medialaws

Rivista di diritto dei media
2/2021 luglio

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

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

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

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

SEDE
CONTACTS

ACCMS Studio Legale
Via Podgora 13 – 20122 Milano

Università Bocconi - Dipartimento di Studi Giuridici
Via Roentgen 1 - 20136 Milano

e-mail: submissions@medialaws.eu

COMITATO SCIENTIFICO- STEERING COMMITTEE

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

COMITATO DEGLI ESPERTI PER LA VALUTAZIONE - ADVISORY BOARD

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

ANNO 2021 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Indice
Index

Saggi

9 **Costituzionalismo, privacy e neurodiritti**
Oreste Pollicino

18 **Norme sulle firme elettroniche a confronto: UE, Italia e Cina**
Giusella Finocchiaro, Hu Guiping

44 **La difesa della democrazia pluralista dinanzi alla paura e alla disinformazione**
Juan Francisco Sánchez Barrilao

67 **Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione**
Marco Bassini

100 **Il ruolo delle reti sociali nel contrasto ai reati commessi all'interno del web. Tendenze evolutive e prospettive di sviluppo**
Sofia Braschi

113 **Diversity of exposure in social media markets: regulating or unbundling content curation**
Maria Luisa Stasi

141 **Siamo tutti giornalisti? Appunti sulla libertà di informazione nell'era social**
Alessandro Lauro

165 **The commodification of our digital identity: limits on monetizing personal data in the European context**
Milena Mursia, Carmine Andrea Trovato

190 **La necessaria applicazione dei principi di *data protection* al diritto di accesso dei consiglieri *ex* art. 43, c. 2, TUEL**
Valentina De Nicola

222 **Quando il datore di lavoro diviene un algoritmo: la trasformazione del potere del datore di lavoro in algocrazia. Quale spazio per l'applicazione dei principi costituzionali?**
Camilla Della Giustina

Note a sentenza

239 **The CJEU's take on unauthorized framing of online content: (only) if technologically precluded, then prohibited**
Giulia Priora

247 **La responsabilità del gestore del sito per i contenuti pubblicati da soggetti terzi**
Silvia Vimercati

252 **Esposto a un ordine professionale: quali confini per il diritto di critica**
Laura Ninni

259 **Consenso, intelligenza artificiale e privacy**
Federica Paolucci

266 **Il diritto di accesso ai dati personali contenuti nello smartphone di una persona deceduta e conservati in cloud**
Valerio Natale

278 **Responsabilità del social network per chiusura immotivata dell'account con distruzione dei dati ivi presenti. Sul rapporto giuridico utente/piattaforma: tra protezione e commercializzazione dei dati personali**
Lorenzo Albertini

Recensioni

295 **"La despazializzazione della giustizia" Un viaggio critico nella fenomenologia del presente**
Benedetta Cappiello

303 **Recensione a Gianpaolo Maria Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Cacucci Editore, Bari, 2021, Collana di Studi sull'integrazione europea**
Giovanna Naddeo

Indice
Index

Essays

9 Constitutionalism, privacy and neuro-rights
Oreste Pollicino

18 Comparative Studies of Laws on Electronic Signatures: EU, Italy And China
Giusella Finocchiaro, Hu Guiping

44 The defense of pluralist democracy in the face of fear and disinformation
Juan Francisco Sánchez Barrilao

67 Freedom of expression and social networks: new public fora and private powers
Marco Bassini

100 The role of social networks in tackling cybercrime
Sofia Braschi

113 Diversity of exposure in social media markets: regulating or unbundling content curation
Maria Luisa Stasi

141 Are we all journalists? Notes on freedom of the media in the social era
Alessandro Lauro

165 The commodification of our digital identity: limits on monetizing personal data in the European context
Milena Mursia, Carmine Andrea Trovato

190 Application of data protection principles to the councillors' right to access in accordance with art. 43, para. 2, of the Italian Code on Sub-State Authorities (TUEL)
Valentina De Nicola

222 When the employer becomes an algorithm: the transformation of the employer's power into algocracy. What scope for the application of constitutional principles?
Camilla Della Giustina

Notes and comments

239 The CJEU's take on unauthorized framing of online content: (only) if technologically precluded, then prohibited
Giulia Priora

247 The website owner's liability for third party comments
Silvia Vimercati

252 Report to a professional association: boundaries of the right to criticize
Laura Ninni

259 Consent, Artificial Intelligence and data protection
Federica Paolucci

266 The right to access personal data contained in a deceased person's smartphone and stored in cloud
Valerio Natale

278 Liability of social networks for unjustified removal of the account with destruction of the relevant data. On the legal relationship user/platform: between protection and commercialization of personal data
Lorenzo Albertini

Book reviews

295 Review to A. Garapon, "La despazializzazione della giustizia"
Benedetta Cappiello

303 Review to Gianpaolo Maria Ruotolo, *Scritti di diritto internazionale ed europeo dei dati,* Cacucci Editore, Bari, 2021, Collana di Studi sull'integrazione europea
Giovanna Naddeo

Su determinazione della direzione, in conformità al regolamento della Rivista, sono stati sottoposti a referaggio anonimo, come indicato in calce a ciascun contributo, i saggi di: Oreste Pollicino, Giusella Finocchiaro-Hu Guiping, Juan Francisco Sánchez Barrilao, Marco Bassini, Sofia Braschi, Maria Luisa Stasi, Alessandro Lauro, Milena Mursia-Carmine Andrea Trovato, Valentina De Nicola e Camilla Della Giustina.

Saggi

Costituzionalismo, privacy e neurodiritti*

Oreste Pollicino

Abstract

Il saggio si propone di esaminare, da una prospettiva comparata e di diritto costituzionale, il complesso tema della tutela di una nuova dimensione, quella dei c.d. neurodiritti, nell'alveo delle consolidate categorie a protezione del diritto alla privacy, già sottoposte a importanti sollecitazioni dall'avvento delle tecnologie digitali.

The paper aims to explore, from a constitutional and comparative law standpoint, the problem of protecting the so called 'neuro-rights' by resorting to the well-established legal categories and concepts in the domain of privacy and data protection.

Sommario

1. Introduzione. – 2. La *rule of law* come terreno comune. – 3. La tutela della privacy attraverso l'Atlantico. – 4. Una visione di carattere costituzionale

Keywords

neurodiritti – privacy – protezione dei dati personali – identità personale - costituzionalismo digitale

1. Introduzione

Il tema che qui si affronta oggi è di fondamentale importanza nell'era dei *big data*[1]. Queste tecniche di trattamento dei dati (anche personali) tendono, per definizione, a emanciparsi dalla questione legata alle singole identità. Come anche osservato da Shoshana Zuboff nel suo libro "Il capitalismo della sorveglianza", tale emancipazione avviene al di fuori del concetto di identità personale[2]. Di conseguenza, la tutela dei

* Relazione al convegno organizzato dal Garante per la Protezione dei Dati Personali "Privacy e neurodiritti: la persona al tempo delle neuroscienze", tenutosi il 28 gennaio 2021. Gli atti del convegno saranno prossimamente oggetto di pubblicazione da parte del Garante.
Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

[1] G. De Gregorio - R. Torino, *Privacy, tutela dei dati personali e Big Data*, in E. Tosi (a cura di), *Privacy Digitale,* Milano, 2019, 447 ss.; G. Della Morte, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018.

[2] S. Zuboff, *Il capitalismo della sorveglianza*, Roma, 2019.

dati personali, come poi tradotta nel regolamento (UE) 679/2016, anche noto come GDPR, viene posta all'angolo perdendo in parte quella capacità di assicurare forme di tutela che derivano dalla matrice personalistica del costituzionalismo europeo. Una matrice che è croce e delizia.
La domanda per il giurista è quale sentinella notturna può opporsi a quell'intrusione del "ladro nella notte" prima evocato dal prof. Marramao. E la risposta non può che essere biunivoca, perché il dilemma che si deve affrontare è quello relativo alla elaborazione di nuovi diritti per nuove istanze di tutela o, invece, alla possibilità che i cataloghi dei diritti preesistenti siano in grado invece di fornire una tutela effettiva a queste nuove istanze.
Non si tratta di una questione formale né nominalistica, ma di una portata sostanziale che è relativa al tema cruciale dell'effettività della tutela dei diritti in gioco nell'era digitale. In particolare, il rischio è quello della possibile inflazione dei diritti, perché non è neutrale aggiungere un nuovo o nuovi diritti al catalogo. Tale inflazione, amplificando la conflittualità potenziale tra i diversi diritti in gioco, potrebbe portare non ad un avanzamento della tutela, ma addirittura a una diminuzione della stessa.
Da questo punto di vista, un'altra questione interessante proviene dalle riflessioni precedenti di Marcello Ienca, che osserva come diverse sfide assai istruttive ai nostri fini si erano già poste per la prima volta all'indomani della diffusione della dimensione digitale. Rispetto a quelle lezioni, le questioni legate al rapporto tra costituzionalismo, privacy e neurodiritti vanno valutate con le sensibilità e con le caratteristiche tipiche dei due modelli costituzionali a confronto in prospettiva transatlantica, cioè quello europeo e quello statunitense.

2. La *rule of law* come terreno comune

Prima di focalizzarsi su queste due sponde, sembra opportuno sottolineare un primo terreno comune, in particolare, quello legato alla *rule of law*, allo stato di diritto[3]. Sul punto è possibile citare un passaggio di un articolo del Presidente della Corte europea dei diritti dell'uomo, Robert Spano, recentemente pubblicato sull'European Law Journal: «Io direi che alla base della *rule of law* vi è il rispetto dell'autonomia personale e l'esclusione dell'arbitrio da parte dei governi e dei poteri, sia pubblici che privati»[4]. Da questo emerge che il concetto dell'autonomia personale è il terreno di incontro tra le due sponde.
In un contesto sempre più digitale, il principio di *rule of law* è sotto pressione[5]. Lo sviluppo di nuovi metodi di trattamento dei dati personali che si traduce nella creazione di profili predittivi è solo un esempio di come valori e principi costituzionali

[3] M. Krygier, *The Rule of Law: Legality, Teleology, Sociology*, in G. Palombella - N. Walker (a cura di), *Relocating the Rule of Law*, Oxford, 2009, 45 ss.; J. Waldron, *The Concept and the Rule of Law*, in *Georgia Law Review*, 43(1), 2008, 1 ss.

[4] R. Spano, *The rule of law as the lodestar of the European Convention on Human Rights: The Strasbourg Court and the independence of the judiciary*, in *European Law Journal*, 2021.

[5] O. Pollicino - G. De Gregorio, *Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics*, IACL Democracy Roundtable, 2020.

vengono percepiti, interpretati e modellati nella c.d. società dell'informazione[6]. Lo stato di diritto non è stato risparmiato in questo processo di inquadratura delle categorie tradizionali alla luce delle dinamiche tecnologiche. La tecnologia costituisce infatti anche un'opportunità per promuovere il principio della *rule of law*, poiché può fornire migliori sistemi di applicazione delle politiche pubbliche nonché un chiaro e un quadro affidabile che compensi le inefficienze che di fatto minano la certezza del diritto.
In questo quadro tra innovazione e rischio, la domanda da porsi è se le tecnologie digitali incoraggino l'esercizio di poteri arbitrari che possano comprimere quell'autonomia personale alla base dello stato di diritto. Il rispetto di tale principio è una precondizione per garantire la parità di trattamento davanti alla legge, tutelando i diritti fondamentali, prevenire l'abuso di potere da parte delle autorità pubbliche e ritenere responsabili gli organi decisionali. Pertanto, il principio di *rule of law* è un baluardo costituzionale che limita l'esercizio delle autorità al di fuori di qualsiasi limite costituzionale e garantisce che questi limiti rispondano a uno schema costituzionale comune. Nella società dell'informazione, questo principio è una garanzia primaria per garantire che, quando gli attori pubblici utilizzano tecnologie digitali, ad esempio, per fornire servizi più efficienti o migliorare lo svolgimento di compiti pubblici, l'esercizio di queste attività non sia discrezionale, ma basato su regole chiare e proporzionate. Allo stesso tempo, la mancanza di esperienza delle autorità pubbliche e il consolidamento dei *gatekeeper online* hanno spinto il settore pubblico a fare sempre più affidamento su attori privati per garantire l'applicazione delle politiche pubbliche online[7]. La pandemia non solo ha amplificato le sfide tecnologiche come nel caso del tracciamento dei contatti, ma ha anche mostrato il ruolo degli attori privati nell'agire come *digital utilities*. Facebook, Amazon e Zoom sono solo tre esempi di attori che hanno permesso lo svolgimento di attività quotidiane durante la pandemia.
Tuttavia, in mancanza di regolamentazione o applicazione orizzontale dei valori costituzionali, il principio dello stato di diritto non limita la libertà di cui godono gli enti privati nello svolgimento delle loro attività, compreso il diritto alla libertà di espressione o alla libertà economica. In un ambiente digitale globale, le minacce per il principio dello stato di diritto non provengono solo dall'attuazione di tecnologie digitali da parte di attori pubblici, ma anche, e principalmente, dalla capacità degli attori privati transnazionali di sviluppare e applicare standard privati in concorrenza con valori pubblici. Detto questo, è evidente che la questione si pone in maniera diversa negli Stati Uniti e in Europa, perché la dimensione sacrale del Primo Emendamento della Costituzione americana chiaramente caratterizza dal punto di vista assiologico il dibattito transatlantico. Secondo la visione statunitense, la libertà di espressione è interpretata come *cognitive freedom* e protetta (quasi) a livello assoluto. Questo approccio nasconde un grande rischio di partire dal presupposto sbagliato per cui il pensiero sarebbe "invincibile" fin quanto resta tale e soltanto quando questo viene estrinsecato allora meriterebbe di

[6] A. Simoncini, *L'algoritmo incostituzionale. intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, 63 ss.

[7] J. R. Reidenberg, *States and Internet Enforcement*, in *U. Ottawa L. & Tech. J.*, 1, 2003, 213 ss.; M. D. Birnhack - N. Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, in *Virginia Journal of Law & Technology*, 8, 2003, 1 ss.

essere anche tutelato. Si tratta di un presupposto sbagliato, per l'appunto.
L'anticipazione della tutela è quindi fondamentale in questo contesto. Come affermato dal Presidente dell'Autorità Garante, il professor Pasquale Stanzione, presto la tutela delle nostre libertà fondamentali potrebbe richiedere non solo un *habeas corpus* (il fondamento dello stato di diritto) e un *habeas data* (fondamento della nozione moderna di privacy) ma anche un *habeas mentem* a fondamento delle libertà individuali e dei diritti della persona in un mondo in cui sfumano i confini tra uomini e macchine.
La buona notizia è che le fondamenta giuridiche dei neurodiritti potrebbero essere già presenti (quasi profeticamente) nelle Carte esistenti. Certo, una prima lettura di tali Carte, accompagnata da un'interpretazione letterale, potrebbe farci pensare al contrario. Il riferimento alla tutela è quasi sempre collegato al momento dell'espressione del pensiero. Il che potrebbe fare presumere, e sarebbe una presunzione errata, che il pensiero in sé, inespresso, avrebbe uno scudo di invincibilità, e quindi non necessiterebbe di tutela costituzionale. Si tratterebbe di una lettura errata che decontestualizza il testo (costituzionale) dal contesto sia storico che tecnologico.
Risulta evidente, infatti, che i *framers* delle carte di prima, seconda e terza generazione non potessero prevedere espressamente ciò che era tecnologicamente imprevedibile. Vale a dire, come si è cercato di fare emergere prima, anche il pensiero non espresso né sussurrato può rappresentare uno spazio potenzialmente a repentaglio e quindi bisognoso di una protezione di carattere costituzionale. Il fatto, tuttavia, di non avere previsto espressamente detta protezione non vuol dire che sia esclusa. Al contrario, una interpretazione evolutiva e tecnologicamente orientata del giudice, non solo costituzionale, sembra in grado, sin da subito, di garantire una tutela effettiva all'*habeas mentem*. Anche perché, come già sottolineato, nuove Carte, e nuovi diritti, non portano per forza di cose ad un innalzamento della tutela dei valori al gioco. Al contrario, l'inflazione dei diritti non può che portare al conflitto e quindi all'effetto esattamente contrario.

3. La tutela della privacy attraverso l'Atlantico

Già a proposito di tecnologie non di carattere neurale ci sono stati degli insegnamenti e delle lezioni da trarre. Brandeis e Warren facevano riferimento a quella *peace of mind*, ossia quella dimensione emotiva che è esattamente la prima pietra angolare della privacy[8], prima che quarant'anni fa – come ricordava il Presidente Stanzione – si passasse da quella dimensione statica del diritto a essere lasciato solo a quella dimensione dinamica del controllo dei dati. È lì che atterra in Europa la *data protection*, nel 1981.
Ma già prima, a cominciare dal 1950 e dall'art. 8 della Convenzione europea dei diritti dell'uomo, è quel diritto a essere lasciato solo che include una dimensione emotiva e non solo fisica. Questo emerge anche quando si guarda al contesto statunitense nel caso *Olmstead*[9], in una delle più importanti opinioni dissenzienti del giudice Brandeis quando precisava che, seppur la conversazione telefonica nel caso in questione era

[8] S. D. Warren - L. D. Brandeis, *The right to privacy*, in *Harvard Law Review*, 4, 1890, 193 ss.

