self itself, the interior space of lived experience within which each individual creates meaning and which is the foundation of freedom, to be exposed to the risk of disintegration because the human being cannot live without giving up meaning to his experience and cannot conceive himself as the result of predictions based on the analysis of accumulated data by monitoring his online activity, collecting his biometric data, listening to his conversations. Indeed, it is reasonable to predict that if someone ever had the chance to meet his “digital

37 G Greenwald, *No Place to Hide. Sotto controllo: Edward Snowden e la sorveglianza di massa*, Rizzoli, Milan 2014, 262 (translation mine).

38 See J Bentham, *Panopticon. Ovvero la casa d’ispezione*, Marsilio Editors, Venice 2009, see in particular 46-51.

39 See G Orwell, *1984*, Newton Compton, Rome 2021.

40 See M Foucault, *Sorvegliare e punire. Nascita della prigione*, Einaudi, Turin 2014, 194.

41 For example, an experiment conducted in 1975 by the psychologists of Stanford University entitled *The Chilling Effects of Surveillance: Deindividuation and Reactance*, goes in this direction. In this case, the participants were subjected to different levels of surveillance and were asked to express an opinion on controversial political issues. For example, regarding the legalization of marijuana, some were told that their answers would have been shared with the police: only 44 percent said they were in favor. However, the percentage of those in favor reached 77 percent among the individuals told otherwise. This experiment is mentioned in G Greenwald, *No Place to Hide*, 270-2. Moreover, the pdf of the entire study is available online at <<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1002.4273&rep=rep1&type=pdf>> accessed 01 February 2022.

42 See G Greenwald, *No Place to Hide*, 275.

avatar”, he would not recognize himself because each individual attributes enormously excedent meanings to his singular story. Therefore, the freedom to create meaning cannot and must not be subtracted.

No matter how much it is taken from me, this inherent freedom to create meaning remains my last sanctuary. Jean-Paul Sartre writes that ‘freedom is nothing other than the existence of our will’, and explains: ‘It is not enough to want, it is necessary, to want to want’. The birth of the will to will is the inner act that assures us of our nature as autonomous beings who project their choices into the world and exercise the self-determination and moral judgment necessary for civilization, of which they are the last bastion. (...) The deeper the prediction imperative is pushed into the self, the more the value of the surplus becomes irresistible, and the operations to capture it increase. What happens to the right to speak in the first person and as oneself when the frenzy to institutionalize activated by the imperative of foresight is trained to capture my sighs, blinks, pronunciation to reach my thoughts, and how to someone else's ends? It is no longer the surveillance capital that grabs the surplus of my searches, purchases, and Internet browsing. The surveillance capital wants something more than my space-time coordinates; it is violating the inner sanctum, with machines and algorithms that decide the meaning of my breath and my gaze, of the muscles of my jaw, of my voice that becomes higher, of all the exclamation marks I had typed with hope and innocence.⁴³

5. Can we talk about digital totalitarianism?

Surveillance capitalism, this new type of trade, can be defined as ‘instrumentalizing power (...) [which] has the task of *structuring and exploiting behavior in order to modify, predict, monetize and control it*’.⁴⁴ Those who take sides against this new type of power – scholars, journalists, activists – often do so by recalling the Orwellian Big Brother and even more the specter of totalitarianism, to the point that the threat embodied by subjects such as Google, Facebook, and the entire commercial surveillance is often referred to as ‘digital totalitarianism’.⁴⁵ However, comparing a new phenomenon to another one already known can be risky. Intellectuals had to elaborate new conceptual categories in order to frame and describe the unprecedented effects due to the totalitarian governments of the last century;⁴⁶ the same

43 S Zuboff, *Il capitalismo della sorveglianza*, 306 (translation mine). The quotation in quotation marks is taken from JP Sartre, *Being and Nothingness*, Washington Square, New York 1993, 573.

44 Ibid 370 (translation mine).

45 See in this regard ‘Move Over Big Brother’, *The Economist* (Dec. 4th, 2004), <<https://www.economist.com/technology-quarterly/2004/12/04/move-over-big-brother>> accessed 01 February 2022; R Blakely, ‘We Thought Google Was the Future but It’s Becoming Big Brother’, *Times* (Sep. 19th, 2014), <<https://www.thetimes.co.uk/article/we-thought-google-was-the-future-but-its-becoming-big-brother-h3psqft8mpt>> accessed 01 February 2022; C Doctorov, ‘Unchecked Surveillance Technology Is Leading Us Towards Totalitarianism’, *International Business Times* (May 5th, 2017), <<https://www.ibtimes.com/unchecked-surveillance-technology-leading-us-towards-totalitarianism-opinion-2535230>> accessed 01 February 2022. For further bibliographical information, please refer to S Zuboff, *Il capitalismo della sorveglianza*, 600 (nt. 1).

46 Several scholars have indicated the will to dominate the human soul among the peculiar characteristics of totalitarian regimes. See, e.g., CJ Friederich, Z Brzezinsky, *Totalitarian Dictatorship and Autocracy*, Harvard University Press, MA 1956; TW Adorno, *Education after Auschwitz*, in *Critical Models: Interventions and*

effort is needed in this historical moment: Shoshana Zuboff, as mentioned above, among others, essayed this undertaking.⁴⁷ It, therefore, becomes a priority to get aware of the fact that the horizon in which what has been defined digital totalitarianism moves is utterly different from that within which twentieth-century totalitarianism took shape.

The instrumentalizing power moves in a different way and towards an opposite horizon. Totalitarianism used violence, while instrumentalizing power uses the means of behavior modification: this is where we need to change focus. The instrumentalizing power is not interested in our souls or in imposing principles. There is no training or transformation for spiritual salvation, no ideology to conform to our actions. The instrumentalizing power is neither interested in possessing the totality of a person nor in exterminating or torturing our bodies in the name of pure devotion. It appreciates [our] data [but] (...) does not aim for pain, bereavement, terror; however much it undoubtedly appreciates the behavioral surplus coming from affliction. It is profoundly and infinitely indifferent to what motivates us and what we consider significant. (...) Even if it does not kill, it is frightening, incomprehensible, and unprecedented, just as totalitarianism was for victims and witnesses. Our encounter with an unprecedented power helps us explain why it has been challenging to baptize and learn about this new kind of coercion. (...) Totalitarianism was a political project allied with economic power to subjugate society. Instrumentalizing power is a market power that converges with digital for a unique type of social domination.⁴⁸

6. The risks for democracy.

The ambitious reform of everyday life outlined up to now has been carried out by private capital; this would not have been possible, however, if there had not been supported from public institutions: the *war on terrorism* 'legitimized the use of certainty produced by machines as a solution to social uncertainty. (...) In the sixteen years of the Bush and Obama administration, the "advancement of information technology" was considered "the most effective" response to the threat of terrorism'.⁴⁹ Americans were allowed to learn what happened regularly in 2013, after Edward Snowden, a young computer scientist who had worked for the CIA and the NSA, made available to some *Guardian* reporters a series of documents revealing the architecture of the most significant security program mass surveillance ever conceived and

Catchwords, Columbia University Press, New York 1996; H Arendt, *Le origini del totalitarismo*, Comunità Edizioni, Milan 1996.

47 Among the most significant categories elaborated by Zuboff we point out the aforementioned *behavioural surplus* (see *Supra* § 1) and that of *rendering* conceived as the set of operations that intervene on the gap between experience and data to ensure that the first one is transformed in the second ones (see S Zuboff, *Il capitalismo della sorveglianza*, 247-9).

48 Ibid 377-8 (translation mine).

49 Ibid 401-2 (translation mine). Internal citations are reported by Zuboff and are taken from P Swire, 'Privacy and Information Sharing in the War of Terrorism', *Villanova Review* 51, n. 4 (2006), 951, pdf available at <<https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1195&context=vlr>> accessed 01 February 2022.

implemented.⁵⁰ It was discovered that the National Security Agency (NSA) had forced every telephone company to provide printouts of all communications between American citizens and foreign countries, regularly acquired data from the giants of information technology and the Internet, spied on political leaders and competitors of American companies, accessed email texts, entered cell phones and computers around the world. Faced with the enormous scandal, American institutions tried to justify themselves by appealing to the rhetoric of “nothing to hide”, concealing behind the increased security needs due to the threat of terrorism and stressing that ‘many of the surveillance procedures described in the Snowden archive referred to the mere acquisition of metadata,⁵¹ not contents’,⁵² as if these practices were less intrusive. Actually, if a government always knows who the recipients of a confident citizen's calls are, knows the times and duration, knows where they are made from and so on, it can collect much more information than it could by intercepting a single conversation. There are several experts who support this.⁵³

6.1. The case of *social credit*.

Where can this trend lead? One possible answer is offered by *social credit*, a system developed – starting from 2015 – by the Chinese government for the purpose to leverage ‘the explosion in personal data generated through smartphones, apps, and online transactions in order to improve citizens’ behavior (...) [The system requires] Individuals and businesses [to be] (...) scored on various aspects of their conduct – (...) [such as frequented places, purchases, acquaintances] – and [then] these scores (...) [are] integrated within a comprehensive database that not only links into government information but also to data collected by private businesses’.⁵⁴ Based on social and financial activities and biometric tracking – starting from fingerprints – subjects inevitably leave signs of their behavior, which are traced by a system that judges them as *good* or *bad* and consequently assigns them rewards and punishments. The purpose of the system is to induce them to adopt *only good* behaviors because, otherwise, the extent of the punishments will be so heavy

⁵⁰ The story is detailed in the book above published by G Greenwald – one of the journalists contacted by Snowden – in which it is also possible to consult some extracts of the documents he had come into possession of thanks to the young computer scientist. See G Greenwald, *No Place to Hide*.

⁵¹ Google and other surveillance capitalists have often resorted to this same argument.

⁵² G Greenwald, *No Place to Hide*, 202 (translation mine).

⁵³ For instance, Edward Felten, a professor of computer science at Princeton, in a sworn deposition in which the American Civil Liberties Union (ACLU) challenged the legality of the metadata collection program practiced by the NSA, brought various examples to support this thesis. In general, he believes that wiretapping is far more cumbersome acquiring metadata due to language barriers such as the use of jargon or coded signals that could – intentionally or unintentionally – obscure the meaning of the message. The transcript of his statements is available online: see The United States Senate, *Written Testimony of Edward W. Felten* (Oct. 2nd, 2013), <<https://www.cs.princeton.edu/~felten/testimony-2013-10-02.pdf>> accessed 01 February 2022.

⁵⁴ R Creemers, ‘China’s chilling plan to use social credit ratings to keep score on its citizens’, *CNN.com*, (Oct. 28th, 2015) <<https://edition.cnn.com/2015/10/27/opinions/china-social-credit-score-creemers/index.html>> accessed 01 February 2022. To consult the text of the law concerning the establishment of the social credit system, please refer to *State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System* (2014-2020), GF n 21 (2014), <<https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>> accessed 01 February 2022.

that it will condemn them to social exclusion. Possible rewards include favorable conditions on loans and rentals, car rental without a down payment, greater visibility on dating websites. According to a *China Daily* article, blocked citizens as debtors or in default of a court order was prevented – for example – from taking the plane and the high-speed train and/or hiring – in the workplace – managerial roles. 55

Could this be an example of *digital totalitarianism*? Can a comparison be made with the world of 1984? Answering these questions is not easy, but what we want to underline in the context of this discussion is the perceptible difference between Western surveillance capitalism and Chinese state surveillance. Although the means used to produce behavioral modification are the same at the basis of capitalism surveillance, the purpose of Chinese politics is quite different, it aims to achieve guaranteed results at a *social level* and not at a *market level*. However, on closer inspection, the logic behind this system is the same underlying websites such as eBay, Uber, and TripAdvisor, on which users are evaluated and thus acquire or lose value and credibility in the eyes of other users.

However, China is not a democracy; therefore, in our context, there is no reason to place too much emphasis on the social credit system. There is also another significant distinction between the West and the Chinese world: surveillance capitalism in the West is mature and offers its tools to the State, which necessarily needs to collaborate if it wants to access a specific type of power. On the other hand, in the Chinese context, the State has assumed a prominent role in transforming social assets because it is the owner of a political project – we repeat, not of a market one – which can only be achieved through an automated solution.