[9] *Olmstead v. United States*, 277 U.S. 438 (1928).

stata intercettata con strumenti tecnologici che sono posti all'esterno dell'abitazione, il quarto emendamento tutela l'individuo dalle interferenze del potere pubblico. Qui si può leggere il riferimento ad Hart, più precisamente al dilemma tra punto di vista esterno e interno, perché evidentemente la maggioranza della Corte Suprema aveva un punto di vista esterno alla tecnologia e quindi evidentemente non poteva considerare che quel tipo di interferenza riguardasse il diritto alla privacy. Invece Brandeis propone un punto di vista interno alla tecnologia, per cui quelle conversazioni *that are only whispered* meritano comunque di essere tutelate. Ebbene quel sussurro oggi è anticipato rispetto al semplice silenzio, attraverso la lettura di possibili proiezioni mentali.

Se è vero che la pietra miliare per la ricostruzione della nascita ed evoluzione della tutela della privacy e dei dati personali è la teorizzazione americana di Warren e Brandeis, è anche vero che, rispetto all'ordinamento giuridico statunitense, in Europa, la protezione dei dati personali e la privacy digitale hanno acquisito lo status di diritti fondamentali. In realtà, questi diritti assumono una natura super fondamentale, che sembra non trovare alcun limite nella dimensione territoriale dell'UE e nel processo di bilanciamento tra diritti fondamentali.

Quando invece si sposta l'attenzione sull'Europa e la sua sensibilità, come è stato detto sottolineato dal Presidente Stanzione, il primo emendamento del costituzionalismo europeo è, prima ancora che la privacy[10], la dignità dell'uomo che evidentemente trova il suo fondamento in quella prima sentenza della Corte costituzionale tedesca del 1983[11], nella quale si identifica la tutela dell'autodeterminazione informativa in due articoli della Costituzione tedesca: l'art. 1, dignità, e l'art. 2, i diritti della personalità. Il diritto al libero sviluppo della propria personalità come riflesso del primo emendamento europeo, cioè dignità, e privacy, caratterizza tutto il sistema europeo. L'attenzione merita di essere posta non solo sull'art. 3 della Carta dei diritti fondamentali dell'Unione europea, o sugli artt. 7 e 8, ma su un articolo che è al di là di qualsiasi sospetto tecnologico, cioè l'art. 8 della Convenzione europea dei diritti dell'uomo, che parla di rispetto della vita privata, e che, come già sottolineato, non poteva prevedere l'evoluzione positiva del diritto alla privacy quando ancora i primi database non erano stati sviluppati in Europa.

Questa evoluzione è iniziata nella seconda metà del XX secolo nel sistema della Convenzione europea dei diritti dell'uomo, quando il diritto alla privacy è stato codificato considerandolo come una sorta di *habeas corpus* riguardante le proiezioni spaziali e relazionali di una persona. Come negli Stati Uniti, anche nel quadro costituzionale europeo il riconoscimento e la codificazione del diritto alla privacy sono stati originariamente pensati lungo la linea "negativa", cioè il riconoscimento del diritto al rispetto della propria vita privata, tuttavia nei decenni successivi questo proprio ha subito una profonda trasformazione. Anzi, soprattutto a causa di un'accelerazione della tecnologia, una dimensione "positiva" del diritto alla protezione dei dati personali ha arricchito la dimensione "negativa", tipica del diritto alla privacy. Questo allargamento alla protezione dei dati personali ha segnato un'espansione di un diritto inizialmente

[10] B. Petkova, *Privacy as Europe's first Amendment*, in *European Law Journal*, 25, 2019, 140 ss.

[11] Decisione della Corte costituzionale federale tedesca del 15 dicembre 1983, 1 BvR 209, 269, 362, 420, 440, 484/83.

limitato al concetto "tradizionale" di privacy. In questo scenario, è stato importante il ruolo svolto dalla Corte europea dei diritti dell'uomo che ha affrontato alcuni cambiamenti tecnologici e le sfide del trattamento dei dati online.

In questo contesto, le istituzioni dell'allora Comunità Europea furono più lente nel codificare un diritto alla protezione dei dati o alla privacy digitale, a causa della loro originale ispirazione economica. Per molto tempo, nell'ordinamento dell'Unione europea, i diritti individuali sono stati riconosciuti quasi esclusivamente al fine di garantire le libertà economiche fondamentali: di conseguenza, in questo contesto, era difficile fare della protezione dei dati personali una questione che potesse catturare l'attenzione delle istituzioni europee per il suo impatto diretto su alcuni diritti fondamentali.

Il punto di rottura è stata la direttiva 95/46/CE, anche se a ispirarla è stata una dimensione economica. La direttiva è stato il primo strumento giuridico nel sistema giuridico dell'UE che ha promosso l'armonizzazione a livello dell'UE delle norme sulla privacy e sulla protezione dei dati e ha stabilito sia alcuni principi generali, sia alcune regole speciali basate su trattamenti particolari. In questo scenario, il diritto fondamentale embrionale alla protezione dei dati personali e alla privacy digitale ha iniziato ad acquisire una declinazione concreta.

In realtà, il riconoscimento e la "costituzionalizzazione" di questo diritto erano strettamente connessi all'evoluzione dell'identità dell'Unione. E, forse, questo è stato un motivo in più per la creazione e il consolidamento di questo diritto super fondamentale. Il diritto alla protezione dei dati personali e della privacy digitale è stato finalmente codificato nella Carta dei diritti fondamentali e sancito dall'art. 16 del Trattato sul funzionamento dell'Unione europea che fornisce la base giuridica per l'adozione di un nuovo quadro normativo per il trattamento dei dati personali, rientrante nell'ambito di applicazione del diritto europeo. Nello specifico, la Carta dei diritti fondamentali dedica due disposizioni in materia, rispettivamente l'art. 7, relativo al rispetto della vita privata e familiare, e l'art. 8, relativo alla protezione dei dati personali.

Risulta quindi chiaro che il diritto alla privacy progettato da Warren e Brandeis come il diritto di essere lasciati soli ha vissuto un processo di migrazione dagli Stati Uniti all'Europa, acquisendo progressivamente una dimensione che non protegge esclusivamente l'aspettativa di privacy dell'individuo ma che vede nella definizione di un sistema di principi e regole per la protezione dei dati un ulteriore momento essenziale per tutelare la personalità. Tuttavia, questa migrazione è stata preceduta da una giurisprudenza molto pervasiva della Corte di giustizia europea orientata ad applicare la visione europea del diritto alla privacy digitale[12].

Guardando al punto di vista della Corte europea dei diritti dell'uomo, è possibile osservare il passaggio dalla privacy all'autonomia personale. Senza passare in rassegna la giurisprudenza della Corte europea dei diritti dell'uomo, è possibile fare almeno un riferimento alla sentenza a *Tysiac v. Poland* del 2007[13]. In questo caso, la Corte sottolinea che il concetto di vita privata va interpretato in maniera estensiva e abbraccia

[12] O. Pollicino - M. Bassini, *Bridge is Down, Data Truck Can't Get Through . . . A Critical View of the Schrems Judgment in The Context of European Constitutionalism*, in *The Global Community - Yearbook of International Law and Jurisprudence*, 2017, 245 ss.

[13] CEDU, *Tysiąc v. Poland*, ric. 5410/03 (2007).

anche aspetti dell'identità sociale, fisica e mentale del soggetto, e quindi l'autonomia personale e l'integrità psicologica. In questo caso emerge un parametro costituzionale di riferimento di natura evolutiva. Tuttavia, tale approccio trova il suo limite nella concettualizzazione giurisprudenziale del fenomeno ossia quel *case-by-case* che dal punto di vista della certezza del diritto necessita di essere compensato attraverso il processo politico, innanzitutto, e rinforzato dai decisori tecnici.
Di conseguenza la domanda che qui emerge è se l'art. 8 della Convenzione europea è un approdo sicuro, o se bisogna riflettere su nuovi diritti, andando quindi verso una codificazione neurotecnologica, che poi segue la stessa impostazione della codificazione della Dichiarazione dei diritti e dei doveri su Internet. Questa esigenza di nuova codificazione sembra far emergere la paura di confrontarsi invece con un dato giuridico che in Europa è già sufficiente per poter cercare di far fronte alle esigenze di tutela.

4. Una visione di carattere costituzionale

Sembra quindi opportuno concentrarsi sulla necessità di una rigenerazione semantica delle carte esistenti, a cominciare dalla Convenzione europea che di fatto trova applicazione proprio in questo contesto, per non menzionare poi l'esempio della Corte di giustizia che applica gli artt. 7 e 8 della Carta a nuovi diritti, come per esempio il diritto a essere dimenticato. Quel *right to be forgotten*, in realtà, non è che una declinazione dei diritti esistenti. Si può quindi fare affidamento su alcune lezioni per quanto riguarda la dimensione digitale che possono essere fatte proprio in questo contesto.
A questo punto, occorre sottolineare alcuni punti. Il primo attiene al livello dell'intervento. Da un punto di vista costituzionale non sembra necessario intervenire con nuove carte, ma intercettare assiologicamente quell'anticipazione della tutela già menzionata, che è già insita nei parametri costituzionali esistenti. Dal punto di vista invece della legislazione secondaria, evitando l'inflazione di carte e di corti, bisognerebbe intervenire su una regolamentazione più specifica, ad esempio, l'art. 22 del GDPR per quanto riguarda la decisione algoritmica. Ebbene, quel tipo di normativa svolge un ruolo importante perché fornisce un tipo di base giuridica specifica in grado di affrontare le sfide del presente ma anche quelle che si porranno per via dello sviluppo tecnologico.
Il secondo punto fondamentale è legato ad un altro possibile terreno comune. La domanda è se, oltre l'autonomia individuale, ci sia un secondo possibile ponte di interconnessione tra le due visioni in contrasto, prima evocate, tra i due "Primi Emendamenti" del costituzionalismo transatlantico, la libertà di espressione da una parte e la privacy (e dignità) dall'altro. La risposta sembra essere positiva. Si tratta del terreno procedimentale che viene chiamato *digital due process*, e che qui potrebbe essere interpretato come *neuro due process*, ossia quella serie di regole che fanno sì che l'interazione tra utente e algoritmo sia rafforzata. Questa tutela è già esistente quando si guarda all'art. 6 della Convenzione europea non verticalmente, ma orizzontalmente, visto lo spostamento nella geometria del potere, non più potere esclusivamente verticale, ma un potere che ha dimensione orizzontale. Quindi l'applicazione orizzontale dei diritti

rileva non soltanto per i diritti sostanziali ma anche per i diritti di matrice procedimentale e il Digital Services Act è proprio un esempio di questo terreno comune da un punto di vista procedimentale può accorciare le distanze delle due sponde dell'Atlantico.

Una terza riflessione attiene invece alla dimensione consumeristica di queste nuove tecnologie. Come precisava Rodotà: «L'indisponibilità dei diritti in questione - qui parliamo di diritti inviolabili - deve essere riferita allo scambio mercantile, non alle attività e alle scelte che attengono al legame sociale». A questo punto occorre domandarsi qual è il *discrimen* ossia qual è la sottile linea rossa in questo contesto tra dimensione sociale e dimensione consumeristica. Sul punto un'altra lezione che si può provare a far propria rispetto agli errori che si sono fatti nella dimensione digitale è legata all'evitare qualsiasi tipo di tentazione relativa alla monetizzazione del neurodato. La monetizzazione del dato nella *digital privacy* è in qualche modo stata forzata dal fatto che quel tipo di illusione che c'è stata in Europa nel '95, cioè l'assoluto controllo dell'utente sui propri dati, si è reputata appunto un'illusione, una promessa non mantenuta. Se non si può avere un controllo assoluto, allora la contropartita è stata la monetizzazione dei dati in una dimensione pragmatica che possa in qualche modo far emergere una gratificazione. Questo tipo di discorso costituisce un punto di non ritorno rispetto al quale bisogna mantenere salde invece le radici del costituzionalismo europeo dei diritti indisponibili contro qualsiasi tentazione consumeristica.

Il terzo punto fondamentale è legato al concetto di autodeterminazione che si declina dal punto di vista del controllo dei dati. Di nuovo è molto importante evitare quello che potrebbe essere invece un tentativo di operare un compromesso tra l'idea di controllo e l'idea invece di consenso come ponte tra le scelte personali e l'ambiente circostante. Come sottolineato da Giorgio Resta, «Attenzione alla delicatezza del consenso perché il ponte tra le scelte personali e l'ambiente circostanti è però infido, perché il problema cruciale sta nel fatto che tale comunicazione non è mai unidirezionale, ma bidirezionale; nel momento in cui opera come dispositivo di regolazione in uscita, il consenso contestualmente apre la sfera soggettiva a tutte le sollecitazioni provenienti dal contesto e segnatamente a quelle del mercato». Questo tipo di doppia proiezione, in entrata e in uscita, è uno dei pericoli in questo momento più rilevanti che vanno affrontati.

A questo punto, occorre concentrarsi sul quarto punto e, in particolare, sull'inflazione di diritti, il conflitto tra diritti, il bilanciamento e le nuove carte. L'ultima lezione che può essere colta dall'esperienza del digitale attiene al ruolo che le corti hanno avuto nell'*enforcement* della *digital privacy* in Europa, da *Google Spain* a *Schrems*. Quel tipo di attivismo ha fatto sì che si siano riscritte alcune regole, che poi sono state codificate dal GDPR. Questo tipo di meccanismo va assolutamente evitato in questo campo. Predieri nel '97, riferendosi alle autorità indipendenti[14], metteva in luce il passo indietro della politica e dell'avanzamento della tecnica. Quando parlava di fare un passo indietro della politica, il riferimento era diretto anche alla politica giudiziaria. In altre parole, bisogna fare attenzione all'*enforcement*, o dal punto di vista del processo politico o dal punto di vista del processo giudiziario, perché la dimensione giudiziaria europea

[14] A. Predieri, *L'erompere delle autorità amministrative indipendenti*, Firenze, 1997

ha prodotto non solo una frammentazione ma anche un nocumento alla certezza del diritto mettendo da parte quello che la stessa Corte di giustizia in *Schrems* fa emergere chiaramente, cioè l'importanza delle Autorità garanti come decisori decentrati di diritto dell'Unione Europea che riscoprano la questione tecnica e la facciano emergere in maniera che possa avere da una parte certezza del diritto e dall'altra parte un'interlocuzione anche alternativa rispetto al singolo giudice del singolo foro.

Occorre quindi prendere atto che la stagione del liberismo tecnologico degli ultimi vent'anni è in qualche modo fallita e insieme a questa la delega in bianco alle piattaforme della possibilità di farsi arbitri dei conflitti tra diritti. Questa è chiaramente un'epoca tramontata. Occorre quindi chiedersi quale sta per iniziare, ossia quella del neurocapitalismo digitale. Sul punto, il potere pubblico e dei decisori tecnici svolge un ruolo importante di guida dell'*enforcement* anche con il fine di riprendersi quel ruolo paracostituzionale che non può essere più minimamente delegato alle piattaforme e ai poteri digitali.

È stato fatto questo errore nella stagione del digitale, sarebbe da evitare in quella delle neuroscienze.

Norme sulle firme elettroniche a confronto: UE, Italia e Cina

Giusella Finocchiaro, Hu Guiping*

Abstract

Con il presente contributo si intende offrire una prospettiva comparata della normativa sulle firme elettroniche, ponendo a confronto la disciplina dettata dall'UNCITRAL, dal legislatore europeo e da quello italiano rispetto a quanto stabilito dalla normativa cinese. Partendo dalla genesi legislativa, si indagano gli aspetti essenziali dei testi normativi, traendo convergenze e divergenze legislative tra i due contesti: europeo e cinese. Laddove tutti i testi legislativi condividono i principi cardine e i concetti di base, le differenze possono incunearsi nelle pieghe dei dettagli esecutivi. Nell'approfondire in chiave comparata le disposizioni della normativa sulle firme elettroniche, si delinea un panorama differenziato relativo anche all'evoluzione di sistema giudiziale. Infine si pone in evidenza la criticità comune dei testi legislativi in esame: il rischio di venire meno della sovranità del titolare delle firme. Il surrogato tecnologico della firma autografa sembra inevitabile in ossequio del principio cardine della libera circolazione di beni.

This contribution is intended to offer a comparative perspective of the legislation on electronic signatures, comparing the discipline dictated by UNCITRAL, the European and Italian legislators with respect to the provisions of Chinese legislation. Starting from the legislative genesis, the essential aspects of the normative texts are investigated, drawing the convergences and divergences between the two contexts: European and Chinese. Where all legislative texts share the cardinal principles and basic concepts, the differences can be wedged in the folds of the executive details. In examining the provisions of the legislation on electronic signatures from a comparative point of view, a differentiated panorama emerges also relating to the evolution of the judicial system. Finally, the common criticality of the legislative texts in question is highli-

* Le opinioni espresse nel presente contributo sono frutto della collaborazione e della riflessione congiunta degli autori. La Prof.ssa Finocchiaro ha sviluppato l'ideazione e la struttura del contributo curandone il coordinamento ed elaborando i par. da 1 a 4, limitatamente alle parti relative alla disciplina internazionale, europea e italiana, mentre la Dott.ssa Hu Guiping ha curato in particolare le parti concernenti la disciplina cinese nei par. da 1 a 4, nonché il par. 5.
Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

ghted: the risk of losing the sovereignty of the electronic signer. The technological substitute of handwritten signature seems inevitable in compliance with the cardinal principle of the free movement of goods.