Europe is certainly not China, but it is necessary to be aware that there are phenomena worth dwelling on even in this part of the world. For example, in 2014, Italy established the Public System of Digital Identity, a Single National Number necessary for citizens to access the online services of the public administration. In addition, the electronic identity card contains a high-tech microprocessor in which essential biometric data such as the scanning of the fingerprints of the indexes and the facial pattern are stored. In France, since 2016, the Titres électronique sécurisé (TES) has been established, i.e., a system for centralizing the biometric data of the population – also, in this case, facial pattern and fingerprints – collected thanks to passports and identification cards in the perspective of integrating it with the missing ones. Finally, we want to refer to an experiment conducted in Sweden in 2018 by the Ministry of the Future on three thousand volunteers, consisting in the installation of a subcutaneous microchip between the thumb and forefinger of one of the hands, and it allows carrying out numerous operations such as payment by credit card, online purchases, booking air and rail tickets, managing house or car keys. 56

55 S Xiaofeng, C Yin, 'Court Blacklist Prevents Millions from Flying, Taking High-Speed Trains', *China Daily* (Feb 14th, 2017), <https://www.chinadaily.com.cn/china/2017-02/14/content_28195359.htm> accessed 01 February 2022.

56 These data are taken from R Curcio, *L'algoritmo sovrano. Metamorfosi identitarie e rischi totalitari nella società artificiale*, Sensibili alle foglie, Rome 2018, 103-6.

We conclude this paragraph with the following reflection: the Coronavirus pandemic – offering the formidable reason for containing infections – has justified the implementation of tracking and data collection systems (including biometric ones) and probably has acted in this sense an accelerator of a process which was already underway.

7. The European legislative response.

Starting from 25 May 2018, the European Union has taken a big step forward in the field of data protection with the adoption of a new General Regulation (GDPR, *General Data Protection Regulation*).⁵⁷ Unlike directives, which must be transposed – through the adoption of national measures – by individual States and which are binding only on the objectives to be achieved – therefore not being mandatory in all their elements –, *regulations* are general. They aim to bring the legal institutions on specific subjects of the Member States as close as possible. Therefore, the Regulation mentioned above aims to respond to the modern need for sustainable development of technological dynamics and aims, through uniformity and simplification, to create a single data protection authority for all EU countries. The main goal of the GDPR is to establish the methods of processing and protecting the data of natural people and to protect their fundamental rights and liberties by establishing that all entities that collect data belonging to people residing in the EU comply with the established rules. The GDPR also introduces new rights for the owner – such as the right to delete data –,⁵⁸ new obligations for companies that process data – such as the imposition of consent which must be granular, unambiguous, and expressed –,⁵⁹ and penalties that may arrive up to twenty million or 4% of the company's annual turnover – if higher – in case of violation of specific articles.⁶⁰ A further tool is also introduced to protect the data owner, namely the *complaint*, which allows you to contact the Privacy Guarantor directly and request verification by the Authority.⁶¹ So, concerning the West, it is possible to immediately notice the difference in approach between Europe and the United States.

Conclusions.

We have tried to describe the phenomenon of digital surveillance by

⁵⁷ Garante per la Protezione dei Dati Personali, *Regolamento Generale sulla Protezione dei dati* (*General Data Protection Regulation*) – GDPR (May 23rd, 2013). The pdf of the italian version of the Regulation is available at

<<https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018.pdf/1bd9bde0-d074-4ca8-b37d-82a3478fd5d3?version=1.9>> accessed 01 February 2022.

⁵⁸ See *ibid* art. 17.

⁵⁹ See *ibid* art. 7.

⁶⁰ See *ibid* art. 83.

⁶¹ See *ibid* art. 77.

analyzing its ethical perspectives and anthropological and political repercussions. First, it must be clear that surveillance capitalism was intentionally conceived in a specific historical period, ‘invented by a particular group of people, in a specific place and time. It has been neither a consequence made inevitable by the development of digital technology nor the only possible expression of information capitalism’;⁶² as we have seen in the introductory part of this study, the ideal assumptions underlying the digital revolution were quite different. The biggest mistake that the inhabitants of the digital world can make is to give up because of inurement, by believing in the rhetoric of inevitability and by declaring themselves willing to assign rights: a fair and sustainable digital future can and must be demanded.

However, theorizing an act of rebellion understood as *resistance from below* appears unreasonable because it would concretely result in the indiscriminate rejection of digital tools. This path does not seem feasible (also in light of the ongoing digitalization of public administration). Furthermore, it would also not be fair for people to be forced to renounce the advantages offered by technology, which are objectively evident. So, a first precaution that users could and should adopt to protect themselves is the use of data encryption systems. Nevertheless, the decisive answer to the data protection problem should first and foremost come *from the top*. In the previous paragraph, we have seen how decisive a constant response from the Legislator is, who, due to the extreme rapidity of technological evolution, must – or should – always be ready to reformulate the rules issued by taking into consideration the possible emergence of new rights to be protected. Many place their hopes in the GDPR of the European Union, which, with the procedural changes introduced and the sanctions envisaged, represents a significant achievement. Only over time will it be possible to pass judgment on its effectiveness and say whether it will be able to restore a division of knowledge in line with the values of a democratic society.

62 See S Zuboff, *Il capitalismo della sorveglianza*, 96 (translation mine).



Potere di controllo datoriale: nuove tecnologie e tutela dei lavoratori nella società digitale

Supervisory power of the employer: new technologies and worker protection in the digital society

CHIARA VITAGLIANO

Ph.D. (c) Università degli Studi di Napoli l'Orientale

Abstract

Nell'attuale società della digitalizzazione il mondo del lavoro ha subito radicali cambiamenti, per effetto dell'introduzione di strumenti tecnologici ed informatici a supporto dell'attività lavorativa.

L'avvento delle moderne tecnologie nelle realtà aziendali ha ampliato il potere di controllo del datore di lavoro dei propri dipendenti, ponendo nuove questioni in tema di tutela della libertà e della riservatezza dei lavoratori.

Il presente lavoro ha l'obiettivo di analizzare le ripercussioni del progresso tecnologico sui rapporti sussistenti tra datore di lavoro e dipendenti, e di verificare se l'attuale normativa garantisca un'effettiva tutela dei diritti fondamentali del lavoratore.

In the current digitalization society, the world of work has undergone radical changes, due to the introduction of technological and IT tools to support work.

The advent of modern technologies in corporate realities has expanded the employer's control power of its employees, posing new issues in terms of protecting the freedom and privacy of workers.

This work aims to analyze the repercussions of technological progress on existing relationships between employer and employees, and to verify whether the current legislation guarantees effective protection of the worker's fundamental rights.



Keywords: Rapporto di lavoro subordinato; controlli a distanza; nuove tecnologie; privacy

Summary: [Introduzione.](#) – [1. La disciplina dei controlli a distanza.](#) – [2. La categoria degli strumenti di lavoro.](#) – [3. L'impatto dell'Industria 4.0 sulla disciplina statutaria.](#) – [4. L'utilizzabilità delle informazioni raccolte.](#) – [Conclusioni.](#)

Introduzione.

La configurazione tradizionale del rapporto di lavoro subordinato attribuisce al datore di lavoro una posizione di preminenza rispetto al lavoratore, esplicitamente riconosciuta nell'art. 2086 del codice civile secondo cui l'imprenditore/datore di lavoro è il capo dell'impresa da cui dipendono gerarchicamente i lavoratori collaboratori.

Tale posizione eminentemente attiva risulta confermata dall'art. 2094 c.c., il quale indentifica il lavoratore subordinato in colui che collabora nell'impresa «*alle dipendenze e sotto la direzione dell'imprenditore*»¹.

Nello svolgimento del rapporto di lavoro subordinato, la supremazia del datore si esplica attraverso il riconoscimento di una triade di poteri giuridici, esercitabili per la tutela di un interesse proprio, e tradizionalmente individuati nel potere direttivo, nel potere di controllo ed infine nel potere disciplinare.

Il potere di controllo è volto a verificare l'esatta esecuzione della prestazione lavorativa dedotta in contratto e tanto anche al fine dell'eventuale esercizio del potere disciplinare.

Tale potere rappresenta la naturale prosecuzione del potere direttivo, giacché consente di controllare che le disposizioni impartite in ordine al tempo ed alle modalità di esecuzione della prestazione lavorativa siano rigorosamente rispettate dal prestatore con la diligenza dovuta ai sensi e per gli effetti dell'art. 2104 c.c.², ed è presupposto logico e giuridico per l'esercizio del potere disciplinare, poiché solo all'esito della verifica di una violazione degli obblighi previsti, il datore di lavoro può irrogare la sanzione disciplinare (art. 2106 c. c.)³.

Il potere di controllo risulta essere particolarmente invasivo della sfera personale dei singoli dipendenti, ancor di più delle altre prerogative datoriali.

L'esercizio di tale potere per essere considerato legittimo deve, dunque, essere necessariamente temperato con i diritti fondamentali del lavoratore, aventi dignità giuridica pari alle contrapposte esigenze datoriali.

¹ Per la nozione di subordinazione giuridica si veda: M.V. BALLESTRERO – G. DE SIMONE, *Diritto del lavoro*, 2ª ed., Torino, 2015, 96 ss., nonché M. ROCCELLA, *Manuale di diritto del lavoro: mercato del lavoro e rapporti di lavoro*, 5ª ed., Torino, 2013, 44 ss.

² Art. 2104 c.c.: «*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*».

³ Cfr. R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. n. 21/2015)*, in *Riv. dir. lav.*, 2016, I, 77 ss.

Espressione del bilanciamento tra contrapposti interessi che deve essere inevitabilmente realizzato nel rapporto di lavoro subordinato è l'art. 41 della Costituzione, che sancisce il principio della libertà d'iniziativa economica privata purché esercitata nel rispetto della sicurezza, della libertà e della dignità umana.

A causa della difficile ricerca di un punto di equilibrio tra l'interesse del datore di lavoro al corretto adempimento della prestazione lavorativa e la tutela della dignità, libertà e riservatezza del lavoratore, la disciplina del potere di controllo del datore di lavoro ha da sempre generato incertezze di natura interpretativa

I tentativi operati dalla dottrina di circoscrivere l'esercizio di tale potere, attraverso la previsione di limiti soggettivi e oggettivi, sono rimasti senza seguito per lungo tempo e tanto anche a causa dell'assenza di un fondamento normativo⁴.

1. Il divieto di controlli a distanza.

La traduzione normativa dell'esigenza di circoscrivere il potere di controllo datoriale si è realizzata solamente con la promulgazione della legge n. 300 del 1970 (Statuto dei Lavoratori), prima fonte normativa a dettare una specifica disciplina in tema di potere di controllo datoriale, mancando nel Codice Civile una disposizione che ne individuasse le modalità di esercizio.

Lo Statuto dei lavoratori si proponeva di modificare il tradizionale assetto del rapporto di lavoro subordinato, improntato ad un'organizzazione di tipo gerarchico e di comando che vedeva il lavoratore in una posizione di soggezione, tendendo al riequilibrio delle posizioni, attraverso l'individuazione di limiti e vincoli all'esercizio dei poteri datoriali⁵.

Se è vero che il contratto di lavoro subordinato legittima l'esercizio di una serie di poteri da parte del datore di lavoro, è altrettanto vero che questi poteri incontrano dei limiti non solo derivanti dalle esigenze tecnico produttive dell'impresa, ma indotti, altresì, dalla necessità di rispettare precisi valori quali la libertà, la dignità e la riservatezza del lavoratore⁶.

Diverse sono le norme contenute nello Statuto dei lavoratori dedicate alla disciplina del potere di controllo datoriale, e dirette a delinearne i confini, come nel caso in cui il datore si avvalga per l'esercizio di detto potere dell'operato di altri soggetti, quali guardie giurate e personale di vigilanza (art. 2 e art. 3 Stat. Lav.).

Particolare rilevanza assume l'art. 4 dello Statuto dei lavoratori che, nella sua originaria formulazione, sanciva un divieto assoluto di utilizzo di

⁴ Come sottolineato dalla dottrina nel codice civile vi è un salto logico e giuridico tra potere direttivo e potere sanzionatorio. Sul punto si veda: R. DEL PUNTA, *op.cit.*; V. FERRANTE, *Controllo sui lavoratori difesa della loro dignità e potere disciplinare a quarant'anni dallo Statuto*, in *Riv. dir. lav.*, 2011, n. 1, II, 73 ss.

⁵ Si veda la Relazione del Ministro Brodolini al Disegno di Legge, che è divenuto poi lo Statuto dei Lavoratori ove viene enunciato l'obiettivo di individuare i presupposti normativi per la creazione «*di un clima di rispetto della dignità e della libertà umana nei luoghi di lavoro, riconducendo l'esercizio dei poteri direttivo e disciplinare dell'imprenditore nel loro giusto alveo e cioè in stretta finalizzazione allo svolgimento delle attività produttive*».

⁶ Sul punto cfr. Cass. Civ., Sez. Lav., 2.5.2017, n. 10637; Cass. Civ., Sez. Lav., 9.2.2016, n. 2351; Cass. Civ., Sez. Lav., 27.5.2015, n. 10955, Cass. Civ., Sez. Lav., 23.2.2012, n. 2722.

apparecchiature tecnologiche e di impianti di videosorveglianza esclusivamente finalizzati al controllo a distanza dell'attività dei lavoratori.