Sommario

1. Sull'approccio normativo. - 2. Prestatore di servizi fiduciari vs certificatore di firme elettroniche. - 3. Sulla responsabilità del prestatore di servizi fiduciari. - 4. Sul valore probatorio della firma qualificata. - 5. Questione sulla sovranità del firmatario elettronico.

Keywords

firme elettroniche – UNCITRAL – Unione europea – Italia - Cina

1. Sull'approccio normativo

Con il presente contributo si intende offrire una prospettiva comparata della normativa sulle firme elettroniche, ponendo a confronto la disciplina dettata dall'UNCITRAL (la Commissione delle Nazioni Unite per il diritto commerciale internazionale), dal legislatore europeo e da quello italiano rispetto a quanto stabilito dalla normativa cinese.
Partendo dall'azione dell'UNCITRAL, la Commissione delle Nazioni Unite ha disciplinato il fenomeno delle transazioni elettroniche a livello internazionale adottando il *Model Law On Electronic Commerce* (di seguito, per brevità, "MLEC") nel 1996 e il *Model Law On Electronic Signature* (nel prosieguo, per brevità, "MLES") nel 2001, svolgendo così un ruolo di armonizzazione e di uniformazione del diritto[1].
I principi su cui si basa l'azione dell'UNCITRAL sono quelli dell'autonomia contrattuale delle parti, della non discriminazione, della neutralità tecnologica e dell'equivalenza funzionale[2]. Mentre il principio dell'autonomia contrattuale non richiede ulteriori illustrazioni, occorre soffermarsi brevemente sugli altri principi.
Secondo il principio di non discriminazione, non si può negare validità giuridica ed

[1] L'UNCITRAL (United Nations Commission of international trade law), istituita nel 1966 e composta da una parte dei Paesi che siedono all'Assemblea generale delle Nazioni Unite, svolge da sempre un ruolo essenziale di armonizzazione del diritto commerciale internazionale, predisponendo strumenti di *hard law* e *soft law*. Cfr. G. Herrmann, *Establishing a legal framework for electronic commerce: the work of the United Nations Commission on International Trade Law (UNCITRAL)*, in *World Trade and Arbitration Materials*, 11, 1999, 45 ss. Inoltre, per una completa analisi sul MLEC e al MLES, si rinvia a: E.A. Caprioli- R. Sorieul, *Le commerce international électronique: vers l'émergence de règles juridiques trasnationales,* in *Journal du droit international*, 1991, 323 ss.; R. Sorieul, *The UNCITRAL Model Law and the modernization of legislation to facilitate electronic commerce,* in *Electronic commerce initiatives of ESCAP: business facilitation needs/ Economic and Social Commission for Asia and the Pacific*, 1998, 59 ss.; R. Sorieul, *The UNCITRAL's Model Law on Electronic Signatures,* in G. Chatillon (a cura di), *Internet International Law. International and European studies and comments*, Bruxelles, 2005, 389 ss.

[2] Per approfondimenti cfr. G. Finocchiaro, *Il ruolo dell'UNCITRAL nello sviluppo della disciplina sul commercio elettronico*, in F. Delfini - G. Finocchiaro (a cura di), *Diritto dell'informatica*, Torino, 2014, 64 e H.D. Gabriel, *The United Nations Convention of the use of electronic communications in international contracts: an overview and analysis*, in *Uniform Law Review/Revue de droit uniforme*, 11, 2006, 288.

efficacia probatoria alle informazioni generate, trasmesse e registrate su un supporto non cartaceo unicamente in ragione della loro forma elettronica.

Il principio della neutralità tecnologica invece sancisce che le disposizioni di legge devono essere tecnologicamente neutre rispetto alla tecnologia, senza riconoscere o privilegiare una soluzione tecnologica specifica per implementare i principi giuridici affermati. In altri termini, la norma giuridica non dovrebbe riferirsi a un livello di sicurezza predeterminato o a una tecnologia specifica, bensì dovrebbe limitarsi a dettare lo scopo da raggiungere senza indicare le modalità tecniche per il suo perseguimento.

Il principio di equivalenza funzionale poi si fonda sull'analisi delle funzioni che svolge il documento cartaceo, al fine di determinare in che modo tali funzioni possano essere ugualmente soddisfatte attraverso gli strumenti elettronici. In particolare, il MLEC fissa criteri e requisiti volti a determinare se le funzioni svolte dalla scrittura[3], dalla firma[4] e dall'originale[5] possano essere ugualmente assicurate attraverso determinate tecniche elettroniche, ogniqualvolta la normativa nazionale prescriva l'uso di documenti "cartacei", "firmati" o "originali". Secondo questa logica, la normativa sulle firme elettroniche, anziché disciplinare la firma elettronica, mira a creare un equivalente che soddisfi le funzioni svolte dalla firma. Ne consegue che la firma elettronica sarà destinata a produrre gli stessi effetti giuridici della firma autografa, qualora sia idonea ad assolvere tutte le funzioni svolte da quest'ultima. Il compito del legislatore diventa allora quello di definire i requisiti che la firma elettronica deve rispettare affinché possano dirsi assolte le funzioni a cui questa è preordinata, producendo conseguentemente i corrispondenti effetti giuridici.

L'UNCITRAL, inoltre, ha stabilito alcuni criteri di affidabilità per l'equivalenza tra firme elettroniche e firme autografe, introducendo in particolare un modello a doppio livello (*two-tier approach*)[6]. Secondo quanto disposto dall'art. 6, c. 1, MLES, in via generale ("primo livello") il *data message*[7] e la firma autografa sono considerati funzionalmente equivalenti «se la firma elettronica offre un livello di affidabilità adeguato allo scopo per cui il messaggio di dati è stato generato o trasmesso, alla luce delle circostanze, incluse le pattuizioni contrattuali»[8]. Inoltre, ai sensi dell'art. 7 del MLES, qualsiasi metodo – purché conforme agli standard internazionali riconosciuti e compatibile con le *rules of private international law*[9] – può essere utilizzato per soddisfare il requisito di firma autografa. Al secondo livello, l'affidabilità della firma elettronica è presunta se tale firma soddisfa i requisiti fissati dall'art. 6, c. 3, MLES, tra cui la corrispondenza

[3] Art. 6, MLEC.

[4] Art. 7, MLEC.

[5] Art. 8, MLEC.

[6] Cfr. U. Draetta, *Internet et le commerce électronique en droit international des affairs,* in *Recueil des cours de l'Académie de Droit International de la Haye*, Dordrecht, 314, 2005, 125; J. Penadés, *Firma electrónica y comercio electrónico. Regulación en España y en la Unión Europea*, in F.J. Orduña – G.A. Aguilera (a cura di), *Comercio, administraciòn y registros electrònicos*, Cizur Menor, 2009, 547 ss., spec. 567 ss.

[7] Giova precisare che il MLES non si riferisce al documento informatico, ma al "*data massage*", che definisce quale «*information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy*» (art. 2, c. 1, lett. *c*), MLES).

[8] Art. 6, c. 1, MLES.

[9] Art. 7, c. 2 e 3, MLES.

esclusiva dei dati per la formazione della firma al firmatario e il controllo esclusivo del firmatario sui dati. La norma contempla altresì metodi di firma elettronica che possono essere riconosciuti *ex ante* da un'autorità statale, da un ente privato accreditato o dalle parti stesse, quali metodi che soddisfano criteri di affidabilità tecnica stabiliti nella legge modello[10].

Il MLEC e il MLES rappresentano dunque i principali strumenti di *soft law*[11] di riferimento per le legislazioni nazionali di oltre sessanta paesi del mondo, fra cui la Cina.

L'approccio legislativo cinese prevede una fedele riproduzione delle prescrizioni dettate dal *Model Law* elaborato dall'UNCITRAL. In vigore dal 1° aprile 2005, la legge sulle firme elettroniche della Repubblica Popolare della Cina si pone l'obiettivo di disciplinare la firma elettronica, determinarne gli effetti giuridici[12], chiarire lo *status* giuridico e le procedure di certificazione del prestatore del servizio di certificazione e, infine, stabilire le misure di sicurezza per l'utilizzo di firme elettroniche. Vengono anche richiamati alcuni principi fondamentali, tra cui quello di autonomia contrattuale[13], di non discriminazione[14], di neutralità tecnologica e di equivalenza funzionale[15]. Con la riforma del 2015, il legislatore cinese ha poi introdotto il meccanismo del doppio livello di verifica dell'affidabilità e della validità della firma, mentre la riforma dell'aprile 2019 ha esteso l'ambito di applicazione della normativa alla sottoscrizione degli atti aventi ad oggetto i beni immobili.

Per quanto riguarda, invece, il panorama italiano, occorre anzitutto chiarire l'approccio che sta a fondamento della disciplina in materia di firme informatiche[16], basato sullo strumento cognitivo della metafora[17]. Sebbene si tratti di entità ontologicamente diverse, il legislatore italiano ha infatti posto in relazione la sottoscrizione autografa e le firme informatiche. Non si tratta tuttavia di un rapporto di identità ma solo di una associazione terminologica sotto il profilo cognitivo. In altre parole, si tratta di una relazione basata sul "come se" e non, invece, sull'"uguale", che consente di stabilire che le firme informatiche sono come la firma autografa[18]. Tale disciplina ha subito, nel

---

[10] Cfr. L.G. Castellani, *I testi dell'UNCITRAL in materia di diritto del commercio elettronico*, in F. Delfini – G. Finocchiaro (a cura di), *Diritto dell'informatica*, cit., 46 ss.

[11] Sulla distinzione tra *soft law* e *hard law* si rinvia a: J.H. Dalhuisen, *Custom and its revival in transnational private law*, in *Duke Journal of Competitive & International Law*, 399, 2008, 355: «*Soft law means rules that do not emerge from an autonomous source of law and are not law in that sense. In the international commercial and financial sphere, soft law often means proposals or sets of principles from Unidroit, Uncitral or other such organizations, or from think-tanks that aspire to reflect the living law particularly at the transnational level. […] To repeat, short of soft law emerging as custom or general principle, it is not law, and therefore not a norm that must be applied, although it may provide guidance (usually supplementary to hard law or as some manifestation thereof)*».

[12] Art. 1 della legge cinese sulle firme elettroniche.

[13] Art. 3 della legge cinese sulle firme elettroniche.

[14] Art. 3, c. 2, legge cinese sulle firme elettroniche.

[15] Artt. 4-8 e 13 della legge cinese sulle firme elettroniche.

[16] Si precisa che la dicitura "firme informatiche" viene impiegata in senso a-tecnico e comprensivo di tutte le firme elettroniche.

[17] Il tema della metafora nel diritto viene illustrato con la consueta ricchezza culturale e profondità di analisi da F. Galgano, *Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto*, Bologna, 2010, 22-23.

[18] G. Finocchiaro, *La metafora e il diritto nella normativa sulla cosiddetta "firma grafometrica"*, in *Dir. Inf.*, 1, 2013, 3.

corso dell'ultimo ventennio, ripetuti interventi legislativi che hanno progressivamente portato alla definizione dell'attuale quadro costituito dall'adeguamento al regolamento (UE) 910/2014 (nel prosieguo, per brevità, "Reg. e-IDAS") e dal Codice per l'amministrazione digitale di cui al d.lgs. 7 marzo 2005, n. 82, come successivamente modificato e integrato (di seguito, per brevità, "CAD")[19]. La ragione di questa continua opera di affinamento compiuta dal legislatore italiano è, in gran parte, riconducibile alla necessità di coordinarsi con le scelte operate a livello europeo.

In sede europea, l'*iter* legislativo ha visto l'adozione, in un primo momento, della direttiva 1999/93/CE e, in un secondo momento, del Reg. e-IDAS. La *ratio* alla base del primo intervento era quella di superare gli ostacoli che le normative dei diversi Stati membri ponevano alla libera circolazione dei beni e dei servizi nel mercato interno. Il legislatore ha tentato quindi di creare un quadro giuridico europeo armonizzato per la fornitura dei servizi di firma elettronica e di certificazione, al fine di favorire lo sviluppo nel mercato interno del commercio elettronico. Questo proposito continua ad essere perseguito, divenendo ancor più concreto, grazie al Reg. e-IDAS che, proprio in virtù della sua natura di regolamento, detta una disciplina generale direttamente applicabile in tutti gli Stati membri dell'Unione europea. L'obiettivo del Reg. e-IDAS è infatti quello di fornire una base giuridica comune che consenta di «garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari»[20]. La previsione di una base giuridica condivisa permette altresì di assicurare l'interoperabilità giuridica e tecnica tra gli Stati membri in relazione agli strumenti di identificazione elettronica, di autenticazione e di firma elettronica. Perseguendo tale finalità, l'art. 6 del Reg. e-IDAS introduce l'obbligo di riconoscimento reciproco transfrontaliero dei mezzi di identificazione *on line* nel settore pubblico. In altri termini, il Reg. e-IDAS prevede a favore degli Stati membri la facoltà di notificare i loro sistemi di identificazione elettronica alla Commissione europea, qualora tali sistemi soddisfino le condizioni relative ai livelli di garanzia previsti dall'art. 7 del Reg. e-IDAS. Una volta accertato il soddisfacimento di tali condizioni, la Commissione pubblica i regimi di identificazione elettronica notificati in un apposito elenco nella Gazzetta Ufficiale dell'UE[21] e, a partire da questo momento ed entro 12 mesi, gli altri Stati membri sono obbligati a riconoscere il sistema di identificazione elettronica notificato. In questo modo, viene consentito a cittadini, imprese, amministrazioni pubbliche o organismi dello Stato membro notificante di accedere ai servizi in rete dei soggetti pubblici di un altro Paese dell'Unione, a condizione che il sistema di identificazione notificato abbia un livello di sicurezza pari o superiore a quello richiesto dal servizio offerto. L'interoperabilità tecnica dei sistemi elettronici all'interno dell'Unione è poi garantita dall'attuazione del già citato principio di neutralità tecnologica che impone requisiti minimi tecnici d'in-

[19] Il CAD è stato, negli anni, oggetto di molteplici interventi legislativi volti a realizzare un apparato normativo organico. In particolare, tra le riforme più recenti, occorre segnalare il d.lgs. 26 agosto 2016, n. 179, che ha provveduto a raccordare la normativa nazionale al Reg. e-IDAS e il d.lgs. 13 dicembre 2017, n. 217 che ha modificato la disciplina probatoria del documento informatico e ha previsto un nuovo processo di firma elettronica avanzata. Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 85.

[20] Art. 1 del Reg. e-IDAS.

[21] Art. 9, par. 2, Reg. e-IDAS.

teroperabilità e di sicurezza per l'identificazione elettronica.
Sempre con riferimento al quadro normativo europeo, appare opportuno sottolineare come il Reg. e-IDAS se, da un lato, mantiene sostanzialmente invariata la normativa previgente relativa alle firme elettroniche, dall'altro, introduce e disciplina anche nuovi strumenti, quali: sigilli elettronici, che garantiscono la provenienza e l'integrità del documento; validazioni temporali elettroniche, che forniscono prova della data e dell'ora del documento opponibile a terzi; servizi elettronici di recapito certificato, che permettono di dare prova dell'invio e dell'avvenuta ricezione dei dati, riducendo rischi di perdita, danneggiamento, furto e modifica non autorizzata di questi; servizi riguardanti i certificati di autenticazione dei siti web, che consentono di dimostrarne l'affidabilità, collegando il sito alla persona fisica o giuridica a cui viene rilasciato il certificato.

2. Prestatore di servizi fiduciari vs certificatore di firme elettroniche

Sempre in prospettiva comparata, giova esaminare la figura del prestatore di servizi fiduciari.
Una compiuta definizione di prestatore di servizi fiduciari non appare né nella direttiva 1999/93/CE né nel *Model Law* dell'UNCITRAL. Entrambi, infatti, si limitano a prevedere la figura del prestatore di servizi di certificazione, descrivendola come l'entità o la persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche[22]. Una scelta differente viene, invece, compiuta dal legislatore europeo nel Reg. e-IDAS tramite l'introduzione di un'espressa definizione di prestatore di servizi fiduciari che consente, se adeguatamente interpretata, di ricomprendere al suo interno anche la figura del prestatore di servizi di certificazione. Ciò è possibile muovendo dal combinato disposto delle norme del Reg. e-IDAS che definiscono rispettivamente il prestatore di servizi fiduciari e il servizio fiduciario. Il primo è quella «persona fisica o giuridica che presta uno o più servizi fiduciari come prestatore qualificato o non qualificato»[23]. Per servizio fiduciario, si intende invece «un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi: a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure b) creazione, verifica e convalida di certificati di autenticazione di siti web; o c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi»[24].
Alla luce di tali definizioni, come anticipato, la figura del prestatore di servizi di certi-

[22] All'art. 2, par. 1, n. 11, direttiva 1999/93/CE. In maniera analoga, l'art. 1, c. 1, lett. e), MLES, definisce il "certification service provider" come «person that issues certificates and may provide other services related to electronic signatures».

[23] Art. 3, n. 19, Reg. e-IDAS.

[24] Art. 3, n. 16, Reg. e-IDAS. La normativa europea distingue tra servizi fiduciari qualificati e non qualificati, a seconda che questi soddisfino i requisiti fissati dal Regolamento e che garantiscano un maggiore livello di sicurezza e di affidabilità nelle transazioni elettroniche. Cfr. L. Greco, *Articolo 3. Definizioni*, in F. Delfini -G. Finocchiaro (a cura di), *Diritto dell'informatica,* cit., 48.

ficazione, disciplinata dalla previgente Direttiva e dal *Model Law*, pare rientrare di fatto in quella del prestatore di servizi fiduciari, che, al pari del primo, fornisce servizi come quelli di creazione, verifica e convalida di firme elettroniche, nonché di rilascio del certificato delle firme. Il legislatore europeo non opera dunque alcuna distinzione di ruolo tra prestatore di firme elettroniche e certificatore, salvo quella relativa allo svolgimento di un servizio "qualificato". Tale attributo, una volta riconosciuto dall'organismo di vigilanza in capo al prestatore di servizi fiduciari, consente a quest'ultimo – tra le altre cose – di rilasciare il certificato della firma elettronica qualificata[25].

Superata tale questione definitoria, è possibile esaminare la disciplina prevista dal Reg. e-IDAS per tutti i prestatori di servizi fiduciari, i quali sono soggetti ai medesimi requisiti ed obblighi.

In primo luogo, il Reg. e-IDAS conferma i principi cardine relativi alla protezione dei dati personali stabiliti dal regolamento (UE) 679/2016, imponendo ai prestatori di servizi fiduciari di rispettare gli obblighi e i principi generali in materia di protezione dei dati personali e, in particolare, quelli inerenti alla sicurezza del trattamento dei dati e alla necessità e finalità del trattamento, secondo cui i dati devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità del trattamento.

In secondo luogo, la normativa europea stabilisce per tutti i prestatori di servizi fiduciari requisiti, specificamente in materia di sicurezza e responsabilità, tali da garantire la dovuta diligenza, trasparenza e attendibilità delle loro operazioni e dei loro servizi[26].

Il Reg. e-IDAS istituisce poi per tutti i prestatori di servizi fiduciari un regime di vigilanza in grado di assicurare parità di condizioni per la sicurezza e l'attendibilità dei loro servizi, in un'ottica di tutela degli utenti e del funzionamento del mercato interno.

L'unica differenza si riscontra nella sorveglianza sui prestatori di servizi fiduciari qualificati e sui prestatori privi di qualifica che, per i primi, avviene *ex ante* e per i secondi *ex post*[27]. A ciò si aggiunga che, nel Reg. e-IDAS, i prestatori qualificati sono soggetti a requisiti e obblighi più stringenti, sempre nella prospettiva di garantire un elevato livello di sicurezza di tutti i servizi fiduciari qualificati offerti. Il medesimo intento emerge dal disposto dell'art. 13, par. 2, Reg. e-IDAS, in cui si afferma che i prestatori qualificati possono stabilire limiti all'uso dei servizi forniti, a condizione che i clienti ne siano debitamente e anticipatamente informati e che tali limiti siano conoscibili a terzi. Il rispetto di tale previsione giova altresì al prestatore qualificato, il quale, adeguando il proprio comportamento a quanto prescritto, potrà mitigare la possibilità di essere chiamato a rispondere per responsabilità legate ad un uso dei servizi eccedente il limite fissato[28].

Con riferimento al quadro normativo italiano, emerge come, sotto il profilo dell'accreditamento e della qualificazione del prestatore di servizi fiduciari, il legislatore abbia

[25] Art. 3, n. 15, Reg. e-IDAS. Ulteriori differenze tra prestatori di servizi fiduciari qualificati e non emergono, come vedremo di seguito, in riferimento ai requisiti e agli obblighi previsti dal Reg. e-IDAS per questi soggetti.

[26] Considerando 35 del Reg. e-IDAS.

[27] Considerando 36 e art. 17, par. 3, Reg. e-IDAS.

[28] Considerando 37 del Reg. e-IDAS.

deciso di stabilire regole più restrittive rispetto a quelle del Reg. e-IDAS[29]. In Italia, infatti, il servizio di certificazione di firma elettronica qualificata può essere fornito solo da un soggetto pubblico o privato costituito nella forma di società di capitali[30].
Per quanto riguarda, invece, il quadro normativo cinese, occorre precisare sin da subito che il legislatore cinese, con la legge sulle firme elettroniche, non detta una disciplina specifica relativa ai prestatori di servizi fiduciari, ma si limita a definire i requisiti che il certificatore cinese deve soddisfare[31]. Il richiedente deve essere una persona giuridica costituita in forma societaria, dotata di sufficiente capitale e di personale tecnico e gestionale adeguato. Questi deve inoltre ottenere una doppia autorizzazione preventiva da parte della *State Cryptography Administration*, ai fini dell'utilizzo di chiavi crittografiche, e da parte del Ministero dell'Industria e dell'Informazione, ai fini dell'accreditamento[32]. Sebbene la legge cinese, diversamente dalla direttiva 1999/93/CE e dal *Model Law* dell'UNCITRAL, non fornisca una definizione di certificatore o di servizio di certificazione elettronica, tale lacuna è colmata dall'art. 2 del Decreto del Ministero cinese dell'Industria dell'Informazione del 28 gennaio 2005, n. 35, recante "Misure per l'amministrazione dei servizi di certificazione elettronica", in vigore dal 1° aprile 2005, ove il servizio di certificazione elettronica è definito come «il servizio pubblico di verifica sull'autenticità e affidabilità per le parti interessate delle firme elettroniche» [33]. Il certificatore, invece, è «un'istituzione di terza parte che presta servizi di certificazione elettronica ai firmatari elettronici e alle parti facenti affidamento sulla firma elettronica». Nel 2009, l'art. 2 del citato decreto ministeriale n. 35/2005[34] viene modificato tramite l'introduzione di un "servizio di certificazione elettronica al pubblico in generale"[35]. Questo servizio, così come chiarito dal decreto ministeriale

[29] Art. 29 del CAD.

[30] L'ultima modifica effettuata dal d.lgs. 217/2017 stabilisce, all'art. 29, c. 2, CAD che «il richiedente deve avere natura giuridica di società di capitali e deve disporre dei requisiti di onorabilità, requisiti tecnologici e organizzativi, nonché garanzie assicurative ed eventuali certificazioni adeguate al volume dell'attività svolta e alla responsabilità assunta nei confronti dei propri utenti e dei terzi. Tali requisiti sono individuati, nel rispetto della disciplina europea, con decreto del Presidente del Consiglio dei Ministri, sentita l'AgID. Il decreto in questione determina altresì i criteri per la fissazione delle tariffe dovute all'AgID per lo svolgimento di queste attività, nonché i requisiti e le condizioni per lo svolgimento delle attività di cui al comma 1 da parte di amministrazioni pubbliche».

[31] Art. 17 della legge cinese sulle firme elettroniche.

[32] Art. 18 della legge cinese sulle firme elettroniche.

[33] 2005年 "电子认证服务管理办法", 第二条 本办法所称电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的公众服务活动。
本办法所称电子认证服务提供者，是指为电子签名人和电子签名依赖方提供电子认证服务的第三方机构（以下称为"电子认证服务机构"）。

[34] 中华人民共和国工业和信息化部令第1号《电子认证服务管理办法自2009年3月31日起施行;
第二条 本办法所称电子认证服务，是指为电子签名相关各方提供真实性、可靠性验证的活动。
本办法所称电子认证服务提供者，是指为需要第三方认证的电子签名提供认证服务的机构（以下称为"电子认证服务机构"）。
向社会公众提供服务的电子认证服务机构应当依法设立。

[35] L'art. 2, c. 1, decreto ministeriale n. 35/2005 recita: «I servizi di certificazione per E-government rivolti agli organi pubblici, sono basati sulla tecnologia crittografica con certificati digitali. I servizi di certificazione elettronica dell'E-government comprendono i servizi di certificazione elettronica di

recante "Misure per l'amministrazione della certificazione elettronica per l'E-government", può essere fornito solamente da un'istituzione di certificazione elettronica (di seguito, per brevità, "CA", ossia *Certificate Authority*) costituita a norma di legge[36]. In particolare, ai sensi dell'art. 15, la CA deve essere «una persona giuridica di un'istituzione pubblica o una persona giuridica di società controllata dallo Stato, che ha ottenuto l'autorizzazione per i servizi di certificazione elettronica». Sono dunque previsti *ex lege* due requisiti. In primo luogo, la società di capitali, avente l'autorizzazione a fornire un servizio di certificazione elettronica, deve essere controllata dallo Stato per poter fornire i servizi all'*E-government* – in altre parole, la norma impone di fatto un regime di monopolio statale del servizio di certificazione riguardo agli affari governativi. In secondo luogo, le società di capitali a controllo statale devono presentare una richiesta di valutazione delle qualifiche alla *State Cryptography Administration* e, in caso di esito positivo, queste potranno essere accreditate ed incluse nell'elenco CA, reso pubblico sul sito di tale Amministrazione.

In definitiva, venendo, ancora una volta, all'analisi comparata delle norme, con riguardo alla definizione di prestatore del servizio di certificazione, occorre notare una differenza tra il Reg. e-IDAS e la legge cinese. Mentre il primo consente tanto ad una persona fisica quanto ad una giuridica di prestare i servizi di firma elettronica, la norma cinese esclude la persona fisica, assegnando tale attività solamente ad una persona giuridica. In aggiunta, se il Reg. e-IDAS fissa obblighi generali, requisiti e responsabilità dei prestatori di servizi fiduciari[37], la legge cinese li prevede solo nei confronti dei prestatori di servizi di certificazione di firma elettronica. Infine, sebbene la normativa cinese stabilisca in modo esplicito i requisiti che il certificatore deve soddisfare, rimane indefinita la questione relativa alla disciplina applicabile ai prestatori di firma elettronica. Di conseguenza, in mancanza di una precisa indicazione da parte del legislatore, i giuristi cinesi[38], sin dall'entrata in vigore della legge in commento, si sono interrogati su chi possa essere accreditato a fornire il servizio di firma elettronica. I principali interrogativi ruotano attorno alla *ratio* sottesa a tale scelta legislativa. Si tratta di una impostazione ereditata dal MLES oppure deriva dall'applicazione del principio di neutralità tecnologica? Al di là del dibattito dottrinale, dall'esame dei siti cinesi emerge come le piattaforme di *e-commerce* prestino servizi quasi onnicomprensivi che vanno dalla certificazione alla firma elettronica, dalla conservazione alla consulenza legale fino all'autenticazione e perizia giudiziaria e così via. A tal proposito giova

E-government per i dipartimenti governativi, per le imprese e le istituzioni, i gruppi sociali e il pubblico in generale».

[36] "电子政务电子认证服务管理办法" L'Annuncio della *State Cryptography Administration* n. 7/2009 sulla pubblicazione delle "Misure per l'amministrazione della certificazione elettronica per E-government", in vigore dal 1° novembre 2009. In questo atto si stabilisce che entro il 1° maggio 2010, il prestatore del servizio di certificazione elettronica, per avviare l'attività per l'*E-government*, deve presentare la richiesta di valutazione di qualifica alla *State Cryptography Administration*.

[37] Art. 19, "Requisiti di sicurezza relativi ai prestatori di servizi fiduciari"; Art. 20, "Vigilanza dei prestatori di servizi fiduciari qualificati"; Art. 21, "Avviamento di un servizio fiduciario qualificato"; Art. 24, "Requisiti per i prestatori di servizi fiduciari qualificati".

[38] Cfr.法制日报 , 作者: 路虹 ,"电子签名法"实施遭遇规章空白 配套机构欠缺, 2005年06月13日11:03

richiamare il caso del certificatore (CA) iTrusChina Co., Ltd.di Pechino[39], il quale offre servizi per autenticare l'identità del soggetto richiedente, servizi di firma elettronica e certificazione, di contratto elettronico e conservazione dei dati con metodi *blockchain*. Anche in virtù di questa situazione di fatto, nel 2019, anno in cui sono state adottate dall'UNCITRAL le *Draft provisions on the cross-border recognition of identity management and trust services*[40] in coordinamento con il Reg. e-IDAS, è entrata in vigore la legge sul commercio elettronico della Repubblica Popolare della Cina che ha permesso di annoverare i prestatori di firme elettroniche tra gli operatori delle piattaforme di *e-commerce*. In questo modo, i primi sono stati assoggettati ai medesimi obblighi generali previsti per i secondi, tra cui la tenuta di un registro dell'impresa[41] e l'ottenimento di una licenza[42] necessari ad avviare l'attività[43], la pubblicazione di specifiche informazioni[44] nonché l'obbligo di ottemperare ad alcuni adempimenti fiscali[45] e il divieto di abusare della propria posizione dominante[46].
Alla luce di questa ricognizione, si può concludere che sia il quadro normativo europeo sia quello cinese sembrano ammettere la prassi di considerare unitariamente i servizi di firma elettronica e quelli relativi alla loro certificazione.

3. Sulla responsabilità del prestatore di servizi fiduciari

Il Reg. e-IDAS disciplina il regime di responsabilità dei prestatori di servizi fiduciari. In particolare, l'art. 13, al par. 1, primo capoverso, prevede una forma di responsabilità extracontrattuale in capo al prestatore nei confronti di qualsiasi soggetto, persona fisica o giuridica, compreso il terzo che non sia legato al prestatore da alcun vincolo contrattuale. Il secondo capoverso pone a carico del danneggiato l'onere della prova del dolo o della negligenza che, tuttavia, subisce un'inversione al terzo capoverso, ove si afferma che il dolo o la negligenza di un prestatore qualificato sono presunti, a meno che questi non dimostri il contrario. La disposizione prosegue, prevedendo al par. 2 un'esenzione di responsabilità del prestatore di servizi fiduciari qualora il cliente utilizzi i servizi oltre i limiti indicati causando così un danno a terzi, a condizione che il prestatore abbia previamente informato, in modo adeguato e tempestivo, i propri clienti dell'esistenza delle

[39] https://www.itrus.com.cn/intro.html. La società ha fornito i suoi servizi di certificazione per quasi 500.000.000 di utenti provenienti da diversi settori, quale governo, banca, sicurezza, assicurazione, magistratura, offerte, finanza Internet, ecc.

[40] A/CN.9/WG.IV/WP.160 – *Draft Provisions on the Cross-border Recognition of Identity Mangement and Trust Services*, 16 September 2019.

[41] Art.10 della legge cinese sul commercio elettronico.

[42] Art.12 della legge cinese sul commercio elettronico.

[43] Si noti, perciò, che non essendoci requisiti a livello di norma ordinaria, le regole relative ai requisiti e alla licenza sono definite unicamente da norme secondarie e attuative.

[44] Artt. 15 e 16 della legge cinese sul commercio elettronico.

[45] Art. 11 della legge cinese sul commercio elettronico.

[46] Art.22 della legge cinese sul commercio elettronico. Si noti che, non essendovi requisiti fissati a livello di norma ordinaria, le regole relative ai requisiti e alla licenza sono dettate da norme secondarie e attuative.

limitazioni d'uso dei servizi da esso forniti e che tali limitazioni siano state rese conoscibili ai terzi[47]. Infine, il par. 3 stabilisce che l'applicazione dei commi precedenti deve avvenire nel rispetto delle norme di ciascuno Stato membro in materia di responsabilità[48]. Di conseguenza, la diretta applicabilità del Reg. e-IDAS non preclude al legislatore nazionale di precisare il regime di responsabilità dei prestatori di servizi fiduciari.

In Italia, diversamente da quanto previsto dal Reg. e-IDAS, la disciplina della responsabilità viene delineata dall'art. 30 del CAD solo con riferimento ai prestatori di servizi fiduciari qualificati che «cagionano danno ad altri nello svolgimento della loro attività» [49], imponendo loro un onere della prova più gravoso rispetto a quello della normativa europea. Si tratta dell'*onus probandi* previsto dall'art. 2050 c.c. per l'esercizio di attività pericolose, in base al quale i prestatori qualificati devono provare di avere adottato tutte le misure idonee ad evitare il danno. Tale disposizione ha suscitato numerosi rilievi critici in dottrina, non solo perché aggrava la posizione del prestatore qualificato rispetto alla norma europea, ma anche perché è riconducibile ad una responsabilità extracontrattuale di natura oggettiva[50].

Volgendo poi lo sguardo alla normativa cinese, come accennato in precedenza, la legge sulle firme elettroniche si occupa delle sole responsabilità del prestatore di servizi di certificazione di firme elettroniche, con particolare riferimento alla pubblicazione del *certificate practice statement* (di seguito, per brevità, "CPS"[51]), alla verifica dell'identità del destinatario del servizio[52], alla garanzia dell'autenticità e dell'integrità delle informazioni sulle firme elettroniche[53], alla tempestiva comunicazione[54] e conservazione di informazioni relative al certificato[55], senza invece prevedere limiti di responsabilità né obblighi sotto il profilo della protezione dei dati personali[56]. Le regole appena richiamate, se violate, comportano l'insorgere di responsabilità di natura civile[57], amministrativa[58] e penale[59].