Per controllo a distanza deve intendersi quella particolare forma di controllo diretta al monitoraggio della prestazione lavorativa ed eseguita per il tramite di strumenti elettronici che ne consentono la registrazione, permettendo, quindi, al datore di lavoro di verificare a distanza di tempo e luogo, l'esatta esecuzione da parte del lavoratore delle mansioni dedotte in contratto⁷.

A tale disposizione seguiva, poi, la facoltà delineata al secondo comma, di installare, a fronte di determinate esigenze ritenute meritevoli di tutela, e a condizione di ottenere la preventiva autorizzazione del sindacato o dell'autorità amministrativa, strumenti dai quali potesse derivare indirettamente la possibilità di un controllo a distanza⁸.

La *ratio* posta a fondamento della summenzionata previsione andava ravvisata nell'intento del legislatore di contemperare l'interesse del datore di lavoro ad utilizzare gli strumenti necessari per la gestione dell'impresa o per la sicurezza di persone e cose, con quello opposto del lavoratore a non veder leso il proprio diritto alla riservatezza, attraverso forme di controllo assiduo e continuo, poste in essere mediante l'installazione incontrollata di apparecchiature idonee ad eliminare ogni zona di autonomia nello svolgimento del lavoro⁹.

In presenza, quindi, di determinate esigenze aziendali era previsto un bilanciamento degli interessi in gioco attraverso una procedura di concertazione diretta a raggiungere una soluzione concordata tra le parti interessate, volta ad evitare potenziali pregiudizi per la dignità e la riservatezza dei lavoratori.

Con l'avvento del progresso tecnologico ed informatico, la disciplina statutaria ha mostrato i suoi limiti, in quanto incapace di stare al passo con l'evoluzione tecnologica e di intercettare le nuove forme di controllo.

L'innovazione tecnologica ha alterato il presupposto su cui si basava la norma statutaria, ovvero la sussistenza di controlli derivanti esclusivamente da apparecchiature esterne alla prestazione lavorativa o comunque distinte dai processi produttivi; con l'avvento delle nuove tecnologie nel mondo del lavoro, invece, il controllo è divenuto possibile attraverso gli stessi strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e, come tali, inscindibili dal sistema produttivo¹⁰.

Detti strumenti, oltre a consentire un controllo costante e persistente del lavoratore, potenzialmente più pervasivo rispetto a quello realizzabile attraverso le apparecchiature esistenti alla data di entrata in vigore dello Statuto dei lavoratori, permettevano la registrazione continua delle

⁷ Secondo M. DELL'OLIO, *Art. 4 stat. lav. ed elaboratori elettronici*, in *Dir. Lavoro*, 1986, 487 ss., la distanza rileva come soluzione di continuità, come mancanza di contatto biunivoco e impossibilità di accorgersi del controllo nel momento in cui viene attuato.

⁸ La giurisprudenza ha affermato la legittimità di quei controlli c.d. difensivi ovvero diretti ad accertare condotte illecite del lavoratore. Detti controlli non rientrano nel divieto sancito dall'art. 4 dello Statuto dei lavoratori. Cfr. sul punto: Cass. Civ., sez. lav., 17 luglio 2007, n. 15892; Cass. Civ., sez. lav., 3 aprile 2002, n. 4746.

⁹ A. BELLAVISTA, *I poteri dell'imprenditore e la privacy del lavoratore*, in *Dir. Lavoro*, 2002, n. 1, 157 ss.

¹⁰ P. ICHINO, *Le conseguenze dell'innovazione tecnologica sul diritto del lavoro*, in *Riv. it. dir. lav.*, 2017, 525 ss.

informazioni relative all'attività svolta per il loro tramite, incrementando il rischio di una lesione della privacy dei lavoratori.

Sotto questo aspetto, dunque, l'art. 4 dello Statuto dei Lavoratori appariva obsoleto e inadatto a realizzare una effettiva tutela della riservatezza dei lavoratori, in quanto si limitava a prescrivere le condizioni di legittimità dei controlli, senza prevedere misure di prevenzione delle violazioni alla privacy dei lavoratori.

Tale criticità ha reso necessario l'intervento del legislatore al fine di prevedere una regolamentazione più incisiva dei controlli a distanza, idonea da un lato a contenere l'accrescimento dei poteri datoriali derivante dall'utilizzo di nuove tecnologie e, dall'altro, a contemperare le esigenze produttive ed organizzative dell'impresa con la tutela della riservatezza dei lavoratori.

Con l'art. 23, D.Lgs. n. 151/2015 (c.d. Jobs Act) e con il successivo art. 5, 2° co., D.Lgs. n. 185/2016, è stato novellato l'art. 4, legge n. 300/1970, adeguandolo alle innovazioni tecnologiche nel frattempo intervenute¹¹.

Il legislatore, preso atto della diffusione di nuove tecnologie e dell'introduzione di strumenti informatici a supporto dell'attività lavorativa, ha individuato un regime differente con riferimento a due distinte fattispecie: la prima concernente impianti audiovisivi, la seconda relativa agli strumenti di lavoro (quali, ad esempio, computer, cellulari, tablet, posta elettronica) ed agli strumenti di registrazione degli accessi e delle presenze.

In riferimento alla prima fattispecie, l'art. 4, 1° comma, vieta l'installazione di impianti audiovisivi e di altri strumenti¹², dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori, salvo che gli stessi siano impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

Va considerato che, sebbene il divieto generale del 1° comma dell'art. 4 St. Lav. nella sua formulazione originaria non risulti più espressamente sancito, lo stesso continua ad essere implicitamente riconosciuto, essendo ammessa l'installazione di impianti audiovisivi o altri strumenti, ivi compresi specifici software, che consentono incidentalmente il controllo a distanza dei lavoratori, solo per determinate e specifiche finalità, risultando, per converso, vietata in ogni altro e diverso caso¹³.

Peraltro accanto alle esigenze organizzative e produttive e alla sicurezza sul lavoro compare, per la prima volta, l'esigenza di tutela del patrimonio aziendale, che sembra aver comportato il superamento della giurisprudenza sui controlli difensivi¹⁴.

¹¹ Sull'argomento: BARRACO-A. SITZIA, *Potere di controllo e privacy (Lavoro, riservatezza e nuove tecnologie)*, Milano, 2016, 83 ss.; V. MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Arg. dir. lav.*, 2015, 1186 ss.

¹² La norma ha sostituito il termine «apparecchiatura» con quello onnicomprensivo di «strumento».

¹³ Sul punto A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello statuto dei lavoratori*, in *Riv. dir. lav.*, 2016, I, 517 ss.; M.T. Salimbeni, *La riforma dell'articolo 4 dello statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *Riv. dir. lav.*, 2015, n. 4, 602 ss.

¹⁴ I. ALVINO, *I nuovi limiti al controllo a distanza dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del codice della privacy*, in *Lab. & Law Iss.*, 2016, vol. 2, n. 1, 3 ss. R. FRATINI e R. MAURELLI, *La nuova disciplina dei controlli a distanza nel dialogo fra art. 4 e codice privacy*, in *Lavoro e prev. oggi*, 2020, 714 ss. Si veda tuttavia in senso contrario Cass. civ., sez. lav., 8 novembre 2016, n. 22662: «In tema di controllo del lavoratore, non è soggetta alla disciplina dell'art. 4, comma 2, st.lav., l'installazione di impianti ed apparecchiature di controllo poste a tutela del patrimonio aziendale dalle quali non derivi anche la possibilità di

È stata, inoltre, confermata l'altra condizione di legittimità per l'installazione, già posta dall'originaria formulazione statutaria, rappresentata dall'obbligo di ottenere il preventivo accordo sindacale o, in mancanza, l'autorizzazione amministrativa dell'Ispettorato del lavoro¹⁵.

Per l'installazione di detti strumenti è, dunque, ancora richiesto al datore di lavoro l'adempimento di una procedura preventiva volta a verificare la legittimità delle ragioni del controllo, nonché a stabilire modalità e limiti del funzionamento degli impianti.

2. La nuova categoria degli strumenti di lavoro.

La novità sostanziale della riforma dei controlli a distanza, contenuta nel D.Lgs. n. 151/2015 come successivamente modificato ed integrato, concerne gli strumenti utilizzati dal lavoratore per lo svolgimento della propria prestazione.

In particolare, il legislatore, preso atto dell'evoluzione tecnologica che ha reso alcuni dispositivi indispensabili per lo svolgimento della prestazione lavorativa, ha inteso creare una disciplina *ad hoc* per gli stessi.

Il secondo comma del nuovo art. 4 prevede che *«i limiti e le procedure di cui al primo comma non si applicano agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze»*.

Pertanto cellulari, computer, tablet, GPS satellitari delle autovetture, e qualsiasi altro strumento utilizzato dal lavoratore per svolgere la propria attività, qualora siano annoverabili tra gli strumenti di lavoro, nonché i badges, non sono soggetti alla duplice limitazione delle finalità del controllo e delle procedure di autorizzazione preventiva a carattere sindacale o amministrativo.

Tale previsione è espressione della volontà del legislatore di snellire l'installazione e l'impiego degli strumenti utilizzati dal lavoratore per eseguire la prestazione lavorativa o per accedere ai luoghi di lavoro, sottraendoli alla disciplina di cui al primo comma.

I controlli dell'attività in tali casi, infatti, derivano da strumenti che per la loro stessa funzione, non possono essere assoggettati a vincoli causali e a garanzie procedurali, senza di fatto andare a limitare l'autonomia organizzativa del

controllo a distanza dell'attività lavorativa, né risulti in alcun modo compromessa la dignità e riservatezza dei lavoratori»; nonché Cass. pen., sez. III, 27 gennaio 2021, n. 3255.

Inoltre, sul punto ed in particolare in tema di vigilanza occulta, Cfr. CEDU, Grand Chamber, 17 ottobre 2019, ric. n. 1874/13 e 8567/13, in *Riv. giur. Lavoro*, 2020, II, 237, con nota di M. D'APONTE, *I controlli a distanza e la videosorveglianza nei luoghi di lavoro tra diritto nazionale e giurisprudenza della CEDU*. In particolare la Corte Europea dei diritti dell'uomo ha stabilito la legittimità della videosorveglianza del datore di lavoro sui propri dipendenti, nonostante la carenza di informazioni, qualora il controllo sia disposto in presenza di evidenti indizi di illeciti dei lavoratori ai danni del patrimonio aziendale purché lo stesso sia proporzionato e adeguato al solo fine di reprimere tali illeciti, nonché bilanciato con i diritti alla riservatezza dei dipendenti.

Cfr. sul punto, altresì, CIRIELLO e ARIANTE, *Videosorveglianza "occulta" sul luogo di lavoro: il caso López Ribalda e altri c. Spagna*, e la giurisprudenza della Corte Europea dei Diritti dell'Uomo, in *Lav. dir. Europa*, 2019, 1 ss.

¹⁵ In proposito, la giurisprudenza reputa inderogabile la sussistenza di un contratto collettivo e, pertanto, non sostituibile dal consenso/autorizzazione dei lavoratori dell'azienda considerati *uti singuli*, anche se risultante per iscritto. Cfr. sul punto: Cass. pen., sez. III, 8 maggio 2017, n. 22148; Cass. pen., sez. III, 24 agosto 2018, n. 38882; Cass. pen., sez. III, 17 dicembre 2019, n. 50919; Cass. pen., sez. III, 17 gennaio 2020, n. 1733.

datore di lavoro che si estende anche alla individuazione dei mezzi necessari all'organizzazione del lavoro.

All'indomani della riforma è sorta sin da subito l'esigenza di individuare i limiti di operatività della predetta disposizione, al fine di evitare un uso distorto della medesima, volto a sottrarre qualsiasi dispositivo offerto in dotazione al lavoratore alla disciplina stringente del primo comma dell'art. 4 Stat. Lav.

E tanto ancor di più se si consideri che manca una nozione semantica di strumento di lavoro, in quanto è da considerarsi tale solo quello che è strettamente connesso con l'attività svolta in concreto dal singolo lavoratore, in ragione, dunque, della funzione che lo strumento assolve in concreto nell'organizzazione aziendale e non delle sue caratteristiche oggettive.

Seppur il 2° comma dell'art. 4 Stat. lav. non individui espressamente gli strumenti di lavoro, né menzioni specificamente gli strumenti informatici, digitali o satellitari, è evidente che il legislatore abbia inteso riferirsi soprattutto a questi.

Rappresentano strumenti di lavoro, pertanto, non soltanto gli impianti e le apparecchiature stabili, e dunque concretamente percepibili dal punto di vista materiale, ma tutte quelle tecnologie incorporate in altre apparecchiature.