L'art. 28 della legge cinese sulle firme elettroniche esclude poi la responsabilità del

---

[47] Cfr. F. Delfini, *Art. 13. Responsabilità e onere della prova*, in F. Delfini – G. Finocchiaro (a cura di), *Diritto dell'informatica,* cit., 153.

[48] Art. 13, par. 3, Reg. e-IDAS: «i paragrafi 1 e 2 si applicano conformemente alle norme nazionali in materia di responsabilità».

[49] Art. 30 del CAD.

[50] F. Delfini, *Art. 13*, cit., 156.

[51] Art. 19 della legge cinese sulle firme elettroniche.

[52] Art. 20 della legge cinese sulle firme elettroniche.

[53] Artt. 21 e 22 della legge cinese sulle firme elettroniche.

[54] Art. 23 della legge cinese sulle firme elettroniche.

[55] Art.24 della legge cinese sulle firme elettroniche.

[56] Solo nel 2018, lo *standard CPS for E-government* ha fissato gli obblighi e la responsabilità del certificatore sotto il profilo della riservatezza e della protezione dei dati personali, della proprietà intellettuale, della garanzia e del funzionamento del servizio. Queste responsabilità, insieme a quelle relative alla conservazione, sono inserite nell'accordo sui servizi di certificazione, sottoscritto dall'utente e dal certificatore o da un suo delegato.

[57] Art. 28 della legge cinese sulle firme elettroniche.

[58] Artt. 29, 30 e 31 della legge cinese sulle firme elettroniche.

[59] Artt. 32 e 33 della legge cinese sulle firme elettroniche.

prestatore qualora questi dimostri che il danno subito dal titolare della firma, o dalla parte facente affidamento sulla firma elettronica, non gli sia imputabile. Nello specifico, il prestatore deve dare prova che i servizi da esso prestati siano stati svolti in stretta osservanza della legge in commento e delle disposizioni dello Stato nonché del CPS depositato presso il Ministero dell'Industria dell'Informazione.

In ottica comparata, dunque, è possibile notare come, nonostante le differenze in materia di responsabilità dei fornitori di servizi, i testi normativi presi in considerazione presentino anche alcuni elementi comuni come la presunzione di dolo o negligenza del prestatore, la responsabilità contrattuale e l'inversione dell'onere della prova.

Un ulteriore tema che si presta ad essere analizzato in chiave comparata è quello delle sanzioni, rispetto alle quali il Reg. e-IDAS detta una norma generale: «Gli Stati membri stabiliscono norme relative alle sanzioni da applicare in caso di violazioni del presente regolamento. Le sanzioni previste sono effettive, proporzionate e dissuasive»[60].

In Italia, con gli interventi dettati dal d. lgs. 26 agosto 2016, n. 179 e dal d. lgs. 13 dicembre 2017, n. 217, il legislatore ha inasprito la pena per la violazione di obblighi previsti dal Reg. e-IDAS e dallo stesso CAD. Riguardo alle sanzioni amministrative inflitte a seguito di violazioni degli obblighi in generale, è stato introdotto un regime sanzionatorio differenziato a seconda della gravità della violazione. In particolare, sono aumentati i minimi e i massimi edittali delle sanzioni pecuniarie che ora possono essere irrogate da un minimo di 40 mila e ad un massimo di 400 mila euro, in base alla gravità della violazione accertata e all'entità del danno cagionato all'utenza. In caso di gravi violazioni del CAD[61], l'Agenzia per l'Italia digitale (nel prosieguo, per brevità, "AgID") può disporre, in aggiunta, la cancellazione del fornitore del servizio dall'elenco dei soggetti qualificati e il divieto di accreditamento o qualificazione per un periodo non superiore a due anni[62]. L'art. 32-*bis*, c. 2, CAD prende poi in considerazione le ipotesi di malfunzionamento nei servizi offerti dai prestatori qualificati tale da comportare l'interruzione del servizio oppure la mancata o intempestiva comunicazione del disservizio all'AgID e agli utenti. In questi casi, a meno che si provi la forza maggiore o il caso fortuito, l'AgID può irrogare sanzioni amministrative al prestatore qualificato. Si prevede altresì la cancellazione dall'elenco pubblico del prestatore qualificato in caso di reiterazione dell'inadempimento nel biennio successivo alla prima diffida dell'Autorità volta a richiedere il ripristino della regolarità dei servizi. Infine, le sanzioni di cui all'art. 32-*bis* sono aumentate fino al doppio in caso di violazioni degli obblighi del prestatore di servizi fiduciari qualificato relativi alla cessazione dell'attività, nonostante l'intimazione da parte dell'AgID ad ottemperarvi entro un termine non superiore a trenta giorni[63].

Muovendo alla legge cinese sulle firme elettroniche, questa riconosce una responsabilità civile in capo al certificatore nelle ipotesi di violazione degli artt. 19, 20, 21, 22 e

[60] Art. 16 del Reg. e-IDAS.

[61] Secondo quanto disposto dall'art. 32-*bis*, c. 1, CAD, si considerano gravi «le violazioni del presente Codice idonee a esporre a rischio i diritti e gli interessi di una pluralità di utenti o relative a significative carenze infrastrutturali o di processo del fornitore di servizio».

[62] Art. 32-*bis* del CAD.

[63] Art. 37, c. 4-*ter*, CAD.

24 per danni cagionati al firmatario e ai terzi che hanno fatto affidamento sulla firma. In particolare, agli artt. 29 e 30 della legge cinese sulle firme elettroniche sono sancite sanzioni di natura amministrativa per le ipotesi di violazione dell'obbligo di tempestiva comunicazione in caso di sospensione e cessazione dell'attività[64], e di esercizio del servizio senza licenza[65]. Nulla, invece, è previsto per i casi di disservizio o disfunzione emergenziale del sistema di certificazione.

Altre sanzioni sono previste per le violazioni degli obblighi relativi al CPS o per l'inadempimento relativo alla conservazione di informazioni, ma possono essere irrogate solamente se il soggetto intimato a porvi rimedio non ottempera all'obbligo prescritto[66]. In questa eventualità, le conseguenze consistono nella revoca della licenza e nel divieto, al dirigente direttamente responsabile e al diretto incaricato, di prestare servizio per un periodo di dieci anni.

Nel 2009, sono state introdotte ulteriori ipotesi di violazione, quali l'occultamento di informazioni[67], il rifiuto dell'obbligo di sostituire il prestatore che cessa l'attività, la mancata notifica di modifiche del CPS e di *policy* di certificato[68]. Nel caso in cui il prestatore di servizio commetta tali violazioni, il Ministero può intimargli di porvi rimedio entro un determinato termine e, in caso di inottemperanza, può irrogare una sanzione pecuniaria dai cinque mila ai dieci mila RMB. La sanzione pecuniaria inflitta per intempestiva comunicazione di sospensione o cessazione dell'attività[69] è, invece, di importo pari a 1.000-7.000€, cifra decisamente modesta se paragonata ai fatturati di prestatori come iTrust Co.ltd che rilascia 500.000 certificati all'anno.

Infine, non sono previste sanzioni pecuniarie per violazioni relative alla verifica dell'identità del destinatario del servizio, alle garanzie volte ad assicurare l'integrità e l'esattezza delle informazioni contenute nel certificato[70] e all'obbligo di conservazione[71]. Quanto invece al risarcimento del danno derivante dalla condotta inadempiente del certificatore, la prassi è quella di stabilirne l'ammontare all'interno dell'accordo contrattuale tra le parti e spesso questo è pari alle spese di rilascio del certificato. In questo modo, viene fissato, di fatto, un limite alla responsabilità del certificatore.

[64] Art. 23 della legge cinese sulle firme elettroniche.

[65] Ai sensi dell'art. 29 della legge cinese sulle firme elettroniche, per le attività illecite di prestazione di servizi di certificazione elettronica senza licenze, oltre all'immediata cessazione dell'attività, è prevista l'irrogazione di una sanzione pecuniaria di importo pari a 300 mila RMB. Per la violazione dell'obbligo di comunicare la sospensione dell'attività, entro il termine stabilito, la sanzione amministrativa prevista dall'art. 30 della legge cinese sulle firme elettroniche va da un minimo di 10.000 yuan ad un massimo di 50.000 yuan.

[66] A questo proposito, si vedano gli artt. 31, 19 e 24 della legge cinese sulle firme elettroniche.

[67] Art. 38 della legge cinese sulle firme elettroniche.

[68] Art. 40 della legge cinese sulle firme elettroniche.

[69] Art. 23 della legge cinese sulle firme elettroniche.

[70] Artt. 21 e 22 della legge cinese sulle firme elettroniche.

[71] Art. 24 della legge cinese sulle firme elettroniche.

4. Sul valore probatorio della firma qualificata

Nel seguente paragrafo sono esaminate le questioni connesse agli effetti giuridici della firma qualificata e all'efficacia probatoria del documento informatico a cui è apposta.
A tale proposito, giova innanzitutto richiamare l'art. 25 del Reg. e-IDAS che sancisce l'equivalenza degli effetti giuridici della firma elettronica qualificata rispetto a quelli di una firma autografa e stabilisce l'interoperabilità delle firme elettroniche qualificate basate su un certificato qualificato tra gli Stati membri.
Analogamente, il legislatore italiano attribuisce alla firma elettronica qualificata un valore giuridico più elevato e riconosce al documento informatico sottoscritto con tale firma un'efficacia probatoria rafforzata rispetto alle altre tipologie di firme informatiche, ossia quella semplice e quella avanzata[72]. L'art. 21, c. 2-*bis*, CAD riserva infatti alla firma elettronica qualificata e alla firma digitale la sottoscrizione degli atti di cui all'art. 1350, c. 1, numeri da 1 a 12, c.c., a pena di nullità. Sotto il profilo probatorio, invece, l'art. 20, c. 1-*bis*, stabilisce che il documento informatico sottoscritto con firma digitale, altro tipo di firma elettronica qualificata o firma elettronica avanzata[73], soddisfa il requisito della forma scritta e ha efficacia probatoria *ex* art. 2702 c.c., ossia fa piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta, a condizione che la sottoscrizione sia legalmente considerata come riconosciuta, o riconosciuta esplicitamente o tacitamente dall'apparente sottoscrittore[74].
Il rinvio all'art. 2702 c.c. consente di richiamare l'istituto del disconoscimento[75] della scrittura privata e della sottoscrizione[76]. Come è noto, il procedimento di disconoscimento della scrittura privata e della sottoscrizione autografa consiste in una formale negazione della paternità, tempestivamente avanzata in giudizio da parte di colui con-

[72] In dottrina sul tema, seppur antecedenti al CAD: A. Gentili, *Documento informatico e tutela dell'affidamento*, in *Riv. dir. civ.*, II, 1998, 163 ss.; A. Graziosi, *Premesse ad una teoria probatoria del documento informatico*, in *Riv. dir. proc. civ.*, 1998, 481 ss.; Id, voce *Documento informatico (diritto processuale civile)*, in *Enc. dir. Annali*, II, Milano, 2008, 492 ss.; M. Orlandi, *La paternità delle scritture: sottoscrizioni e forme equivalenti*, Milano, 1997; Id, *Il falso digitale*, Milano, 2003. Tra le opere monografiche: G. Navone, Instrumentum *digitale: teoria e disciplina del documento informatico*, Milano, 2012.

[73] Giova precisare che, a seguito della riforma operata dal d.lgs. 217/2017, è stato introdotto un ulteriore processo di firma consistente nel «processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore». Anche tale documento ha l'efficacia probatoria *ex* art. 2702 c.c. ed è ritenuto idoneo a soddisfare la forma scritta.

[74] Ai sensi dell'art. 20, c. 1-*bis*, CAD, il documento informatico non sottoscritto o sottoscritto con firma elettronica semplice, invece, è, sotto il profilo probatorio, liberamente valutabile dal giudice, tenuto conto delle sue caratteristiche oggettive di sicurezza, integrità e immodificabilità in concreto. Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 87 e 88.

[75] Cfr. G. Buonomo, *La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio (alla luce delle modifiche introdotte dalla l. 221/2012)*, in *Dir. Inf.*, 2, 2013, 255 ss.

[76] Art. 214 c.p.c., rubricato "Disconoscimento della scrittura privata": «Colui contro il quale è prodotta una scrittura privata, se intende disconoscerla, è tenuto a negare formalmente la propria scrittura o la propria sottoscrizione. Gli eredi o aventi causa possono limitarsi a dichiarare di non conoscere la scrittura o la sottoscrizione del loro autore». Si veda anche l'art. 216 c.p.c., rubricato "Istanza di verificazione": «La parte che intende valersi della scrittura disconosciuta deve chiederne la verificazione, proponendo i mezzi di prova che ritiene utili e producendo o indicando le scritture che possono servire di comparazione».

tro il quale è prodotta la scrittura privata cartacea o la sottoscrizione autografa. La parte che voglia avvalersi della scrittura o sottoscrizione eventualmente disconosciuta dovrà esperire un procedimento di verificazione affinché il giudice disponga la comparazione di scrittura e di grafia, con l'eventuale supporto di una perizia grafologica[77], al fine di accertare la paternità della scrittura e della sottoscrizione autografa, intesa come diretta riferibilità di questi ultimi al sottoscrittore. La firma autografa è infatti un gesto fisico personale che imprime sulla carta un segno indelebile della volontà del sottoscrittore ed è, dunque, indissolubilmente legata al firmatario[78].

Alla luce di quanto appena esposto, appare inverosimile pensare di riferirsi al concetto di paternità – tradizionalmente inteso – anche in relazione alle firme informatiche apposte sul documento informatico. Invero, queste ultime non sono il risultato della mano che traccia, fissando la grafia su un supporto analogico. Si tratta piuttosto di un processo che il firmatario, avvalendosi di un dispositivo per la creazione di firma o di servizi offerti da soggetti terzi, realizza seguendo istruzioni ben precise. Il processo è impersonale, soprattutto quando vi è una scarsa consapevolezza da parte del firmatario o quando non si ha simultaneità tra il gesto manuale e la volontà, frammentando e segmentando così l'espressione di sovranità. In considerazione delle differenze di cui sopra, il disconoscimento della scrittura privata e della sottoscrizione autografa non sembra ammissibile in caso di firma elettronica qualificata e firma digitale[79]. Se lo fosse, il destinatario del documento informatico dovrebbe adempiere ad un *onus probandi* pressoché impossibile. Dal canto suo, invece, il titolare della firma potrebbe limitarsi a negare l'utilizzo della firma[80].

Nel tentativo di porre rimedio ai problemi di autenticità collegati all'uso della firma elettronica qualificata che non consente di individuare il soggetto che effettivamente utilizza il dispositivo di firma, ma solamente colui che ne è titolare[81], il legislatore italiano compie un passo ulteriore rispetto alla disciplina europea[82]. Infatti, grazie all'introduzione dell'art. 20, c. 1-*ter*, CAD, viene sancito che «l'utilizzo del dispositivo di firma

[77] Art. 216 del c.p.c.

[78] F. Carnelutti, *Studi sulla sottoscrizione*, in *Riv. dir. comm.*, I, 1929, 509.

[79] Trattano il tema del disconoscimento della firma: A. Gentili, *I documenti informatici: validità ed efficacia probatoria*, in *Dir. internet*, 2006, 308 e il Consiglio di Stato – Sezione Consultiva per gli Atti Normativi, nel parere reso in occasione dell'adunanza del 30 gennaio 2006, n. 31, avente ad oggetto la bozza di decreto legislativo recante disposizioni correttive e integrative al d.lgs. 7 marzo 2005, n. 82, entrambi ritenendolo come del tutto peculiare.

[80] Cfr. G. Finocchiaro, *La firma digitale. Formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici.,* in F. Galgano (a cura di), *Libro VI, Della tutela dei diritti, art. 2699-2720. Commentario del Codice Civile Scialoja-Branca*, Bologna, 2000, 127.

[81] G. Finocchiaro, *La firma digitale*, cit., 7.

[82] Gli artt. 29 e 30 del Reg. e-IDAS introducono alcuni importanti requisiti. In primo luogo, i dispositivi di creazione di firma qualificata devono essere muniti di certificazione di sicurezza. In secondo luogo, la firma elettronica qualificata deve essere munita di un certificato qualificato fornito da un prestatore di servizi fiduciari qualificato. Queste disposizioni – assieme ad altre – sono volte ad assicurare l'identificabilità del soggetto titolare del dispositivo per la creazione della firma. In particolare, il certificato qualificato ha una funzione identificativa del soggetto titolare della firma e del soggetto che l'ha certificata, nonché di affidabilità rispetto al registro su cui essa è stata pubblicata per la consultazione. La qualifica di titolare della firma, in questi casi, si riferisce al titolare del dispositivo per la firma, ossia della chiave privata certificata.

elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria». Si introduce, quindi, una presunzione di corrispondenza tra l'utilizzatore del dispositivo e la figura del firmatario, il quale è di norma il titolare legittimo del dispositivo, a meno che non ne perda il possesso.
Da tale presunzione relativa è possibile far discendere due corollari principali.
In primo luogo, il titolare del dispositivo è gravato dell'obbligo di diligenza nella custodia e nella cura del dispositivo di firma elettronica qualificata. Infatti, ai sensi dell'art. 32 del CAD, rubricato "Obblighi del titolare di firma elettronica qualificata e del prestatore di servizi di firma elettronica qualificata", «il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma». Tali obblighi non sono, invece, previsti dal Reg. e-IDAS.
In secondo luogo, il titolare del dispositivo è gravato dell'onere di fornire la prova contraria nel caso in cui intenda negare che si tratti della propria firma. Ciò comporta che questi, per vincere la presunzione, debba dimostrare che un terzo si sia servito della chiave privata dopo essersene indebitamente impossessato[83].
Ci si interroga, allora, riguardo al tipo di prova di cui il titolare del dispositivo può concretamente disporre per contestare la riferibilità della sottoscrizione di un documento informatico mediante una firma elettronica qualificata o digitale. A questo proposito occorre evidenziare che, diversamente dal disconoscimento previsto dall'art. 241 c.p.c., l'oggetto del disconoscimento di cui all'art. 20, c. 1-*ter*, CAD, da parte dell'apparente sottoscrittore non è la firma o la scrittura, bensì l'utilizzo del dispositivo di firma elettronica qualificata o digitale. Di conseguenza, il giudice valuterà il fatto in base ad un criterio di responsabilità alla luce dei criteri dell'art. 32 CAD già esaminati, e non invece sulla base di un criterio di paternità[84].
Dunque, in caso di utilizzo abusivo causato da perdita o furto del dispositivo di firma qualificata, il titolare del dispositivo può provare il falso, dimostrando: a) di non aver utilizzato il dispositivo in un dato momento, con l'allegazione attestante la perdita del dispositivo in un momento anteriore all'apposizione della firma (ad esempio, la denuncia di smarrimento del dispositivo); b) che la causa della perdita o del furto del dispositivo non gli è imputabile; c) di aver adottato tutte le misure tecniche e organizzative per

[83] A tal riguardo, il Consiglio di Stato, nel parere emesso il 30 gennaio 2006, ha affermato che «il documento informatico, munito di firma digitale, sembra porsi, per effetto dell'inversione dell'onere della prova in tema di disconoscimento, come una sorta di *tertium genus* tra la scrittura privata e l'atto pubblico, avendo in giudizio la stessa efficacia probatoria di una scrittura privata munita di sottoscrizione legalmente riconosciuta, ed essendo, in realtà, in nulla diverso da una scrittura privata munita di sottoscrizione non autenticata». Cfr. F. Delfini, *Documento informatico, forma analogica e forma elettronica: dalla scrittura privata autenticata all'atto pubblico informatico,* in F. Delfini – G. Finocchiaro (a cura di), *Diritto dell'informatica*, cit., 2014, 262.

[84] Il Consiglio di Stato, Sezione Consultiva per gli Atti Normativi, nell'Adunanza del 7 febbraio 2005, ha sottolineato l'importanza di «superare i vecchi concetti di falso, strettamente legati al principio di 'paternità' della firma e non a quello di 'responsabilità' per la firma». Si veda anche il parere del Consiglio di Stato emesso il 30 gennaio 2006. In questa occasione, il Consiglio di Stato ha affermato che «sarebbe (…) opportuno individuare il tipo di prova che consente il disconoscimento secondo un criterio di responsabilità nella conservazione e nell'utilizzo della chiave privata».

evitare i danni ai terzi, allegando la richiesta al prestatore di servizi fiduciari qualificato di revoca o sospensione del certificato[85] non appena sia venuto a conoscenza della perdita o della compromissione del dispositivo; d) di essere estraneo alle dichiarazioni emesse imputategli dalla firma digitale; e) di non conoscere il destinatario delle dichiarazioni firmate digitalmente. Tali prove sono finalizzate a sottrarre qualsivoglia valore giuridico al documento sottoscritto, eliminandone – oltre all'efficacia sua propria – qualsiasi ulteriore effetto attribuitogli dalla legge. Il titolare del dispositivo può, altresì, citare in giudizio il prestatore di servizio fiduciario qualificato, qualora si sia verificato un ritardo nella pubblicazione delle informazioni relative allo smarrimento del dispositivo, ossia un'anomalia del processo di firma. Come già accennato, l'apprezzamento del giudice si baserà sul criterio di responsabilità del titolare del dispositivo e del prestatore di servizi fiduciari qualificato. In particolare, in tema di responsabilità del prestatore di servizi fiduciari qualificato, si è precedentemente ricordato che l'art. 13, par. 1, Reg. e-IDAS dispone che «i prestatori di servizi fiduciari sono responsabili di danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento». Al contrario, l'art. 30, c. 1, CAD attribuisce al prestatore di servizi fiduciari qualificato la responsabilità risarcitoria per il danno cagionato ad altri nello svolgimento della loro attività, a meno che non provi di aver adottato tutte le misure idonee ad evitare il danno. In conclusione, pare possibile individuare solo un limitato numero di mezzi di prova di cui il titolare della firma elettronica qualificata o digitale dispone per eccepire che la firma gli sia imputabile. Al fine di ovviare a tali criticità, sembra auspicabile affidarsi alla tecnologia, creando un meccanismo procedimentale che garantisca l'identificazione del soggetto nel momento di effettiva apposizione della firma da parte di questi.

Discorso diverso è invece quello relativo all'invalidità della firma digitale. In dottrina, sono state elaborate diverse ipotesi di invalidità della firma digitale, quali l'erronea attribuzione del certificato, l'utilizzo abusivo della chiave privata e così via. Nell'ipotesi di utilizzo abusivo della chiave privata in un rapporto giuridico contrattuale, ci si è domandati se la fattispecie sia riconducibile al riempimento non autorizzato del foglio firmato in bianco, *absque pactis*, o alla fattispecie del *falsus procurator* o *falsus dominus*[86]. Il primo caso ricorre quando l'autore del riempimento non sia stato autorizzato dal sottoscrittore con preventivo patto. Nel secondo caso, per *falsus procurator* si intende colui «che ha contrattato come rappresentante senza averne i poteri o eccedendo i limiti delle facoltà conferitegli dal rappresentato»[87], mentre con *falsus dominus,* ci si riferisce alla fattispecie generale della dichiarazione sotto falso nome o sotto nome altrui. La questione necessiterebbe di una trattazione più approfondita che esula tuttavia dallo scopo della presente analisi. In ogni caso, occorre sottolineare che, con riferimento all'efficacia probatoria e ai rimedi processuali, l'orientamento dottrinale prevalente riconosce l'applicabilità della disciplina del foglio firmato in bianco e della querela

[85] Art. 32, c. 3, lett. g), CAD.

[86] Cfr. G. Finocchiaro, *La firma digitale,* cit., 134 ss.

[87] Art. 1398 c.c., rubricato "Rappresentanza senza potere": «colui che ha contrattato come rappresentante senza averne i poteri o eccedendo i limiti delle facoltà conferitegli, è responsabile del danno che il terzo contraente ha sofferto per avere confidato senza sua colpa nella validità del contratto».

di falso al documento informatico firmato con chiave privata usata abusivamente[88]. Al contrario, si è respinta la possibilità di assimilare l'ipotesi di utilizzo abusivo della chiave privata, alle fattispecie del *falsus procurator* e del *falsus dominus* che presuppongono che l'autore dell'atto abusivo sia individuabile e sia conosciuto dal firmatario o dal *dominus*[89]. Nel contesto della sottoscrizione tramite firma elettronica qualificata o firma digitale, infatti, è assai improbabile che il legittimo titolare del dispositivo possa identificare l'utilizzatore abusivo dal momento che quest'ultimo non instaura alcun rapporto giuridico obbligatorio con il titolare legittimo della firma, ma solamente con il destinatario delle dichiarazioni, diretto beneficiario delle dichiarazioni emesse dall'apparente sottoscrittore. Di conseguenza, il criterio di responsabilità contrattuale tra il titolare del dispositivo e l'utilizzatore abusivo non sembra potersi applicare, a meno che l'utilizzatore abusivo sia egli stesso il destinatario delle dichiarazioni oggetto della controversia. Altrettanto inverosimile è la configurazione di una responsabilità di natura extracontrattuale: qualora l'utilizzo del dispositivo da parte dell'utilizzatore abusivo, in luogo del legittimo titolare, venga qualificato alla stregua di atto illecito, riconducibile all'art. 2043 c.c., il soggetto danneggiato finirebbe per dover produrre le prove del dolo o della colpa dell'utilizzatore abusivo, per giunta ignoto. Questo ragionamento non è condivisibile data la difficoltà per il danneggiato di adempiere a tale onere probatorio. Sotto questi profili, la normativa cinese appare innovativa.

Nel 2015, infatti, la legge cinese sulle firme elettroniche ha introdotto l'art. 14, ai sensi del quale: «una firma elettronica affidabile ha i medesimi effetti giuridici di una firma autografa o di un sigillo». Per rendere effettiva la disposizione, il governo cinese ha adottato una strategia di ampio respiro. In primo luogo, al fine di assicurare l'affidabilità tecnologica e gestionale della firma, è stato ideato un progetto per la creazione di una rete fiduciaria basata sul *Public Key Infrastructure* (nel prosieguo, per brevità, "PKI") che si interfaccia con il sistema di autenticazione elettronica attraverso un processo gestionale di autorizzazione, valutazione e individuazione di responsabilità. In secondo luogo, sono state predisposte ingenti risorse da investire in ricerca e sviluppo dei prodotti crittografici insieme a sistemi gestionali, quale *core technology* della certificazione della firma elettronica[90]. Inoltre, occorre sottolineare che, sul versante tecnologico, il governo cinese ha designato le società, come E Sign, preposte a sviluppare prodotti crittografici per uso commerciale, prodotti e sistemi autonomi sviluppati in Cina, per assicurare la sicurezza di rete e di informazione[91]. La *State Cryptography Administration* ha

[88] Cfr. G. Finocchiaro, *La firma digitale,* cit., 142.

[89] Ivi, 136 e 139.

[90] Cfr. http://www.sca.gov.cn/sca/xwdt/2006-05/26/content_1002342.shtml国家密码管理局魏允韬副局长在"电子签名法" 实施一周年暨电子认证服务业发展研讨会"上的讲话. In un intervento del 26 maggio 2006, il vice direttore della *State Cryptography Administration* Wei Yuntao ha fatto un bilancio a distanza di un anno dall'entrata in vigore della legge cinese sulle firme elettroniche, ribadendo che il codice segreto è la *core* tecnologia per l'applicazione della legge. Lo stesso vice direttore ha dichiarato che è pronta una gamma di prodotti crittografici commerciali ormai consolidati per soddisfare le esigenze del settore dei servizi di certificazione elettronica.

[91] Cfr. https://baijiahao.baidu.com/ CA. Stando ai dati dell'Istituto di ricerca dell'industria dell'informazione, alla fine del 2017, vi erano 34 service *providers* di firme elettroniche da parte di terzi, di cui 7 affiliate a prestatori di certificazione elettronica (CA), mentre 22 dedicate prettamente ai contratti elettronici. Il volume di affari ha visto un incrementato del 200% dal 2015 al 2017 e ha raggiunto un

il compito di accreditare la CA che utilizza codici segreti per uso commerciale nei servizi di certificazione elettronica *e-government*, e di gestire insieme ai relativi dipartimenti le firme elettroniche e i messaggi di dati utilizzati in attività governative[92].

Sul versante della regolamentazione, invece, a partire dal 2016, è stata adottata una serie di norme tecniche volte a uniformare il format dello standard nazionale del documento elettronico[93] e il processo di apposizione di firma elettronica affidabile. In particolare, dal novembre 2016, è in vigore il National standard GB/15843.3-2016 per l'autenticazione di soggetti, che adotta il meccanismo di firma digitale[94], compatibile con lo standard ISO/IEC 9798-3:1998, IDT. Dal 2018, invece, è entrato in vigore lo standard nazionale GB/T 36651-2018 "Protocollo di tecnologia informatica della sicurezza per l'identificazione biometrica in ambiente attendibile"[95]. Si tratta di uno dei trentasei standard nazionali in vigore per l'identificazione biometrica che la Cina ha sviluppato dal 2012 al 2018 in tema di autenticazione dell'identità. Nello stesso anno, sono state adottate le "Specifiche tecniche generali della tecnologia informatica di sicurezza per la firma mobile"[96] e i "Requisiti tecnici per la creazione e verifica delle firme elettroniche affidabili basati sul certificato digitale con l'infrastruttura PKI"[97]. Questi ultimi mirano a colmare la lacuna legislativa relativa ai requisiti tecnici per la creazione e la verifica della firma affidabile. Inoltre, qualificando come affidabile la firma elettronica basata sul certificato digitale, il legislatore si pone in continuità con la prassi internazionale.

Infine, la strategia adottata dal governo cinese in materia di prove informatiche comprende numerosi interventi in ambito giudiziario. In particolare, a partire dalla metà del 2016, con l'avvento di *Internet Plus*, il sistema giudiziario cinese è diventato digitale e la tecnologia informatica sta trasformando i tribunali in luoghi virtuali ampiamente

miliardo di Yuan nel 2018. La piattaforma E-Sign (e签宝) ha superato i 100 milioni di yuan di fatturato nel 2019, con 400 mila utenti aziendali e 10 milioni di utenti individuali. Nel 2016, 10 aziende cinesi raggiungevano un fatturato di oltre 1 milione di yuan. Inoltre, sempre nel 2016, stando ai dati di Saizhiku citato dell'Istituto, 35 piattaforme di firma elettronica gestite da terzi hanno investito più di 100 milioni di yuan in ricerca e sviluppo tecnologico.

92 Cfr. Art. 29 della legge sulla crittografia della Repubblica Popolare della Cina, in vigore dal 1° gennaio 2020.
第二十九条　国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定，会同有关部门负责政务活动中使用电子签名、数据电文的管理.

93 Si fa riferimento allo "Standard nazionale OFD per l'immodificabilità del documento elettronico". Tale standard si applica all'archiviazione, lettura, EDI e utilizzo di documenti standard, in ambiti *e-commerce*, *e-government*, EDI, rilascio di informazioni, pubblicazione digitale e gestione degli archivi.

94 "信息技术安全技术实体鉴别第3部分：采用数字签名技术的机制（补篇）", 2016年11月实施. 由国家质量监督检验检疫局与国家标准化管理委员会联合发布。pubblicato il 25 aprile 2016 dall'Amministrazione nazionale di supervisione, controllo e quarantena insieme alla Commissione di gestione in standardizzazione nazionale.

95 "信息安全技术基于可信环境的生物特征识别身份鉴别协议".

96 "信息安全技术移动签名通用技术规范". Il documento definisce i termini tecnici relativi alla firma mobile e specifica le regole sui dispositivi dotati di funzione di comunicazione mobile, sull'applicazione, progettazione, sviluppo e test dei sistemi di firma elettronica nei dispositivi di comunicazione.

97 "信息安全技术/公钥基础设施基于数字证书的可靠电子签名生成及验证技术要求" 2017年12月29日发布， 2018年7月1日实施. Adottato dalla Commissione nazionale di standardizzazione tecnica della sicurezza cibernetica, pubblicato il 29 dicembre 2017, in vigore dal 1° luglio 2018.

accessibili. La solennità del Palazzo di giustizia e del processo è stata sostituita dai colloqui informali via *Wechat* o *Skype*, con la possibilità di seguire le udienze in qualsiasi luogo fisico. Dal 2017, sono state istituite tre *Internet Court*[98]. Nel 2018, la Corte di Internet di Hangzhou[99] ha inaugurato la prima piattaforma[100] per l'acquisizione di prove informatiche basate sulla *blockchain*[101], con un *database* di oltre 1,95 milioni di prove, tra cui certificati notarili e prove peritali, prove di piattaforme da parte di terzi, prove di conservazione e di verifica, atti pubblici, prove di decisioni arbitrali. Nel giro di pochi anni, sono nati anche la piattaforma del sistema giudiziario nazionale per i servizi di iscrizione a ruolo di cause via *Wechat*[102] e il sistema *one-stop* di servizio di arbitrato *online* istituito da Fadada insieme all'arbitrato Guangzhong e il micro-tribunale mobile. Al fine di innovare il proprio sistema giudiziario, assicurando processi più semplici e ve-

[98] https://baike.baidu.com/item/杭州互联网法院. La Corte di Internet di Hangzhou è stata inaugurata il 18 agosto 2017, come la prima corte pilota nazionale che tratta controversie *online*. A settembre 2018, sono state istituite altre due corti a Pechino e Guangzhou. La Corte di Internet, ricorrendo alle tecnologie di rete, completa l'intero procedimento giudiziario *online*, dall'atto di citazione, iscrizione a ruolo, deposito di prove, udienza, al giudizio sino all'esecuzione. L'obiettivo è quello di facilitare il processo giudiziario civile per i cittadini, risparmiando risorse giudiziarie. L'innovazione del meccanismo è integrata tramite la predisposizione di molteplici e diversificati metodi di risoluzione delle controversie come quelli in via preventiva, mediazione di terze parti e processo. Grazie ad una gestione professionale, efficiente e conveniente delle controversie *online*, avvalendosi di tecnologie di analisi di *Big Data* e facendo un raffronto tra vari moduli, si cera di formulare regole strutturate e standardizzate di giudizio su Internet.