Il termine generico «strumenti» deve riferirsi, difatti, a entrambe le componenti di un sistema: l'hardware, ossia lo strumento di lavoro, (quale il computer, il cellulare, il tablet) ed i software nonché gli applicativi, ovverosia tutti quei programmi a cui accede il lavoratore, che consentono il fisiologico e sicuro funzionamento dei dispositivi¹⁶.

Ciò comporta una necessaria individuazione della funzionalità di ciascun software al fine stabilire il tipo di controllo effettuabile e la disciplina applicabile¹⁷.

La posta elettronica aziendale¹⁸ e l'accesso alla rete internet sono, ad esempio, annoverabili tra gli strumenti di lavoro, ma, in determinati casi, sono suscettibili di diventare veri e propri strumenti di controllo a distanza¹⁹.

Sul punto il Garante ha precisato che, qualora vi siano dei sistemi che permettano un controllo minuzioso del traffico e-mail da parte del datore di lavoro (nella forma di c.d. backup) attraverso software aggiuntivi che consentano una conservazione massiva dei dati al di fuori delle esigenze tecniche di funzionamento/sicurezza del servizio, allora si tratta di strumenti di controllo a distanza del lavoratore, con tutte le conseguenze che ne derivano²⁰.

¹⁶ A. MARESCA, *I controlli tecnologici a distanza*, in *Lavoro e prev.* oggi, 2021, 10 ss.

¹⁷ P. TULLINI, *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 97 ss.

¹⁸ Cfr. Linee guida del Garante per posta elettronica e internet del 01.03.2007, doc. web n. 1387522.

¹⁹ In tema di controllo datoriale occulto sulla navigazione internet e sulla posta elettronica aziendale, cfr., CEDU, Sez. IV, 12 gennaio 2016, ric. n. 61496/08, *Barbulescu c. Romania*, in *Riv. it. dir. lav.*, 2016, II, 279 ss., con nota di C. CRISCUOLO, *Il controllo sugli account di posta elettronica e di messaging aziendale*; nonché C. JERVIS, *Barbulescu v Romania: Why There is no Room for Complacency When it Comes to Privacy Rights in the Workplace*, in *EJIL: Talk!*, 2017; F. PERRONE, *La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei Diritti dell'Uomo e giurisdizione nazionale dopo la sentenza Barbulescu*, in *Labor*, 2018, 283; E. SYCHENKO E D. CHERNYAEVA, *The Impact of the ECHR on Employee's Privacy Protection*, in *Italian labour law e-journal*, 2019, 171.

²⁰ Cfr. Provv. Garante per la protezione dei dati personali, 13 luglio 2016, n. 303, nonché con riguardo alla posta elettronica aziendale: Garante per la protezione dei dati personali, 30 luglio 2015, n. 456, doc. web n. 4298277; Garante per la protezione dei dati personali, 22 dicembre 2016, n. 547, doc. web n. 5958296; Garante per la protezione dei dati personali, 1 febbraio 2018, n. 53, doc. web n. 8159221; Garante per la protezione dei dati personali, 4 dicembre 2019, n. 216, doc. web n. 9215890.

Ad analoga conclusione si deve giungere per i sistemi di geolocalizzazione installati sui tablet, smartphone e sulle vetture concesse in uso al dipendente, ma solo laddove gli stessi siano necessari per rendere la prestazione lavorativa, come nel caso in cui il lavoratore incaricato della manutenzione di impianti debba effettuare gli interventi in diversi luoghi.

Diversa è l'ipotesi in cui la prestazione lavorativa non sia caratterizzata da mobilità territoriale. In tal caso, il sistema di geolocalizzazione non risulterebbe funzionale alla corretta esecuzione della prestazione lavorativa divenendo strumento riconducibile alla fattispecie degli strumenti di controllo, legittimi ai sensi dell'art. 4, 1° comma, solo se finalizzati a soddisfare una delle esigenze ivi previste²¹.

La ricostruzione proposta trova conferma nei chiarimenti forniti dal Ministero del Lavoro che, con la nota del 18 giugno 2015, nell'illustrare la corretta interpretazione da attribuire all'espressione *«per rendere la prestazione lavorativa»*, ha precisato che *«l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che "serve" al lavoratore per adempiere la prestazione: ciò significa che, nel momento in cui tale strumento viene modificato (a esempio, con l'aggiunta di appositi software di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione»*.

Rilevante è anche il chiarimento fornito dal Garante per la protezione dei dati personali che, con verifica preliminare del 16.03.2017, ha precisato che possono considerarsi strumenti di lavoro tutti quei dispositivi *«utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa»*, ovvero *«direttamente preordinati all'esecuzione della prestazione lavorativa»*.

L'interpretazione fornita alla fattispecie in esame risulta essere, dunque, particolarmente restrittiva, in quanto volta a circoscrivere la sfera di azione libera per il datore di lavoro, negando l'applicazione della disciplina di cui al 2° comma, a tutti quei componenti ed applicativi aggiunti, non costituenti mezzo di esecuzione della prestazione, bensì installati ed utilizzati prevalentemente ad altri fini, pure se accessori o connessi ad essa (quali ad esempio quelli di sicurezza come i programmi antivirus). Dette modifiche, se potenzialmente capaci di controllo a distanza, possono avvenire solo alle condizioni ricordate sopra: la ricorrenza di particolari esigenze, l'accordo sindacale o l'autorizzazione amministrativa.

La seconda tipologia di strumenti sottratti alla procedura autorizzatoria di cui al 1° comma è costituita dagli strumenti di registrazione degli accessi e delle presenze.

Si tratta prevalentemente della categoria dei badges aziendali che registrano l'entrata e l'uscita dall'azienda, che altro non è che l'evoluzione dei cartellini marca-tempo.

Anche per tale categoria si deve propendere per una interpretazione più garantista per il lavoratore, limitandola a quegli strumenti che consentono

²¹ Si veda in tal senso la circolare del 07.11.2016, n. 2 dell'INL. Nello stesso senso: Garante per la protezione dei dati personali, 16 marzo 2017, n. 138, doc. web n. 6275314; Garante per la protezione dei dati personali, 18 aprile 2018, n. 232, doc. web n. 9358266. Nonché in tema di geolocalizzazione dei dipendenti: Garante per la protezione dei dati personali, 9 gennaio 2020, n. 8.

esclusivamente il controllo sui dati dell'entrata, della permanenza e dell'uscita dal luogo di lavoro, ed escludendo quegli apparecchi che raccolgano anche altre informazioni, quali spostamenti interni ed esterni ai locali aziendali, permessi, pause, e relative tempistiche²².

A causa della laconica formulazione della disposizione di legge, inoltre, non è chiaro se il 2° comma della norma in commento, debba ritenersi limitato solo agli accessi fisici, oppure comprenda anche agli accessi virtuali tramite computer o sistemi informatici.

Il tenore letterale della norma non sembra ostare alla possibilità di ricondurre alla fattispecie tipica anche le registrazioni di accesso alla rete informatica aziendale²³.

3. L'impatto dell'Industria 4.0 sulla disciplina statutaria.

I problemi sin qui descritti in ordine alle potenzialità intrusive del controllo datoriale risultano amplificati nella Industria 4.0, in cui si sta diffondendo un approccio lavorativo sempre più digitalizzato, che richiede necessariamente l'integrazione tecnologica per lo svolgimento della prestazione lavorativa, con l'evidente rischio di una dilatazione dell'area di esonero di cui all'art. 4, 2° co., St. Lav.²⁴.

La digitalizzazione applicata ai processi produttivi (specialmente Cloud Computing, Internet of Things) rende ancora più labile, sino ad annullarla, la distinzione tra strumento di controllo e strumento di lavoro, in quanto pressoché tutti gli apparati tecnologici sono utilizzati per rendere la prestazione lavorativa.

In tale contesto, le tecnologie informatiche e digitali sono diventate gli strumenti principali di esecuzione della prestazione lavorativa e di gestione delle relazioni aziendali, dando vita ad una nuova configurazione del rapporto di lavoro.

Gli strumenti di lavoro finiscono con l'identificarsi con il sistema informatico aziendale e al quale si connettono i dipendenti per svolgere la prestazione lavorativa, attraverso postazioni, fisse o mobili, poste all'interno o all'esterno del luogo di lavoro.

Al tempo stesso l'utilizzo delle risorse informatiche all'interno dei locali aziendali, o in collegamento remoto, consente forme di controllo della

²² Secondo la dottrina prevalente la previsione concerne altresì i badges che registrano l'accesso a particolari aree. Sul punto M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in *Arg. dir. lav.*, 2016, 505 ss.

I badges Radio - Frequency Identification (c.d. RFID) - sono invece considerati strumenti di controllo e come tali non rientrano nella previsione del comma 2: Cfr. sul punto Cass. Civ., Sez. Lav., 13.5.2016, n. 9904.

²³ A. MARESCA, *I controlli tecnologici a distanza*, 14.

²⁴ Sul rapporto tra innovazione tecnologica e controllo dei lavoratori si veda: cfr. R. BALDWIN, *Rivoluzione globale. Globalizzazione, robotica e futuro del lavoro*, Bologna, 2020; C. CROUCH, *Se il lavoro si fa gig*, Bologna, 2019; V. NUZZO, *La protezione del lavoratore dai controlli impersonali*, Napoli, 2018; A. SITZIA, *Coronavirus, controlli e "privacy" nel contesto del lavoro*, in *Lav. giur.*, 2020, 495 ss.; A. INGRAO, *Data-Driven management e strategie collettive di coinvolgimento dei lavoratori per la tutela della privacy*, in *Labour Law Issue*, 2019, 129 ss. Sull'evoluzione digitale e sui suoi impatti nel potere di controllo del datore di lavoro, si veda: A. SARTORI, *Il controllo tecnologico sui lavoratori*, Torino, 2020; I. PICCININI e M. ISCERI, *IA e datori di lavoro, verso una e-leadership?*, in *Lav. dir. Europa*, 2021.

prestazione lavorativa particolarmente pervasiva, oltre che un trattamento automatizzato dei dati dei lavoratori.

In particolare, l'esigenza di garantire l'integrità e la sicurezza della rete aziendale fornisce ai datori di lavoro nuovi strumenti potenzialmente idonei a consentire un controllo (spesso occulto) sull'operato dei dipendenti²⁵.

All'interno della rete aziendale i controlli sulle informazioni sono riconducibili a due tipologie: controlli effettuati dall'amministratore di sistema, attraverso l'analisi di file di log, e controlli bidirezionali dei dati trattati dallo strumento di lavoro, effettuati con firewall e proxy.

Detti strumenti, attraverso il monitoraggio del traffico di rete e dei singoli accessi, permettono di processare in maniera automatica i dati e di ottenere, così, informazioni anche non attinenti alla prestazione lavorativa.

L'ampliamento della sfera di azione libera del datore di lavoro costituisce, dunque, l'inevitabile conseguenza della struttura della Industria 4.0, nonché dell'attuale formulazione dell'art. 4 St. Lav.

In tale contesto si corre il rischio di legittimare il controllo a distanza da parte del datore di lavoro, divenuto parte integrante dell'ambiente digitale, giacché l'uso dei nuovi strumenti di lavoro incorpora fisiologicamente una componente di controllo.

Analoghe difficoltà incontra l'applicazione della disciplina statutaria laddove l'attività lavorativa sia esternalizzata, sfruttando le risorse del web e la connettività da remoto con l'impresa.

È il caso del lavoro agile, c.d. smart working, emblema dell'impatto della digitalizzazione sul rapporto di lavoro, che consente al lavoratore l'esecuzione della prestazione lavorativa in forma delocalizzata, mediante l'utilizzo di dispositivi mobili connessi alla rete aziendale.

È da premettere che ogni dispositivo in grado di interfacciarsi con una rete, pubblica o privata, con conseguente condivisione dei contenuti, comporta il rischio di una sottoposizione ad un controllo occulto da parte di terzi.

Il datore di lavoro, sfruttando le predette potenzialità, può accedere agevolmente al contenuto del dispositivo utilizzato dal lavoratore e alla navigazione internet effettuata mediante il server aziendale, come pure alla posta elettronica.

Per rendere la prestazione a distanza il lavoratore può avvalersi di due differenti modelli: il BYOD (Bring Your Own Device) che prevede la possibilità di utilizzare i propri dispositivi per collegarsi alla rete aziendale, ed il COPE (Corporate Owned Personally Enabled), dove è l'azienda a fornire ai dipendenti i dispositivi da utilizzare durante la propria attività lavorativa²⁶.

Tali modelli pongono la questione di bilanciamento del diritto del datore di lavoro di implementare misure di sicurezza per contenere i pericoli a cui viene esposto il patrimonio aziendale, e quello alla tutela dei dati personali del lavoratore.