[99] In un anno, la Corte di Internet di Hangzhou ha trattato 12.103 casi concludendone 10.646.

[100] Cfr. https://www.8btc.com. La piattaforma è collegata a più interfacce di dati. La Corte può trasmettere, verificare e archiviare rapidamente, attraverso la piattaforma, i dati elettronici rilevanti. La Corte può altresì accedere direttamente alle piattaforme di *e-commerce* per ottenere informazioni sulla transazione relativa alla causa. Tutti i più importanti *service provider* come Taobao, JD.com e piattaforme *e-commerce*, di contratti elettronici e conservazione di certificati, possono diventare fornitori di prove informatiche per la piattaforma della Corte. Ciò significa che se le parti desiderano proporre le prove sulle transazioni attraverso la piattaforma *e-commerce*, possono semplicemente inserire nella piattaforma di contenzioso o nella piattaforma di prove informatiche il numero d'ordine per recuperare le informazioni rilevanti sulla transazione. Se i dati del caso sono conservati su un'altra piattaforma già connessa, le parti devono solo inviare il numero *hash* della conservazione di dati, mentre spetterà alla Corte di Internet il compito di completare la comparazione intelligente dei valori *hash* ed accedere ai dati attraverso la piattaforma di prove informatiche. Se i dati verificati risultano corrispondenti ai fatti, sono assunti nell'ambito della domanda giudiziaria.

[101] Cfr. https://www.chinacourt.org/article/detail/2018/10/id/3522776.shtml. La *blockchain* è strutturata in tre livelli. Il primo è il livello del programma di *blockchain*. L'utente può, tramite il programma, registrare direttamente nella *blockchain* tutte le sue operazioni ossia consegnare *online* le prove informatiche quali contratto elettronico, processo di tutela dei diritti e specifiche del processo di servizio. Il secondo è il livello di competenza di tutto l'itinerario della *blockchain*. In questa fase si forniscono servizi fiduciari affidabili quale l'autenticazione del nome reale, la firma elettronica, la marca temporale, la conservazione di dati. Il terzo è il livello di alleanza giudiziaria. Mediante la tecnologia *blockchain*, si possono connettere istituti notarili, CA/RA, il centro di valutazione giudiziario e i tribunali, ed ognuno rappresenta un nodo della catena. Con tale impalcatura, la *blockchain* giudiziaria è in grado di risolvere i problemi di affidabilità dei dati elettronici per tutto i loro ciclo di vita.

[102] Cfr. https://www.qianzhan.com. Il 25 dicembre 2017 è stata istituita la prima piattaforma nazionale del sistema giudiziario che offre servizi via *Wechat* di iscrizione a ruolo di cause. L'attore, in qualunque posto e qualsiasi momento, una volta ottenuto via *Wechat* il numero d'iscrizione a ruolo, può effettuare via telefono mobile tutto la procedura, tra cui l'invio di materiali di contenzioso, il deposito delle prove, l'autenticazione dei nomi reali e il pagamento di spese di giustizia. Si tratta di contenzioso amministrativo e civile in materia di commercio.

loci per i cittadini[103], il governo cinese ha saputo sfruttare al meglio l'incremento del livello tecnologico imprenditoriale delle firme elettroniche così come lo sviluppo di Internet mobile, *cloud computing*, *blockchain*, "*mobile phone shield*" – sistema di autenticazione mobile "sicuro e conveniente" –, sistemi di conservazione di firme elettroniche e sistemi di certificazione "blockchain".

Se in passato i professionisti facevano affidamento su autorità terze, come i notai, per acquisire e costituire le prove, oggi, il crescente ricorso a prove informatiche in giudizio ha determinato la nascita, in Cina, di molte piattaforme di dati elettronici gestite da soggetti terzi, tra cui Factom e E-Sign[104]. La piattaforma E-Sign, ad esempio, si coordina con le istituzioni di valutazione giudiziaria, gli istituti notarili, gli arbitrati, i tribunali e altre istituzioni considerate affidabili per costruire un'alleanza *blockchain*, ossia un *database* di prove congiunte, attraverso il sistema di archiviazione distribuita della *blockchain*, caratterizzata dall'immodificabilità dei *file* che, utilizzando l'algoritmo *hash* irreversibile, generano una catena di codici memorizzata sulla piattaforma. Il medesimo *file* viene contestualmente memorizzato presso istituzioni di valutazione giudiziaria, istituti notarili e arbitrali, realizzando una validazione incrociata delle prove. Così facendo, tali piattaforme hanno realizzato un modello di *business* costruito sulla base delle loro condizioni tecniche e dei loro obiettivi commerciali, diretto ad offrire servizi verso terzi di raccolta e acquisizione di prove informatiche.

Al fine di legittimare l'uso delle tecnologie disponibili, il 18 giugno 2018 sono state adottate "Le disposizioni della Corte suprema del popolo su alcune questioni processuali nella corte di Internet"[105] (di seguito, per brevità, "Disposizioni"). In particolare, l'art. 11[106] prevede che la Corte di Internet riconosca i dati elettronici presentati dalle parti, mediante mezzi tecnici di raccolta, acquisizione e antimanomissione di prove informatiche quali firme elettroniche, marcatempo affidabile, verifica sui valori dell'*hash* e della *blockchain*, oppure per mezzo di certificati rilasciati dalla piattaforma di costituzione e acquisizione di prove, che dimostrino la loro autenticità. Dunque, per la prima volta, la Cina ha riconosciuto, in via interpretativa, i mezzi di costituzione e acquisizione di prove come marca temporale e *blockchain*. Il primo caso di assunzione di prove informatiche acquisite con la tecnica della *blockchain* nell'ambito del primo grado di giudizio è stato presentato innanzi alla Corte di Internet di Hangzhou che ne ha confermato l'efficacia probatoria all'interno di un contenzioso civile[107]. A tal proposito, è stato tuttavia precisato che la Corte mantiene un atteggiamento aperto e neutro volto

[103] Giova sottolineare, al riguardo, che la durata media del processo *online* è di 28 minuti ed il termine di conclusione di una causa è di 41 giorni, con una riduzione rispettivamente di tre quinti e metà del tempo rispetto a un processo tradizionale. Il tasso di accettazione della sentenza di primo grado è del 98,59%.

[104] "云法通" "可信时间戳" "存证云" "安存语录""e签宝" 为第三方电子数据平台.

[105] 2018年9月6日最高院发布《最高人民法院关于互联网法院审理案件若干问题的规定》，9月17日实施。Le Disposizioni offrono per la prima volta una specifica interpretazione giudiziaria dei casi presentati alla corte di Internet.

[106] "互联网法院审理案件若干问题的规定" 第11条: "当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认"。

[107] Cfr. http://www.sohu.com/a/240775254_100130948.

a valutare, caso per caso, tutti gli elementi ai fini della decisione[108], lasciando con ciò intendere che il primo caso giurisprudenziale sulle prove informatiche ottenute con la tecnologia *blockchain* non possa costituire un precedente giudiziario vincolante.

Dal quadro appena tratteggiato, emerge come la tecnologia della *blockchain*[109] abbia avuto un ruolo centrale nel permettere di acquisire le prove informatiche imponendo una nuova prospettiva nella prassi giudiziaria[110].

Alla base della spinta propulsiva verso le nuove tecnologie, vi sono i sostenitori della costruzione di un'alleanza *blockchain* per tutta la rete di tribunali a livello azionale[111].

Nonostante gli entusiasmi, non mancano alcune voci che invitano alla prudenza evidenziando le criticità della tecnologia *blockchain*[112].

Tra i difetti della *blockchain* si annoverano l'impossibilità di garantire l'autenticità dei

[108] Ivi. Così dichiarava la vice presidente Wang Yifei della Corte di proprietà intellettuale presso l'Alta corte popolare della Provincia dello Zhejiang.

[109] La *blockchain* è essenzialmente una struttura di archiviazione di dati che ricorre ad un algoritmo distribuito e decentralizzato così da creare diversi valori di memorizzazione in più nodi, con l'effetto di migliorare l'integrità e l'immodificabilità dei dati. Il cuore della tecnologia di marca temporale, crittografia e *blockchain* è la verifica del valore *hash*. I dati elettronici possono essere calcolati per ottenere un'unica "carta d'identità" non modificabile per garantirne l'integrità (Cfr. https://www.fadada.com/notice/detail-1496.html, 19 settembre 2018). Ogni transazione forma una struttura di dati indipendente, memorizzata in blocco. Il blocco contiene una marca temporale, il numero del blocco precedente, il valore *hash* del blocco precedente, i dati del blocco corrente. La *blockchain* garantisce, attraverso un meccanismo POS (*Proof of Stake*) e DPOS (*Delegated Proof of Stake*), che solo una persona possa produrre e trasmettere lo stesso blocco, e che altre persone possano sincronizzare la copia, senza possibilità di effettuare nessuna modifica. Il tentativo di manomissione dei dati su un blocco implica due operazioni da compiere contestualmente: ricalcolare il blocco corrente e tutti i blocchi successivi e sincronizzare la propria *blockchain* con la maggior parte dei nodi in tutta la rete. Poiché i nodi sulla *blockchain* aumentano costantemente, modificare decine di migliaia di nodi sull'intera rete prima che venga generato il blocco successivo, richiede una potenza di calcolo del nodo superiore della somma di potenza di calcolo di tutti gli altri nodi (Cfr. https://www.jianshu.com/p/8f0906077d73). In tema di *blockchain*, cfr. G. Finocchiaro – C. Bomprezzi, *A legal analysis of the use of blockchain technology for the formation of smart legal contracts*, in *questa Rivista,* 2, 2020, 111 ss.

[110] A questo proposito, giova ricordare che l'art. 9 del MLEC, con riferimento alle prove informatiche, dispone che la loro valutazione da parte del giudice debba avvenire sulla base di alcuni parametri, quali la loro affidabilità, il modo in cui i dati sono stati generati, archiviati o comunicati nonché il modo in cui l'integrità delle informazioni è garantita e in cui il mittente è stato identificato.

[111] Cfr. https://www.8btc.com/article. Secondo tal proposta, ogni tribunale, basandosi sul sistema processuale esistente, costituisce un nodo dell'alleanza della *blockchain* che ha il compito di verificare, firmare e supervisionarsi a vicenda tra più di 3.500 tribunali in Cina. Nella catena dell'alleanza giudiziaria applicata alla struttura gerarchica di corte suprema, provinciale, media, fino alla corte di base, si impiegherebbero tra gli 8 e i 10 minuti per sincronizzare tutti nodi utilizzando il meccanismo del consenso. Per costruire il sistema nazionale di acquisizione di prove informatiche con tecnica di *blockchain*, si calcola che la rete di 3.500 tribunali richiede la configurazione di circa 5.000 *server*. Si prevede un investimento iniziale di circa 20 milioni di yuan, ed un successivo costo annuo di circa 700 mila-10 milioni di yuan. In questo modo, con un modesto investimento, si potrebbe risolvere il problema della fiducia nelle prove informatiche e del controllo giudiziario su di esse, se si affida all'ordinamento giudiziario la direzione della "catena di alleanze" di prove informatiche, così da tutelare anche la sovranità giudiziaria della Cina.

[112] Cfr. http://www.nbd.com.cn/articles/2018-09-10. Il consigliere Xiao Feng dell'Associazione di ricerca giuridica della Bank of China rileva che i fatti del mondo reale non possono essere registrati meramente dalla tecnologia *blockchain*, come nel caso delle controversie concernenti i sinistri assicurativi aerei. In diverse occasioni, sono le registrazioni manipolate sulla catena a provocare il meccanismo di consenso. Il consigliere ritiene che per provare che i fatti siano effettivamente avvenuti, sia necessario verificare le prove documentali tradizionali, i messaggi di dati e le prove materiali.

dati aggiunti fuori dalla *blockchain* e l'incapacità di tenere il passo con la rapida evoluzione tecnologica. Infine, vi sono problemi di protezione dei dati personali e di sicurezza. Richiedendo impianti ad alta tecnologia per assicurare adeguate risorse computazionali, vi è soprattutto il rischio di dispersione, incompletezza o perdita di prove. Inoltre, le prove memorizzate nella piattaforma possono essere falsificate o manomesse e l'arco temporale a cui risale la prova elettronica può essere modificata in base ad una nuova impostazione della macchina, causando perdita di effetti giuridici e così via. A tal proposito, occorre rilevare che lo stesso art. 11 delle Disposizioni non precisa il controllo dello standard sul *software* applicativo e la validazione legale dei mezzi di costituzione e acquisizione delle prove[113].

Un'ulteriore questione critica riguarda la tendenza a concentrare il settore in esame nelle mani di pochi prestatori di firme elettroniche che detengono le tecnologie più avanzate. Ad esempio, la già citata E-Sign (e-签宝), una società di servizi di firme elettroniche fondata nel 2002, è l'unica del settore ad aver ottenuto i tre certificati rilasciati dalla *State Cryptography Administration*: il certificato del modello di dispositivo crittografico commerciale, il certificato di azienda designata per produrre i dispositivi crittografici commerciali, la licenza commerciale per prodotti crittografici. Nel 2018, la società è entrata a far parte dell'alleanza di tecnologie e industrie affidabili. I suoi prodotti alimentano tutti i sistemi domestici, quali *chip*, sistemi operativi, *database*, *middleware* e *file*, capaci di fornire servizi anche a clienti con elevate esigenze di sicurezza, quali *E-government* e alta finanza. Attraverso tale meccanismo di certificazione, una volta valutata l'affidabilità della tecnologia utilizzata, questa viene automaticamente riconosciuta anche alla firma elettronica derivata, senza necessità di una valutazione da parte del giudice.

Tuttavia, lo stretto connubio tra tecnologia e giustizia comporta il rischio di una potenziale ingerenza, in campo giudiziario, dei detentori di competenze tecnologiche. Nell'ordinamento giudiziario, tali soggetti, invece di essere sottoposti a sorveglianza, finiscono per dettare le regole sull'affidabilità, mentre gli interpreti del diritto sono relegati al ruolo di "apprendisti" delle regole tecniche. I protagonisti che partecipano alla redazione di standard nazionali sono le società di *software*. I *service provider* di dimensioni gigantesche hanno propri centri di ricerca e sviluppo e immettono sul mercato nuovi prodotti che vengono in seguito disciplinati dagli interpreti del diritto. La catena di alleanze tra l'apparato giudiziario, centri di valutazione giudiziaria, centri di certificazione e *service provider* presenta pertanto un altissimo grado di interdipendenza al punto di rendere molto difficile districarne le relazioni interne per rivendicare la terzietà e l'indipendenza della giustizia.

5. Questione sulla sovranità del firmatario elettronico

Le criticità connesse all'implementazione della firma elettronica erano ben note al le-

[113] Cfr. https://www.jianshu.com/p/8f0906077d73. È auspicabile che vengano stabilite al più presto norme uniformi per l'acquisizione di prove, comprese regole di implementazione procedurali e tecniche in conformità con le Disposizioni.

gislatore europeo sin dall'inizio della rivoluzione digitale. Difatti, la direttiva 1999/93/CE avvertiva della possibilità di registrazione e copia di dati per creare firme elettroniche che avrebbe potuto «costituire una minaccia per la validità giuridica delle firme elettroniche»[114].

La sicurezza rappresenta le fondamenta su cui regge l'intero impianto normativo e caratterizza, dall'inizio alla fine, il processo delle firme elettroniche. Non solo, la sicurezza riguarda tutta l'infrastruttura della comunicazione e delle transazioni economiche[115]. Da qui l'esigenza che sistemi come quello di PKY, dove i prestatori di certificazione delle firme elettroniche forniscono chiave privata e pubblica, garantiscano un elevato livello di sicurezza. Tuttavia, è altresì cruciale, ad esempio, che il firmatario possa mantenere un esclusivo controllo sui dati utilizzati per la creazione della firma elettronica. In questo scenario, dove l'interesse a tutelare la sicurezza potrebbe porsi in conflitto con quello di protezione dei dati personali, occorre operare un bilanciamento.

In Cina, tale operazione risulta alquanto problematica dal momento che, diversamente da quanto accade nell'Unione europea, la legge cinese sulle firme elettroniche non fa alcun espresso rinvio alla normativa a tutela dei dati personali. Solamente la legge sulla tutela dei diritti dei consumatori della Repubblica Popolare della Cina stabilisce[116] che «l'operatore della piattaforma non può divulgare né vendere i dati personali dei consumatori e deve adottare misure tecniche per impedire la divulgazione o la perdita delle informazioni personali del consumatore"[117]. La stessa legge, però, non prevede disposizioni specifiche relative all'attribuzione di responsabilità al prestatore di servizi[118].