Vi è il potenziale rischio, difatti, che il datore di lavoro, nel monitorare l'attività svolta e nell'installare applicativi volti a garantire la sicurezza dei dati aziendali, realizzi una violazione della privacy del lavoratore, acquisendo

²⁵ Per tutti, E. MINGIONE, *Lavoro: la grande trasformazione*, Milano 2020; A. CIPRIANI, A. GRAMOLATI e G. MARI, *Il lavoro 4.0 La quarta rivoluzione industriale e la trasformazione dell'attività lavorativa*, Firenze, 2018.

²⁶ Cfr. A. STROZZIERI e M. PARPAGLIONI, *Controlli a distanza sui lavoratori e tutela della privacy*, Milano, 2021;

informazioni che esulano dall'ambito strettamente lavorativo e riguardino, piuttosto, la vita privata del dipendente²⁷.

E tanto ancor di più nel caso del modello BYOD, ove all' interno del medesimo dispositivo si creano due diverse aree informatiche, dedicate rispettivamente ai dati personali del lavoratore e ai dati aziendali, con l'inevitabile rischio di possibili interferenze fra le stesse.

In mancanza di una prescrizione restrittiva contenuta nella norma statutaria in relazione alla titolarità del dispositivo, non può escludersi a priori che i dispositivi c.d. BYOD possano essere annoverati tra gli strumenti di lavoro ex art. 4, 2° comma St. Lav., purché siano effettivamente funzionali allo svolgimento dell'attività lavorativa da parte del dipendente, ancorché di sua proprietà.

Tuttavia i rischi di controllo e di profilazione del lavoratore connessi a tali tecnologie, appaiono inevitabili, in quanto connaturati a detta tipologia di rapporti di lavoro.

In ogni caso, al fine di evitare che il dispositivo sia oggetto di un controllo occulto da parte di terzi, si renderà opportuna l'adozione di filtri o di altri meccanismi analoghi che riducano, se non addirittura eliminino, la possibile interferenza dei due ambienti.

Le considerazioni appena svolte consentono di sostenere che, nei contesti produttivi ad elevata digitalizzazione, ove il lavoro è svolto prevalentemente in rete e spesso all'esterno dei locali aziendali, l'attuale disciplina statutaria appare inadeguata a regolamentare in maniera incisiva l'esercizio del potere di controllo tecnologico datoriale e a garantire un'effettiva tutela del lavoratore, in quanto le tecnologie di ultima generazione, divenute di uso comune anche nel mondo del lavoro, consentono un controllo a distanza dell'attività lavorativa senza soluzione di continuità.

4. L'utilizzabilità delle informazioni raccolte.

Sebbene il legislatore, abbia inteso non sottoporre gli strumenti di cui al 2° comma ai vincoli causali e alle garanzie di cui al 1° comma, ha ritenuto necessario tutelare il lavoratore per quanto concerne l'aspetto le informazioni raccolte attraverso gli stessi, individuando i limiti entro i quali le stesse possono essere utilizzate.

Le moderne tecnologie, difatti, consentono di svolgere trattamenti ulteriori rispetto a quelli strettamente connessi all'attività lavorativa e ciò, all'insaputa o senza la piena consapevolezza dei lavoratori.

Nell'attuale mondo del lavoro il problema maggiore non è esclusivamente quello di impedire che il personale dipendente sia sottoposto ad un controllo costante ed occulto, ma è, altresì, quello di evitare che il datore di lavoro, venuto in possesso di dati personali relativi al lavoratore, possa utilizzarli abusando dei propri poteri.

²⁷ L. FIORILLO e A. PERULLI, *Il jobs act del lavoro autonomo e del lavoro agile*, Torino, 2018, 213; C. SPINELLI, *Tecnologie digitali e lavoro agile*, Bari, 2018.

L'art. 4 nella versione statutaria non si premurava di disciplinare il profilo dell'utilizzabilità delle informazioni raccolte, limitandosi a dettare le condizioni di legittimità per la predisposizione del controllo.

L'attuale formula dell'art. 4 Stat. Lav. disciplina una fase logicamente successiva dell'esercizio del potere di controllo, quella dell'utilizzazione dei dati che inizia quando le informazioni reperite attraverso gli strumenti di cui ai precedenti commi, entrano nella disponibilità del datore di lavoro²⁸.

Nel 3° comma dell'articolo in commento è, dunque, racchiusa la tutela del dipendente destinata ad operare nella fase in cui, all'esito dei controlli a distanza legittimamente effettuati conformemente ai commi precedenti, il datore di lavoro si avvalga dei dati acquisiti, utilizzandoli per tutti i fini connessi al rapporto di lavoro²⁹.

Sia che si tratti di impianti audiovisivi o di altri strumenti di potenziale controllo a distanza, sia che si tratti di strumenti di lavoro, le informazioni raccolte attraverso gli stessi possono essere utilizzate per «*tutti i fini connessi al rapporto di lavoro*» e, dunque, anche a fini disciplinari, purché siano rispettate le condizioni di cui all'art. 4 Stat. Lav.

L'utilizzo dei dati raccolti, orbene, è legittimo solo alla duplice condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e che sia garantito il rispetto della disciplina vigente a tutela della privacy.

Il nuovo art. 4 Stat. Lav. rafforza i diritti conoscitivi del lavoratore, richiedendo al datore di lavoro l'obbligo di fornire ai propri dipendenti un'adeguata informazione delle modalità d'uso delle apparecchiature di controllo e di effettuazione dei controlli, attraverso un apposito regolamento interno.

L'informativa deve essere redatta in maniera chiara, comprensibile ed esaustiva e deve contenere l'indicazione, in maniera particolarmente dettagliata, degli strumenti che consentono il controllo a distanza, delle modalità e delle regole di utilizzo di tali strumenti, del tipo di controlli che potranno essere effettuati dall'azienda e delle eventuali sanzioni.

Quanto alla forma, l'informativa può essere contenuta in documenti autonomi, formati *ad hoc* dal datore, oppure, in alternativa, può essere inserita anche nelle policy aziendali tramite una loro integrazione.

In ogni caso si rende necessario che la stessa sia portata a conoscenza di tutti i lavoratori con modalità adeguate, o attraverso comunicazioni individuali, o mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori.

L'obbligo informativo posto a carico del datore di lavoro costituisce, dunque, uno strumento di tutela del lavoratore, il quale deve essere posto in una condizione di consapevolezza, con la conseguenza che in caso di mancata informazione, il trattamento dei dati raccolti sarà illecito e gli stessi saranno inutilizzabili sia dal punto di vista sostanziale, che dal punto di vista processuale, non potendo essere impiegati come prova in giudizio.

²⁸ A. Maresca, *op.cit.*, 522 ss.

²⁹ Secondo G. BUSIA, *Così vicini, così distanti: i controlli da remoto del datore di lavoro e la riservatezza del dipendente*, in *Lav. dir. Eur.*, 2020, è emblematico che all'interno dell'ordinamento italiano la tutela dei dati personali del lavoratore abbia preceduto quella del consumatore e del cittadino.

Tuttavia, nell'attuale era della digitalizzazione, il rischio è che, nonostante la prescrizione dell'obbligo di informativa, determinate tipologie di monitoraggio sfuggano alla consapevolezza del dipendente, il quale si trova ad interfacciarsi con tecnologie particolarmente avanzate con conseguente difficoltà di comprensione delle concrete possibilità di controllo dalle stesse promananti.

A questo onere di informazione deve, comunque, affiancarsi, il dovere di fornire ai lavoratori apposita informativa ex artt. 13 e 14 del Regolamento europeo (ex art. 13 D. Lgs. 196/2003)³⁰.

Ulteriore condizione di legittimità per l'utilizzabilità di tutti i dati raccolti nel corso del rapporto di lavoro, attraverso gli strumenti tecnologici e/o strumenti di lavoro, è il rispetto della disciplina in materia di trattamento e protezione dei dati personali, e dunque del D.Lgs n. 196/2003, c.d. Codice della Privacy, e del Reg. UE 2016/679 (GDPR).

L'art. 4, 3° comma, Stat. Lav., prevede espressamente la possibilità di utilizzare le informazioni acquisite con il controllo, purché siano rispettati i principi che governano il trattamento dei dati personali³¹.

La disciplina di protezione dei dati personali consente che il datore di lavoro tratti i dati personali dei lavoratori, anche relativi a categorie particolari di dati (cfr. art. 9, par. 1, del Regolamento), nel rispetto dei principi generali del trattamento, ossia il principio di liceità, correttezza, trasparenza, limitazione della finalità perseguita, minimizzazione, esattezza dei dati, limitazione della conservazione e integrità³².

Tali principi, in buona sostanza, impongono al titolare del trattamento, e dunque al datore di lavoro, di ridurre i rischi di un trattamento illecito dei dati.

L'esercizio del potere di controllo è, in particolare, condizionato dai principi di finalità e minimizzazione del trattamento che impongono al titolare di garantire che i dati personali siano raccolti per finalità determinate, specifiche e ben definite, e che successivamente siano trattati in modo compatibile con dette finalità.

³⁰ A. MARESCA, *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore*, Milano, 2016, secondo cui l'informativa sulle modalità d'uso degli strumenti e di effettuazione dei controlli non coincide con l'informativa relativa alla privacy. Si veda anche A. SITZIA, *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore)*, in *Labour & Law Issues*, 2016, 83 ss.

³¹ G. PROIA, *Trattamento dei dati personali, rapporto di lavoro e l'«impatto» della nuova disciplina dei controlli a distanza*, in *Riv. it. dir. lav.*, 2016, 547 ss.

³² Cfr. art. 5 GDPR «I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il trattamento, al contempo, deve presentarsi adeguato pertinente e limitato a quanto necessario rispetto alle finalità per le quali si è inteso operarlo.

Il datore di lavoro nell'esercizio del potere di vigilanza deve utilizzare, quindi, gli strumenti di controllo strettamente indispensabili, al fine di minimizzare l'accesso ai dati riferibili ai lavoratori e adottare tutte le misure organizzative e tecnologiche idonee a ridurre al minimo il trattamento dei dati da raccogliere, e procedere alla cancellazione di quelle informazioni eccedenti rispetto alla finalità dichiarata.

E tanto in virtù del principio di accountability, alla base del Regolamento Europeo, che richiede al datore di lavoro di rispettare i predetti principi e di essere in grado di dimostrare di aver adottato comportamenti proattivi idonei a ridurre il rischio di un trattamento illecito³³.

Alla luce della novella, il datore di lavoro dovrà, pertanto, prestare particolare attenzione agli strumenti di controllo che deciderà di adottare in azienda, in quanto il rispetto dei limiti finalistici e procedurali previsti dalla norma statutaria non è di per sé sufficiente a garantire la liceità del trattamento, essendo necessario che il potere di controllo sia esercitato nel rispetto dei limiti sostanziali, rinvenibili nella disciplina privacy.

A ben vedere, dunque, sebbene la condizione procedurale e contenutistica prevista dall'art. 4, 3° co., St. Lav., rafforzi la tutela dei lavoratori, la stessa non pare avere una piena efficacia deterrente rispetto ad un'indebita intrusione del datore nella sfera personale del dipendente, e tanto ancor di più nell'attuale contesto lavorativo, ove la digitalizzazione sfrutta le potenzialità delle nuove tecnologie per la raccolta, la rielaborazione elettronica e l'interconnessione di una notevole mole di dati dei dipendenti, acquisiti sia in dipendenza dello svolgimento dell'attività lavorativa, che mediante la consultazione di fonti esterne, e tanto anche a prescindere da una specifica volontà in tal senso.

Conclusioni.

Alla stregua delle considerazioni che precedono è evidente che nell'attuale era della digitalizzazione le moderne tecnologie intervenute nell'ambito dell'organizzazione produttiva se da un lato rappresentano una risorsa, dall'altro rappresentano fattori di rischio per la dignità e la riservatezza del lavoratore.

L'impatto della digitalizzazione e della trasformazione del mondo del lavoro nella Industry 4.0 è così dirompente da sollevare alcuni dubbi circa l'efficacia dell'art. 4 St. Lav., per quanto novellato, a disciplinare il potere di controllo, giacché l'uso delle tecnologie in tali casi risulta eminentemente funzionale allo

³³ Tale principio è consacrato nell'art. 24 del GDPR che stabilisce: «1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento».

svolgimento della prestazione lavorativa, con una conseguente dilatazione dell'ambito di operatività dell'art. 4, 2° comma, St. Lav.

La diffusione di tecnologie nel mondo del lavoro, inoltre, ha enormemente ampliato il potere datoriale di controllo, il cui esercizio è divenuto possibile non solo mediante le tradizionali apparecchiature ma anche attraverso gli strumenti utilizzati quotidianamente dal lavoratore, i quali sono in grado di realizzare un controllo capillare, costante e delocalizzato dell'attività lavorativa, particolarmente pervasivo.

Detto potere, divenuto una parte integrante dell'ambiente digitale, ha assunto nuovi connotati, che lo rendono più pervasivo per la possibilità di profilazione dei lavoratori offerta dalle nuove tecnologie.

Computer, smartphone, tablet, internet e posta elettronica, strumenti oggi necessari per lo svolgimento della prestazione lavorativa, oltre a costituire un'occasione di controllo del lavoratore, consentono, difatti, al datore di lavoro di acquisire, a posteriori, una quantità enorme di informazioni non solo attinenti alla prestazione lavorativa, ma anche di natura strettamente personale.

D'altra parte, la diffusione di detti strumenti, oltre che nel contesto lavorativo anche nella vita quotidiana, ha comportato una progressiva accettazione del controllo: il lavoratore tendenzialmente non percepisce le tecnologie digitali ed informatiche come una possibile causa di lesione ai propri diritti, quali la dignità e la riservatezza.

Di fronte all'incapacità del diritto del lavoro di rispondere efficacemente alle istanze di garanzia dei lavoratori, una funzione contenitiva dei poteri datoriali è senz'altro svolta dalla disciplina in materia di protezione di dati personali.

Tuttavia in assenza di specifiche disposizioni normative è richiesto un arduo compito esegetico agli operatori del diritto al fine di armonizzare la disciplina giuslavoristica con quella in materia di privacy.

Non si può escludere che in futuro si renderà necessario un nuovo intervento del legislatore, idoneo a regolamentare i nuovi strumenti di controllo al fine di garantire una tutela effettiva dei diritti fondamentali del lavoratore, primo fra tutti il diritto alla privacy.



The importance of being aware when acting in a commercial world.

IVANA GENESTRONE
Lawyer

Abstract

The Italian SA (Garante per la protezione dei dati personali) fined Enel Energia ('EE') over EUR 26.5 million on account of unlawfully processing users' personal data for telemarketing purposes. The Authority also imposed EE to implement several corrective measures to bring its processing activities into compliance with EU and domestic data protection law.

At the core of this impressive decision lies the heavy blame on a big market player such as EE for not having seriously taken and honoured the principle of accountability set forth by the combined provisions of art. 5, par. 2 and 24, GDPR¹.

As it results from the explanations given by the Authority for its enforcement provisions, the accountability required from a big player of the market towards the data subjects/consumers is at the highest level.

Under the new GDPR, a data controller must adopt proper means to (i) observe the legal obligation of being constantly aware of the respect of the fundamental rights of natural persons due to data subject/consumers, and (ii) demonstrate such awareness at any time.

Companies acting on the market need to adopt proper organisational model and KPI indicators to guarantee the awareness required by the new GDPR.



Keywords: accountability; privacy by design; GDPR; telemarketing; unsolicited communications; Italian SA; Garante per la protezione dei dati personali; EDPB; D.Lgs 231/01; sales network; organisational and technical measures; organisational model; KPI.

Summary: [Introduction](#). – [1. The complaints](#). – [2. EE's defense](#). – [3. The Italian SA allegations](#). – [4. The accountability principle as a legal obligation of the data controller to be constantly aware](#). – [Conclusions](#).

Introduction.

The Italian SA (*Garante per la protezione dei dati personali*) fined EE over EUR 26.5 million on account of unlawfully processing users' personal data for telemarketing purposes. In addition to paying the fine, the company was also ordered to implement several corrective measures imposed to bring its processing activities into compliance with EU and domestic data protection law.

Hundreds of complaints were to be addressed by the Italian SA, regarding Italian citizens who had received unsolicited calls made on behalf of EE, found it difficult to exercise their data protection rights, or more generally complained various issues related to the handling of their data in connection with the supply of utility services, including the processing of data performed on the dedicated area in the company's website and/or through the app released to manage power consumptions.

This act of enforcement marked an important take of the Authority, observing the dramatic rise of telemarketing issues in the utilities sector linked with the upcoming switch to the unregulated market regime for electricity and gas suppliers, who compete to get clients.

In effect, the investigations carried out in response to the above complaints showed 'pervasive, unrelenting as well as increasingly invasive reliance on unsolicited promotional calls without the required consent, addressed to off-directory users or to users listed in the opt-out register; additionally, the feedback to users requests to access their personal data or to object to processing for marketing purposes is increasingly delayed or is missing altogether'¹ which led to the following enforcement measures:

- a Euro 25,513,977 fine
- the order to implement appropriate organizational and technical measures to ensure the respect of the GDPR, also with specific regard to (i) marketing and promotional schemes involving actions within EE sales network based on calls admitted by the Register of Communications

¹ Garante per la Protezione dei dati personali, Press Release, 'Aggressive telemarketing: Italian SA fines Enel Energia EUR 26.5 millions. Consumers' data were used without their consent and the accountability principle was not complied with' < <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9737661> > accessed 27 May 2022.

Operators² and (ii) the handling of data subjects' requests to exercise their rights.

At the core of this impressive decision lies the heavy blame on a big market player such as EE for not having seriously taken and honoured the principle of accountability set forth by the combined provisions of art. 5, par.2 and 24, GDPR.

As it results from the explanations given by the Authority for its enforcement provisions, the accountability required from a big player of the market towards the data subjects/consumers is at the highest level, based on the consideration that such accountability, as supported by various GDPR provisions, shall consist in the legal obligation of being constantly aware of the respect of the fundamental rights of natural persons due to data subject/consumers in relation to the processing of personal data, where such legal obligation results out of the combination of the accountability and other GDPR provisions and principles.

1. The complaints.

The decision was issued following complex inquiries the SA had started to clarify the circumstances which originated hundreds of complaints against the conducts synthetised here below.

Several complaints regarded the circumstance of receiving unsolicited calls made for telemarketing purposes on behalf of EE. Within such complaints, some of the calls were:

- received on telephone numbers not shown in public directories and without the consent of the data subject;
- received on telephone numbers shown in public directories but contained in the Public Opt-Out Register in order to block promotional calls³;

² The Italian Communications Regulatory Authority (AGCOM) was established by Law, 31 July 1997, no. 249. With Deliberation, 26.11.2008, no. 666, AGCOM adopted the Regulation for organizing and maintaining the Registry of Communications Operators (ROC), as further integrated by Deliberation, 25.11.2010, no. 608/10/CONS. The so called 2017 Italian budget law (Law, 11.12.2016, no. 232), amending Article 24-bis, Decree Law 22.06.2012, no. 83, provided, among others, that all economic operators carrying out call centres activities using Italian phone numbers must enroll with the ROC, and disclose AGCOM all the telephone numbers made available to the public for call centres activities.

³ The combined provisions of Article 6, paragraph 1, GDPR and Article 130, Italian Personal Data Protection Code (Legislative Decree, 30.06.2003, no. 196) require that the use of automated calling systems without human intervention for the purposes of direct marketing or sending advertising material, or else, for carrying out market surveys or interactive business communication shall only be allowed with the subscriber's consent. The same provisions also apply to electronic communications performed by e-mail, facsimile, MMS or SMS-type messages or other means for purposes referred to therein. Except as provided above, further communications for the same purposes, as performed by different means, shall be allowed in pursuance of Articles 6 and 7, GDPR as well as under the further terms set forth by Article 130, comma 3-bis, Italian Personal Data Protection Code. This latter provides that processing by telephone and mail of the personal data as contained in publicly available paper or electronic directories shall only be allowed in respect of any entities that have non exercised their right to object, via simplified mechanisms including the use of electronic networks, by entering such data in a public opt out register (Public Opt Out Register). With Presidential Decree, 07.09.2010, no. 178, the public register of contractors opting out of the use of their personal data and telephone number for sales or commercial promotions was established, along with the provisions to manage it. Consequently, the operator who intends to carry out advertising campaigns by telephone must consult the Public Opt Out Register and respect the data subject's choice for opting out. Recently, the Italian Legislator further dealt with such register, by issuing the Presidential Decree,

- performed through pre-recorded messages.

The complaints about receiving marketing messages and being profiled without the due explicit consent of the data subject were lodged by several citizens in connection with the access and use of online and app services made available by EE to facilitate the monitoring of the contractual relationship and the payments of the bills.

In some cases, the data subjects complained about having unsuccessfully requested EE to exercise their rights to (i) object the processing of their numbers for marketing purposes and (ii) request the erasure of personal data when no longer needed from the controller.

2. EE's defense.

EE's first and primary defense consisted in affirming that the above calls had not been made or authorised by EE: they had been carried out by third parties, unlawfully using EE's name and/or operating unbeknownst to EE⁴.

EE affirmed this even if the promotional calls had been made, in effects, to the advantage of EE: the calls were actually aimed at inviting the data subjects to subscribe an electric and gas contract with EE. In some cases, the goal of the call was to propose a visit by the commercial partner of EE.

In many cases EE was not able to provide the Authority with the information and documentation requested.

As to the complaints about the unsuccessful exercise of the right of the data subject based on GDPR, EE pointed out that it faced problems to respond precisely because it was overwhelmed by such requests, not caused by EE itself.

With specific regard to the data of subjects who complained about unsolicited calls performed through pre-recorded messages, EE disclosed it had collected such data directly or through some commercial partners, based on previous activities, such as handling preceding requests to exercise the rights of the data subjects or monitoring the client appreciation.

Finally, in respect to the complaint about receiving marketing messages or being profiled in connection with the access and use of the online and app services made available by EE without explicit consent of the data subject, EE disclosed that, in order to simplify such facilities, a so called 'Single Profile' (Profilo Unico) had been implemented, consisting in one single account for each

27.01.2022, no. 26, Regulation laying down provisions on the establishment and operations of the public register of contractors who opt out of the use of their personal data and their telephone number for sales or commercial promotions, pursuant to Article 1, comma 13, Law 11.01.2018, no. 5. In particular, it is now provided that the Public Opt Out Register is extended to all national telephone numbers, both landline and mobile, allowing the citizens to opt out both of unsolicited telemarketing calls, also by revoking consent to advertising, and of the transfer to third parties of previously provided personal data.

⁴ This specific defense is completely similar to other ones adopted in analogous cases regarding other big energetic and communication market players, also sanctioned by the Italian SA. In this respect, see, among others, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9570997> Autorità Garante per la Privacy, Ordinanza ingiunzione nei confronti di Fastweb, Doc. web Nr. 9570997. In particular, during the investigation at hand, as well as in other similar ones, it has emerged the use of telephone numbers either fictitious or not entered into the ROC by such big market players, to carry out telemarketing activities. As pointed out by the Italian SA in the above mentioned ordinance against FASTWEB, it seemed to be dealing with a sort of undergrowth of abusive call centers which carried out telemarketing activities in total contempt of the provisions set forth by the GDPR and the Italian Personal Data Protection Code.

customer, allowing to access not only all ENEL web portals, but also any app of ENEL Group companies. In order to complete the profile and get the above accesses, the user was only requested to confirm the information provided by the data controller, without being required to express consent to the aim of receiving promotional communications and getting profiled. Basically, by creating a single username and password, it was possible for each customer to access any digital service provided within the ENEL Group, without a new registration being needed to enter into a new web portal, especially in case the new portal was provided by a different company.

EE asserted that within the ENEL Group only the Single Profile, i.e., the single Username and Password was shared, and that the personal data of the customer were not being communicated by the relevant company (which has the direct contractual relationship with the customer) to the other entities of the Group.

In particular this issue, combined with the lack, for the Authority, of proper evidence and information regarding the manner of collecting, storing and using the consent for marketing and profiling purposes by EE, led to the decision of the Authority to directly carry out a specific inspection. In this way the Italian SA found out that the registration process to create the Single Profile of the customer only allowed in a separate and successive step to express or reject the consent to marketing and profiling purposes, both for EE and other companies within the ENEL Group, in a confusing and not 'user-friendly' manner.

3. The Italian SA allegations.

At the end of its complex and articulated investigation activities, the Italian SA notified EE the 15 infringements to the GDPR provisions synthetised below

1. Art. 31, GDPR (Cooperation with the Supervisory Authority), for not having provided the Authority with a relevant amount of the information and documentation requested especially regarding the possible communication of personal data to third parties, while limiting itself to insisting that most of the complaints referred to processing of personal data not carried out by EE⁵.

2. Art 5, par. 2, combined with Art. 25, par. 1, GDPR (Accountability and Privacy by Design), for not having adopted effective countermeasures even when the huge dimension of unlawful use of personal data of EE's customers had been made manifest to EE itself⁶. In the view of the Italian SA, in such

⁵ Recital 82, GDPR makes clear the close relationship between the accountability principle and the provision set forth by Article 31, GDPR, which imposes both the controller and the processor to cooperate on request with the supervisory authority in the performance of its tasks: 'in order to demonstrate compliance with this Regulation, the controller and the processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations'.

⁶ Recital 74, GDPR underlines the importance, for both the controller and the processor, of being constantly able to demonstrate that the measures adopted are not only appropriate but also effective throughout the life of specific processing of personal data: 'the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures'.

circumstances EE should have exercised (and been able to demonstrate) - in a complete and exhaustively aware manner - its legal obligations of accountability and Privacy by design, by adopting proper measures (characterized by the inclusion of elements of prevention, functionality, safeguard, transparency) to protect the data subjects. In facts, precisely the circumstance that the calls were made using EE's name should have caused proper actions for constant supervision and monitoring of the complained phenomena, taking into account the primary role of the ENEL Group in the energy market and its significant possibilities to adopt organizational and managing measures.

In this regard, EE showed no evidence of having adopted any of such measures not even towards its commercial partners, while such measures should have been adopted based on the legal obligation of accountability and privacy by design. EE should have evidenced specific measures to automatically control the means used and/or shared by EE's personnel and further commercial partners/members of EE's sales network to activate promotional campaigns or services towards EE's customers. For instance, a proper organization and scheduling of such promotional campaign could have been considered and implemented, including the design of the relevant actions to ensure that, by default, in real time, attempts to upload on the EE's digital platform contracts not evidencing the requirements of correctness and transparency or manifestly infringing GDPR provisions could be detected and blocked.

The Italian SA further questioned that EE neither did evidence the criteria and requirements defined for proper selection of commercial partners, nor the audit activities to be made from time to time to the aim of assessing the maintenance of such requirements, including automatic means to control the processing of personal data. This also with regard to both the continuous safeguard of the access to the personal data of the customers, and the constant monitoring that only correct contracts as mentioned above are uploaded on platforms withing ENEL Group.

The general comment of the Authority on this issue is that measures of the kind suggested above, if adopted, could have put EE in condition to correctly demonstrate the awareness of the company (even in terms of proper actions taken by its governance board) at the time when such circumstances emerged that could undermine and compromise not only the rights of the customers, but also the reputation of the Group.

3. Art.5, par., 2, GDPR (accountability), for not being able to demonstrate the compliance with the principles relating to processing personal data, with specific regard to unsolicited promotional communications made by a commercial partner.

A major role in this allegation is played by the lack of evidence of whatsoever action taken by EE towards its commercial partners, after EE had been made aware about the existence of complaints regarding unsolicited communications⁷.

⁷ Already in the so called Fastweb ordinance (see above, note no. 5) the Italian SA raised the theme of the control of the whole chain of the effective partners regarded by marketing activities on behalf of the data controller. In facts, FASTWEB was sanctioned for not having implemented proper measures to control and

4. Art. 5 par. 2 and 24, GDPR (accountability and responsibility of controller), for not having monitored the activity of commercial partners, and not having adopted proper organizational and technical measures, with respect to the calls made to the advantage of EE even if not carried out by EE's personnel⁸.

5. Art. 5, par.1, lit. d), GDPR (principle of accuracy), for having erroneously, and in an automatic manner, associated to the contact data of a customer the telephone number dialed by such customer at the time when he contacted the free line exclusively dedicated to the customer service.

6. Art. 5, par. 1, lit. d), and 6 GDPR (principle of accuracy and lawfulness of processing) for having transmitted the personal data of a customer to another one, based on an incorrect association of such data (the data was simply similar to one another).

7. Art. 12, GDPR (transparency and modalities for the exercise of the rights of the data subject), for not having responded in a timely manner to the requests of the customers to exercise their right to access the data processed by EE and to object the use of their data for marketing and/or profiling purposes.

8. Art. 5, par. 1, lett. a) and 12, par. 2, GDPR (principle of Accuracy and transparency) for having given an inconsistent response to the Authority with regard to the request of a customer to exercise the right to object the receiving of promotional calls performed through pre-recorded messages, by affirming both (in the answer given to the customer) that there effectively was an erroneous contact on the EE side, and (in the documentation given to the Italian SA for the defense in this proceeding) that another customer was to blame for such error, i.e. the other customer declared to EE the data of another person when subscribing a new energy contract.

9. Art. 21, GDPR and art. 130, comma 1 and 2, D. Lgs. 196/2003 (unsolicited communications and the right to object), for having unduly sent unsolicited communication via e-mail, notwithstanding the explicit denial expressed by the customer at the time when the energy contract was subscribed and a further communication (properly executed) to EE about the right to object such processing of data.

10. Art. 130, comma 4, D. Lgs. 196/2003 (soft spam) for having sent to a customer the notification of the registration to a fidelity program, without having any evidence of the previous proper information given to the customer.

11. Art. 31 (cooperation with the Supervisory Authority), for not having provided the Authority with the information and documentation requested twice regarding the manner to obtain consent for marketing and profiling purposes within the digital facilities made available to the customers.

12. Art. 5, par 1, lett. a), 12 and 13, GDPR (principle of transparency and obligation of providing information as to where personal data is collected from

not being able to clearly represent the whole chain effectively used to collect personal data for marketing purposes, with the result that the data controller was not in condition to demonstrate that the processing of personal data were performed in accordance with GDPR from the first contact. A similar position of the Italian SA can be found also in another recent ordinance against Iren Mercato Spa. See <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9670025> Autorità Garante per Privacy, Ordinanza ingiunzione nei confronti di Iren Mercato S.p.A., Doc web Nr. 9670025.

the data subject) for having shown on the same website two information pages inconsistent with one another, with specific regard to the identity of data controller (it resulted unclear whether the data controller was EE or Enel Italia SpA).

13. Art. 5, par. 1, lett. c), GDPR (principle of minimisation), for having designed a procedure for processing personal data on the web portals of Enel Group companies, which consented the transmission to other companies of the Group of data which is not adequate, relevant and necessary. In facts, the above-described Single Profile, allowed the customer to access the digital service of several companies of the Group and, in turn, allowed the companies included in this portal network to share the data of the customer. Furthermore, in order to avail himself of the services provided by the web portal and applications of the Group, the customer was conditioned to give more data than necessary.

14. Art. 12 and 13, GDPR (Transparency and information to the data subject) for having released poor information about the activation of the Single Profile and, in particular, the consequent possibility of other companies of the Group and other commercial partners to be recipients of the personal data submitted with the Single Profile.

15. Art. 6, par.1, GDPR and 130, comma 1 and 2 (Lawfulness of processing and unsolicited communication) for not having acquired specific and proper consent with regard to the specific processing activities performed by several, distinct data controllers.

4. The accountability principle as a legal obligation of the data controller to be constantly aware.

Following the description of the above infringements, and the defense of EE, the Italian Authority further exposed its considerations in facts and in law.

Such considerations point out that the accountability of the data controller include the legal obligation to be constantly aware of its legal obligations of accountability and privacy by design as existing from time to time, so that, while some assessments of the supervisory authority are to be made necessarily *ex-ante* (taking into account the possibility of the data controller to design, adopt and maintain organisational and technical measures adequate to protect the data subject as required by the GDPR at the time of the design of the processing data structure), other evaluations of the Authority shall take into account (i) the possibility of reaction and response of the data controller in case anomalies or complaints of data subject arise, and (ii) the capacity of the data controller to constantly be aware of its compliance to the provisions protecting the data subject.

Furthermore, the dimensions and the relevance of the data controller as a market player shall have a specific impact on the assessment of the supervisory authority both requirements that are to be met *ex-ante*, and the ones which are to be valued *ex-post*, particularly in terms of the ability to react and correct anomalies and non-compliance cases which may emerge from time to time during the economic life of the data controller.

Here below are exposed the concepts articulated by the Italian Authority in such meaning.

The principal theme used by EE for defense was that most of the unsolicited communications received by the complaining data subjects were not made by EE itself.

In this regard, the Authority explained that Articles 5, par.2, 24 and 25, par. 2, GDPR, outline a precise frame of accountability of the data controller, which imposes not only that proper measures are adopted to guarantee the respect of the principle governing the processing of personal data as required by GDPR, but also that the controller is able, at any time, to demonstrate with proper evidence the compliance to the GDPR of its processing activities.

To this aim it is necessary for the data controller to give evidence also of the preliminary evaluation made on the handling of data concretely carried out in its economic life, together with proper evidence of the evaluation of the risks as well, and the effectiveness of the measures adopted.

Within this legal frame, the evidence requested to the data controller imposes an adequate selection and monitoring of other parties possibly involved in the handling of personal data made in the interest of the data controller, so that it continues to maintain the accountability of handlings of data made on its behalf or to its advantage, without the possibility to set free from such accountability merely based on the formal affirmation 'It was not me'⁹.

The GDPR accountability principle, articulated both from a legal perspective (art. 5, par. 2 and art. 24, GDPR) and a more modern and technological one (art. 25, GDPR), outgrows, in facts, the merely formalistic compliance logic, by providing that the data controller adopt mechanisms for systematic control, and in the *ex-ante* evaluation of the perimeter of the data processing and its peculiar risks, and in the *ex-post* circumstances as they evolve during the time¹⁰, involving the monitoring and control of the risks deriving from data processing carried out by other entities, acting on behalf of the data controller or, in any case, to its advantage.

In this view, the circumstance that several complaints are lodged by the Italian Authority for unsolicited communications to the advantage of EE should have been an alarm bell for such entity, causing proper reaction to protect the personal data and the fundamental rights of its customers.

Furthermore, the Italian Authority pointed out that the history, the structure and the organisational dimensions of EE should have made possible to this leader player in the energetic market, to adopt advanced organisational measures to protect the personal data of its customers, including proper mechanisms to control the entire chain of controllers and processors of such data involved by the economic activity of EE, if only EE had applied the diligence

⁹ Here again, recital 74 is to be pointed out with specific reference to EU Legislator's position with regard to the 'responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf...'.

¹⁰ In this regard, see also *G BUTTI*, 'Audit e GDPR: competenze e linee guida per svolgere correttamente le verifiche in ambito privacy', 15 October 2019, Cybersecurity 360, <https://www.cybersecurity360.it/legal/privacy-dati-personali/audit-e-gdpr-competenze-e-linee-guida-per-svolgere-correttamente-le-verifiche-in-ambito-privacy/>, accessed 05 September 2022.

due to its dimensions, also considering the volume of its customers (9 millions of customers at the time of the decision).

As a consequence, when facing such an amount of complaints for unsolicited marketing activities, EE should have controlled that the other companies of the Group and commercial partners would not have infringed any of the GDPR provisions.

A mechanism of control should have been designed and adopted from the beginning of the activities of data processing and been maintained along all the activities of the Group which involve the handling of personal data. And EE, as data controller, should have been able to demonstrate with proper evidence to have done so.

To better assess the possibility for EE to adopt proper controls, the Italian Authority points out that, in facts, EE is already organised to validate the energetic contracts, because precisely for the phase of validation of the agreement with the customer, an amount of information is gathered and associated to the single contract, such as: contract code, code of the officer in charge for the contract, channel code, each of them well visible on the application form sent to the customer for subscription and available on EE website. Notwithstanding these links, and, with them, the ability to control the validation phase of the contract based on the traceability of the officers and the channels used to close the agreements, still, EE did not offered any evidence of having made controls to prevent unfair commercial practices, which boils down, for EE, to accept being vulnerable towards the business finders EE should have known and taken into consideration within its sales network.

Also, the lack of measures adopted by EE for the registration to the aim of creating the Single Profile to protect the rights of the data subject as set forth by the GDPR, in the view of the Italian Authority, paves the way for possible unauthorized 'business finders', able to 'grab' the data of the customers who constantly and consistently complained to the Authority unsolicited calls made on behalf of EE.

In previous decisions¹¹ the Italian Authority had already given, in precedent decisions, indication on the need to respect the Privacy by design principle by adopting organisational measures aimed to prevent the contractual activation of contracts in case the conclusion of the agreement is not clearly and unambiguously connected and traceable to activities carried out in the respect of the provisions protecting the rights of the data subjects/consumer from the first contact and acquisition of the data.

The same measures required as above are to be considered requested with regard to the marketing campaigns which admittedly EE launched following the pandemic emergency

Two more issues of this decision are to be mentioned:

a) the responsibility of EE for unlawfully processing of data is not exempted just for the 'good faith' of the controller: the Italian SA explains that the accountability under art. 5, GDPR can achieve exemption only if the

¹¹ See <<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9485681>> Autorità Garante per la Privacy, 'Ordinanza ingiunzione nei confronti di Vodafone, 12 November 2020', Doc. web Nr. 948568, and the ordinance against FASTWEB mentioned above (see note no. 5).

controller is able to demonstrate that the unlawful treatment, even if generated by an error, was inevitable. In this view, the accountability set forth by art. 5, GDPR is similar to the one provided by D. Lgs. 231/01 in the Italian law, imposing that companies must demonstrate that they have effectively adopted compliance programs called 'models of organisation, management and control' (the so called '231 Models') with the aim of identifying, preventing and mitigating the risk of commission of crimes in relation to business activities¹².

b) the absence or delay of proper response to the requests of the data subjects to exercise their rights based on GDPR is not acceptable, so EE's defense is not excusable, because it is just based on the affirmation that the difficulty to respond is due to the huge amount of requests. In facts, once again, this is another critical issue derived by a lack of proper organization of the data controller, who has to adopt proper means to assure the respect of the rights of the data subjects, even introducing corrective measures and penalties within its network in case of violation of the instructions given by the data controller. In this case, it is recalled the logic of the '231 Model' again, which can exempt the company from the accountability in case of noncompliance of certain legal provision only if it is proofed to be effective, that is, it must¹³ a) identify the activities in relation to which offences may be committed; b) provide for specific direct protocols and schedule training and implementation of decisions by the body regarding offences to be prevented; c) identify procedures for managing financial resources which are fit to prevent the commission of offences; d) provide for obligations to disclose information to the organisation tasked with overseeing the working of and compliance with the models; e) introduce a new disciplinary system to punish noncompliance with the measures set out in the model.

The final decision of the Italian SA is based on the appraisal of the organisational model adopted by EE to be compliant to the GDPR. Such organizational model (art. 24, GDPR) should have had at its backbone, the

¹² M IASELLI, *Manuale operativo del D. P. O.* (2nd edn, Maggioli Editore 2021) 10; C SANTORIELLO, 'Il Modello Organizzativo' in M Iaselli and others, *I rapporti tra normativa privacy e modello 231* (Maggioli Editore 2022), 57; R PANETTA, 'Le 5 sfide che attendono il futuro del DPO', in R Panetta, T Mauro, F Sartore, *Il data protection officer tra regole e prassi* (Giuffrè Francis Lefebvre, 2021), 158; M PEREGO, S PERSI, C PONTI, *Il modello organizzativo Privacy – MOP* (1st edn, Giuffrè Francis Lefebvre 2020) 5; D COSTA, 'I modelli 231 e la compliance aziendale sulla tutela dei dati personali. Aspetti comuni e divergenze a quattro anni di distanza dall'entrata in vigore del GDPR' [2020] *Giurisprudenza Penale Web*, nt. 5. <<https://www.giurisprudenzapenale.com/2020/05/01/i-modelli-231-e-la-compliance-aziendale-sulla-tutela-dei-dati-personali-aspetti-comuni-e-divergenze-a-quattro-anni-di-distanza-dallentrata-in-vigore-del-gdpr/>> accessed 16 May 2022; M MAGLIO, P GHINI, 'Privacy, nuovo regolamento Europeo. L'importanza delle misure Organizzative. Punti di contatto con la Normativa 231/2001' (2017) 1 (1) *Rivista231*, 41 ff; V VISICCHIO 'MOG231/01 e GDPR: sue sistemi di compliance a confronto' (2018) Università Cattolica del Sacro Cuore, available at www.rivista231.it; A LAUDATI, 'Le possibili convergenze tra la recente Normativa privacy e il decreto Legislativo 231/2001' (2019) 1(1) *Rivista231*, 11 ff; C MATTEUZZI, A PEDICO, 'The paradigm: Model 231/01 & cybersecurity quality system' [2019] *Diritto di Internet*, <<https://dirittodiinternet.it/wp-content/uploads/2019/11/Versione-inglese.pdf>>, accessed 16 May 2022; A CICCIA MESSINA, 'Modelli organizzativi privacy e 231: differenze e possibili sinergie per le imprese', 19 June 2018, *Quotidiano Ipsoa*, <<https://www.ipsa.it/documents/lavoro-e-previdenza/amministrazione-del-personale/quotidiano/2018/06/19/modelli-organizzativi-privacy-231-differenze-possibili-sinergie-imprese>> accessed 16 May 2022; FEDERPRIVACY Online Workshop, 'Privacy e Dlgs 231/2001', 15 May 2021, with the participation, among others, of A GHIGLIA (member of the Italian SA) – L CARROZZI (official of the Italian SA). <<https://www.federprivacy.org/attivita/modelli-organizzativi-gli-spunti-di-integrazione-tra-dlgs-231-2001-e-gdpr>> accessed 16 May 2022.

¹³ Art. 6, comma 2, D. Lgs. 231/01.

respect of the principle of accountability (art. 5, 2, GDPR) and Privacy by design (art. 25).

The kind of appraisal made by the Authority was aimed to prove, in particular, the effectiveness of such organisational model.

A shift in the cultural approach of the companies is needed, in order to really comprehend what does 'accountability' stands for¹⁴.

Art. 25, paragraph 1, GDPR clearly states that 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects'.

In this regard it is useful to recall a key message of the Article 29 Working Party: 'Fundamental principles applicable to the controllers (i.e. legitimacy, data minimisation, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable.'¹⁵

This key message has been reaffirmed by EDPB, when insisting that effectiveness at any moment is at the heart of the concept data design¹⁶:

'13. Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller. This observation has two consequences.

First, it means that Article 25 does not require the implementation of any specific technical and organizational measures, rather that the chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question. In doing so, the measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk.

¹⁴ In this regard the former European Data Protection Supervisor, Giovanni Buttarelli, was very clear since 2016. See, <https://edps.europa.eu/data-protection/our-work/publications/speeches/accountability-principle-new-gdpr-0_en>, G BUTTARELLI, 'The accountability principle in the new GDPR', Speech at the European Court of Justice, Luxembourg, 30 September 2016.

¹⁵ See, <https://ec.europa.eu/justice/article29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>, Article 29 Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks', adopted on 30 May 2014, Doc. Number 14/EN WP218, page 3, Key Message 4.

¹⁶ See <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf>, 'Addressing effectiveness', EDPB, Guidelines 4 (2019) on Article 25 Data Protection by Design and by Default, Version 2.0.

Second, controllers should be able to demonstrate that the principles have been maintained.

The implemented measures and safeguards should achieve the desired effect in terms of data protection, and the controller should have documentation of the implemented technical and organizational measures... To do so, the controller may determine appropriate key performance indicators (KPI) to demonstrate the effectiveness. A KPI is a measurable value chosen by the controller that demonstrates how effectively the controller achieves their data protection objective. KPIs may be quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or qualitative, such as evaluations of performance, use of grading scales, or expert assessments. Alternatively, to KPIs, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards.'

In the light of the above, after having considered several aggravating circumstances, (the gravity of the infringements, their duration, the number of the data subject involved, the negligence and the specific reiteration of the conducts representing infringements), the Italian SA imposed on EE an Eur 25,513,977 fine.

Additionally, EE was ordered to:

a) bring all processing of data by its sales network into compliance with proper arrangements and measures, in order to become able to demonstrate that promotional schemes and services or contracts are only activated following promotional calls addressed to numbers that are listed in the Opt-Out Public Register and

b) implement further technical and organisational measures in order to correctly handle data subjects' requests to exercise their rights including, in particular, the right to object to processing for promotional purposes, in such a manner that proper response is given to such requests by no later than thirty days after the Italian SA's order.

Conclusions.

In its decision regarding EE, the Italian SA expressly considered the accountability principle under GDPR as a legal obligation, for the data controller, to be constantly (i) aware of the risks involving the data subject and the effectiveness of the countermeasures adopted from time to time, and (ii) able to demonstrate that awareness.

Such an obligation necessarily imposes to the data controller the adoption of an organisational model, based on the concrete risks assessment and the adoption of adequate measures to prevent such risks concretely and effectively. To be effective, the organisational model shall (i) take into consideration the dimensions and possibilities of the data controller, (ii) consequently allocate adequate resources for adoption and constant maintenance of the preventive measures, and (ii) comprehend a disciplinary system (internal or external, in this case through proper arrangements) to

punish violations of the instructions given by the data controller to assure the respect of GDPR.

This position recalls the experience (and the jurisprudence) of D. Lgs. 231/01 in the Italian Law, regarding the responsibility of the companies for certain unlawful conducts.

It is clear that

a) the accountability under GDPR is to be assessed in its necessary combination with the principle of privacy by design set forth in art. 25, GDPR;

b) the assessment of the measures adopted, including their respect of the principle of privacy by design, are aimed at checking their effectiveness, on the basis both of an *ex-ante* evaluation (taking into account the risks and the relating appropriate countermeasures that the data controller could envisage at the moment of designing the GDPR model) and on a '*ex-post*' appraisal of the measures applied at the time of the processing itself;

c) in order to maintain proper awareness along the time, and the ability to demonstrate it, the data controller has to adopt adequate and, when possible, automatic mechanisms of control, which should include Key Performance Indicators;

d) the KPI to be adopted in order to constantly monitor and collect evidence of the effectiveness of the 'privacy organisational model', should necessarily include (i) the formalised detection of anomalies or incorrect conducts based on complaints or even just consistent requests of the data subjects to exercise their rights (setting what circumstances are to be held as an 'alarm bell'), (ii) adequate keys to monitor the providers of services who could be involved in the data processing activities of the data controller;

e) the data controller, when designing its GDPR model, shall be aware of all the providers of services or other parties involved in its economic sphere of action who could have access to personal data. Therefore, all the risks carried with the involvement of such parties shall be correctly mapped, the map of the risks shall be maintained updated, and proper countermeasures shall be set forth and maintained updated, too;

f) the model should provide proper sanctions in case of infringement of the instructions given by the data controller (i.e., with adequate termination and penalty clauses in the relevant agreements with external parties or, also, disciplinary sanctions in case of personnel);

g) the GDPR model should also include automatic mechanisms aimed at correcting the adopted countermeasures, whenever anomalies or incorrect actions are detected, with proper evidence of the detection system and the corrective measures adopted.

JEREMY A. ANTIPPAS – Professor of Law, University of South Brittany.

LIVIA AULINO – Research Fellow, Università degli Studi di Napoli Federico II.

ILARIA AMELIA CAGGIANO – Full Professor of Private Law, Università degli Studi Suor Orsola Benincasa, EJPLT Vice-Director.

MARIA GIORGIA CARACENI – Research Fellow of Fondazione Magna Carta of Rome
Doctor in Philosophy of Law.

ROBERTO CARLEO – Full Professor of Private Law, Università degli Studi di Napoli Parthenope.

MARIA ANTONIA CIOCIA – Full Professor of Private Law at Università degli Studi della Campania Luigi Vanvitelli.

GIOVANNA D'ALFONSO – Associate Professor of Private Law, Università degli Studi della Campania Luigi Vanvitelli.

DAVIDE SILVIO D'ALOIA – Ph. D. (c) in *Humanities and Technologies: an integrated research path* at Università degli Studi Suor Orsola Benincasa.

CARLOTTA DE MENECH – Senior Researcher in Private Law, Pavia University.

ALESSIO DI AMATO – Full Professor of Business Law at University of Salerno.

MARIA CRISTINA GAETA – Lecturer in Private Law at Università degli Studi Suor Orsola Benincasa, EJPLT Editorial Board Coordinator.

LUCILLA GATT – Full professor of Private Law, Università degli Studi Suor Orsola Benincasa, EJPL Editor in Chief.

IVANA GENESTRONE – Lawyer of the Lucca Bar Association.

SERGIO GUIDA – Independent Scholar, Data Gov. & Privacy(Sr Mgr), eHealth, Behavioral AI.

LUIGI IZZO – Ph.D. (c) in *Humanities and Technologies: an integrated research path* at Università degli Studi Suor Orsola Benincasa.

UGO MATTEIS - Full Professor of Private Law at Università di Torino, Emeritus Professor at University of California

MARIANA MERIANI – Ph.D. in law at Bocconi University.

ANNA ANITA MOLLO – Postdoctoral Research Fellow, Scuola Superiore Meridionale.

VINCENZO ORSINI – Postdoctoral Researcher of Business Law, University of Salerno.

DIANORA POLETTI – Judge of the Supreme Court of Cassation, Formerly Full Professor of Private Law at Università di Pisa.

FEDERICO SERGIO – Ph.D. (c) in *Humanities and Technologies: an integrated research path* at Università degli studi Suor Orsola Benincasa.

REMO TREZZA – Ph.D. in Civil Law and Contract Professor of Private law, Università degli Studi di Salerno.

EMILIANO TROISI – Ph.D. (c.) in *Humanities and technologies: an integrated research path*, Università degli Studi Suor Orsola Benincasa di Napoli.

CHIARA VITAGLIANO – Ph.D. (c) Università degli Studi di Napoli l'Orientale.