Alla luce del quadro delineato, emerge una differenza, anche culturale, tra il contesto normativo europeo e quello cinese. In Europa, vi è una consolidata disciplina a tutela dei consumatori, sintetizzabile nell'espressione "circolazione sicura dei dati". Al contrario, in Cina, il meccanismo di tutela è stato appena costruito e necessita di un collaudo giurisprudenziale. Per questo motivo appare utile, soprattutto in ottica comparata, formulare alcune considerazioni sul sistema giudiziario cinese, il quale presenta alcune sostanziali differenze con quello italiano. L'analisi comparata dei due sistemi infatti mette in luce l'esistenza di una radicale differenza. In Italia, il processo giudiziario è lento e fondato su un rito processuale ormai consolidato, in cui la "nuova" norma

---

114 Considerando 18 della direttiva 99/93/CE.

115 Si noti come nei servizi di *E-government*, i governi designano le aziende preposte alla ricerca e allo sviluppo di prodotti sicuri nell'ambito del sistema crittografico a chiave pubblica, e confidano nella affidabilità della firma elettronica da questi fornita (ad esempio, in Cina, l E-sign).

116 "中华人民共和国消费者权益保护法" 第二十九条 经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。

经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

117 Art. 29 della legge cinese sulla tutela dei diritti dei consumatori.

118 Si noti tuttavia che tale vuoto normativo viene colmato dalla legge cinese sul commercio elettronico con gli artt. 23, 25, 32, 79 e 87.

deve armonizzarsi con l'ordinamento giuridico esistente. In Cina, invece, il processo è improntato all'innovazione ed è rimesso alla valutazione del giudice speciale: l'intero impianto giuridico sembra doversi adeguare alla legge cinese sulle firme elettroniche eretta sulla base dell'architettura delineata dal modello UNCITRAL e non il contrario. Il principio del giudice naturale, tutelato dalla Costituzione italiana[119], si contrappone all'istituzione del giudice cinese nato nel 2017 per la giurisdizione delle controversie *online*. Considerando che i rapporti negoziali *online* sono destinati a crescere, ci si domanda se il tribunale "ordinario" cinese sia contestualmente destinato a scomparire, sostituito dalla Corte di Internet.

In conclusione, le questioni di cui si è dato conto nel presente contributo sembrano potersi ricondurre al tema della sovranità. Un tempo l'uomo era sovrano della propria mano, la mano esprimeva la sovranità dell'uomo capace di agire. Oggi, l'impianto giuridico sulle firme elettroniche riflette una separazione tra la mano e il corpo, creando un surrogato tecnologico che assicura il coordinamento tra la mano e la mente. Nel momento in cui la legge vieta al prestatore di servizi di firma elettronica qualificata di copiare la chiave privata, ammette la possibilità che quest'ultimo la copi. La mano che non si stacca dal corpo è la vera e unica garanzia della propria sovranità, mentre la garanzia del surrogato tecnologico è imposta dal legislatore che deve misurarsi con il potere tecnologico esercitando il potere coercitivo sanzionatorio. A tale proposito, emerge una certa debolezza del legislatore cinese. Il *vulnus,* creato dall'adozione da parte del legislatore italiano dello strumento cognitivo del modello e della metafora per la disciplina delle firme informatiche, si palesa nell'inapplicabilità dell'istituto ideato per la tutela della firma autografa. Le firme informatiche non sono come la firma autografa, proprio in ragione della progressiva perdita della sovranità dei titolari di queste firme. Questi sono trascinati nel mondo virtuale dove la firma si compone di numeri, codici, segni irriconoscibili e dove spesso il sottoscrittore perde consapevolezza dell'atto stesso della firma. Una firma autografa è riconoscibile dal suo autore che, in caso di falsificazione della firma, può avvalersi dell'istituto del disconoscimento. L'onere di presentare l'istanza di verificazione e produrre le prove grava sulla parte che intende fare valere la firma. In mancanza di tale istanza oppure di esito positivo, il documento firmato non può essere utilizzato nel processo. Diversamente, per le firme informatiche, non potendo essere riconosciute ad occhio nudo dai propri titolari, non è possibile ricorrere all'istituto della verificazione di cui all'art. 216 c.p.c. Per ovviare a tale problema è stata introdotta la presunzione, ai sensi dell'art. 20, c. 1-*ter*, CAD, dell'utilizzo del dispositivo in capo al titolare del medesimo. Tuttavia, ciò comporta un aggravamento dell'onere della prova in capo al titolare del dispositivo di firma (si pensi, ad esempio, al caso di furto o di smarrimento di questo).

In Cina, gli effetti giuridici delle firme elettroniche sono riconosciuti in via automatica in presenza dei requisiti previsti dalla legge e, di fronte allo strapotere dei prestatori delle firme elettroniche, ci si domanda quale sia il mezzo di cui potrebbe disporre il titolare del dispositivo nell'ipotesi di copia della chiave privata, oppure di creazione o manomissione di prova da parte del certificatore. L'evoluzione del diritto civile attorno

[119] Art. 25, c. 1, Costituzione italiana: «Nessuno può essere distolto dal giudice naturale precostituito per legge».

al principio cardine della circolazione di beni permette che questi circolino inarrestabilmente ad un ritmo sempre più veloce. Contemporaneamente, l'uomo accetta – spesso inconsapevolmente – di perdere la propria sovranità, travolto dalla crescita esponenziale dei prodotti della potente macchina dei *Big Data* e dell'intelligenza artificiale. L'uomo alimenta la macchina immettendovi i propri dati, finendo però per essere privato dalla stessa della propria indipendenza e della propria dignità. Le informazioni che, mai come oggi, l'uomo concede volontariamente (o meno) ai *service provider*, fanno sorgere sempre più robot di intelligenza artificiale, che torneranno a spogliarlo fino all'ultimo velo della sua essenza.

La difesa della democrazia pluralista dinanzi alla paura e alla disinformazione*

Juan Francisco Sánchez Barrilao

Abstract

Il paper tratta della paura come fattore politico e di esercizio del potere, che finisce con il condizionare l'esercizio della democrazia stessa; e all'ombra di questa, la trascendenza costituzionale che tutto ciò determina quando la paura è manipolata al fine di instaurare forme di dispotismo o determinare un'involuzione democratica. Ai fini dello studio di questo fenomeno, l'autore analizza, in primo luogo, come la società si caratterizzi in funzione della paura, e soprattutto il ruolo che in questo contesto gioca la disinformazione attraverso Internet e i social network; in seguito, come la democrazia affronti al giorno d'oggi una politica compromessa dalla paura, dalla post-verità e dalla disinformazione, così come l'apparizione di nuovi conflitti e le risposte illiberali che sono state a lungo postulate; inoltre, come affrontare costituzionalmente, dalla prospettiva della Spagna, la difesa della democrazia pluralista di fronte alla paura e la sua manipolazione in relazione alla sicurezza, al patriottismo costituzionale, oltre ad altre forme di contenimento e promozione, tra cui la nuova "Procedura di azione contro la disinformazione"; e per finire, ovviamente, si proporranno alcune considerazioni conclusive che discendono da un'analisi critica di questa proposta.

The paper deals with fear as a factor in politics and the exercise of power, which ends up conditioning the democratic process; and in the shadow of this, the constitutional transcendence that all this determines when fear is manipulated in order to establish forms of despotism or bring about a democratic involution. With a view to studying this phenomenon, the author analyzes, firstly, how society is characterized by fear, and above all the role that disinformation plays in this context through the Internet and social networks; later, how democracy nowadays faces a politics compromised through fear, "post-truth", and disinformation, as well as the appearance of new conflicts and the illiberal responses that have long been postulated; moreover, how to constitutionally address, from the perspective of Spain, the defense of pluralist democracy in the face of fear and its manipulation concerning security, constitutional patriotism, as well as other forms of containment and promotion, including the new "Action plan against disinformation"; and to finish, of course, some conclusive considerations will be proposed on the bases of the critical analysis of this proposal.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Sommario

1. Introduzione: bugie, paura e disaffezione Costituzionale. - 2. Società della paura e post-verità - 2.1. Dal mero rischio alla paura. - 2.2. Internet, post-verità e società della paura. - 3. Democrazia, post-verità e paura. - 3.1. Politica e paura. - 3.2. Conflitti e democrazia illiberale. - 4. Affrontare la paura dalla prospettiva costituzionale dinanzi alla disinformazione. - 4.1. Sicurezza e democrazia pluralista. - 4.2. Misure per il contenimento della disinformazione e in promozione della democrazia: la "procedura di attuazione contro la disinformazione". - 5. Considerazioni conclusive.

Keywords

democrazia pluralista – società della paura – fake news – post-verità – Internet

1. Introduzione: bugie, paura e disaffezione Costituzionale

L'era Trump inizia ormai a sgretolarsi[1], anche se bisogna vedere cosa ne sarà della sua eredità politica (il "Trumpismo") in un sistema democratico, quello americano (ma non solo), analizzandolo con attenzione. Sebbene Biden abbia ricevuto circa 75.000.000 di voti, Trump ha raggiunto più di 70.500.000 dopo una prima e controversa elezione nel 2016 (conquistandone, da allora, altri 6 milioni), un intero mandato di governo con una pandemia in corso, compresi gravi scontri sociali, e una nuova campagna e un processo elettorale caratterizzato da "bufale", provocazioni e intimidazioni; per non parlare del rifiuto iniziale di Trump di accettare la vittoria di Biden, basato su una presunta frode elettorale di massa. Senza dubbio, questa è stata la principale notizia veicolata dai media in gran parte del mondo durante i primi giorni di novembre 2020, dinanzi alla quale il COVID-19 sembrava passare in secondo piano.

Anche in Spagna i media si sono concentrati sui risultati elettorali degli Stati Uniti, insieme, ovviamente, all'aggravarsi della seconda ondata della pandemia. Ma entrambe le notizie sono state accompagnate per alcuni giorni dalla controversa pubblicazione ufficiale di una "Procedura di azione contro la disinformazione", approvata quasi un mese prima dal Consiglio di sicurezza nazionale il 6 ottobre 2020[2], accompagnata dalla denuncia alla potenziale censura e conseguente limitazione alla libertà di espressione e informazione (art. 20 della Costituzione spagnola, in seguito "CE") da parte del governo spagnolo; un'ulteriore discussione sulla limitazione dei diritti è stata aperta in Spagna durante questa fase segnata da allarmismo e COVID-19[3], quando la coalizione

[1] Sulla configurazione di un'*era Trump*, e (precisamente) in relazione al tema dei social network, cfr. J.F. Sánchez Barrilao, *El Internet en la era Trump: aproximación constitucional a una nueva realidad*, in *Estudios en Derecho a la Información*, 9, 2020, 50 ss.

[2] *Boletín Oficial de Estado*, 5 novembre 2020, 292, 96673 ss.

[3] RRDD 463/2020, 14 marzo, e 926/2020, 25 ottobre, che hanno dichiarato lo stato di allarme per la gestione della situazione di crisi sanitaria causata da COVID-19, prima, e poi per contenere la diffusione della pandemia causate dal SARSCoV-2. Rispetto al primo, v. J.F. Sánchez Barrilao – E. Guillén López, *La crisis sanitaria originada por el COVID-19, 2020 y el Real Decreto 463/2020 declarando el estado de alarma para*

di governo è stata accusata di voler controllare l'informazione nei media e nelle reti digitali, e così distorcere la democrazia e il sistema costituzionale spagnolo. Tuttavia, la questione è sembrata sgonfiarsi nel giro di pochi giorni alla luce dell'approvazione a Bruxelles di questo piano.

Si tratta, tuttavia, di emozioni e paure; di disturbi dell'umore individuale e collettivo non tanto di fronte a pericoli certi o sconosciuti, o potenziali perdite di ciò che si possiede o si possa (o si creda di) arrivare ad avere[4], ma in funzione della possibilità di manipolare quanto sopra, e in particolare amplificando artificialmente l'idea di privazione, di perdita di ciò che si ha (o si può o si crede di avere), e quindi promuovere il confronto, oltre la rabbia, l'odio e persino la vendetta[5]. Si tratta, quindi, della paura come fattore politico e di esercizio del potere[6], che finisce con il condizionare l'esercizio della democrazia stessa; e all'ombra questa, la trascendenza costituzionale che tutto ciò determina quando la paura viene manipolata al fine di instaurare forme dispotismo[7] o determinare un'involuzione democratica[8]. La paura, quindi, come catalizzatore della ritrattazione democratica e costituzionale.

E ciò comporta che la paura, e sotto il suo alone, la frustrazione, la rabbia e l'odio, vengano strumentalizzati per promuovere un disagio e un'irritazione culturale, sociale e politica che nasce spontaneamente[9] dall'incapacità mostrata di fronte a sfide, difficoltà e incertezze che ci perseguitano da anni[10], e che oggi con la pandemia stanno aumentando ancora di più. In questo senso, e rispetto a Trump (di nuovo), Nussbaum ha analizzato la manipolazione della paura e del risentimento che il Presidente uscente ha promosso negli Stati Uniti; di come, appellandosi all'immigrazione e all'insicurezza, al multiculturalismo e al terrorismo, alla globalizzazione e al trasferimento di industrie, ecc., Trump abbia ottenuto un consenso popolare sufficiente a raggiungere ed esercitare democraticamente il potere al fine di promuovere politiche costituzionalmente recessive; di come la paura e la frustrazione vengano fatalmente e artificialmente potenziate e strumentalizzate a beneficio politico dei leader che, come Trump[11], ripudiano

abordarla, in Aa. Vv., *Los derechos fundamentales ante las crisis económicas y de seguridad en un marco constitucional fragmentado*, Cizur Menor, 2020, 529 ss.

[4] Di notevole interesse, sul tema della paura e dell'ignoranza, v. K. Riezler, *The Social Psychology of Fear*, in *American Journal of Sociology*, 49(6), 1944 489 ss.

[5] Cfr. C.R. Sunstein, *La última mitología. El mundo según StarWars*, Barcellona, 2017, 134-135 e 143-145.

[6] Per esempio, F. Cerrato, *Forme e governo della paura: mutamenti di paradigma concettuali e crisi delle istituzioni di controllo*, in *Governare la paura. Journal of interdisciplinary studies,* 2012.

[7] Sulla paura come elemento identificativo del dispotismo e contro la democrazia stessa, cfr. J. Keane, *Miedo y democracia*, in *Pasajes: Revista de Pensamiento Contemporáneo*, 8, 2002, 13 ss.

[8] O al contrario, M.A. Graber - S. Levinson - M. Tushnet, *Constitutional Democracy in Crisis?*, Oxford, 2018.

[9] Di particolare interesse risulta, al principio della passata decade, S. Hessel, *¡Indignaos!*, Barcellona, 2011.

[10] J. F. Sánchez Barrilao, *La constitucionalización de la integración regional europea. ¡Más Europa!: de vuelta a una constitución para Europa, ante la situación de crisis de la Unión*, in *Estudios de Deusto*, 60(2), 2012, spec. 78 ss.

[11] M. C. Nussbaum, *La monarquía del miedo (Una mirada filosófica a la crisis política actual)*, Barcellona, 2019; di interesse anche W. Davies, *Estados nerviosos (Cómo las emociones se han adueñado de la sociedad)*, México, 2019. E soprattutto, sulla retrocessione democratica e costituzionale che ha comportato il mandato di Trump, cfr. J. Havercroft – A. Wiener – M. Kumm – J.L. Dunoff, *Donald Trump as global constitutional*

valori che ritenevamo democraticamente conquistati, e nell'impulso di una crescente "disaffezione" costituzionale[12]. In altre parole, ciò significa istigare il malcontento, l'insoddisfazione e la delusione per il sistema democratico-costituzionale[13]; anche la stessa promozione del distacco e degli interrogativi di carattere ideologico sui fondamenti del sistema costituzionale pluralista[14].

Non a caso, la scarsa distribuzione della ricchezza generata dallo sviluppo tecnologico e dalla globalizzazione (accentuata dalla fragilità delle politiche sociali di fronte a quest'ultima e dalla crisi economica che ha generato), insieme alla debolezza mostrata dal costituzionalismo di fronte agli stessi, oltre ai conflitti esistenti tra élite globalizzate e localizzate, così come le identità (sempre più estreme), hanno costituito il presupposto di una tempesta perfetta per il costituzionalismo democratico-pluralista: l'impulso interno, dal pluralismo stesso, dei movimenti sociali e politici di profonda insoddisfazione per il sistema, e allo stesso tempo la sua articolazione ideologica in gruppi critici non solo nei confronti delle suddette debolezze costituzionali, ma anche in relazione ai valori e agli elementi essenziali su cui si articola il costituzionalismo contemporaneo, per quanto questi movimenti si presentino rispettosi della democrazia e della Costituzione. Non si tratta, quindi, di semplici gruppi considerati anti-sistema[15] o populisti[16] in risposta a deficit costituzionali e democratici, ma di: movimenti che, senza essere violenti, si integrano in un modo quasi naturale in un sistema politico pluralista, ma che al loro interno, nei loro discorsi e nelle loro azioni esprimono un evidente spirito di disaffezione, rifiuto e reazione (battuta d'arresto) nei confronti del pluralismo[17]; gruppi ostili ai presupposti di base dei sistemi democratici e costituzionali, nonché promotori e/o manipolatori di una paura con cui conciliare le affinità popolari con e di fronte agli altri, fermo restando che ne difendono principi e/o contenuti, ribadiamo), democratico e costituzionale. Sono collettivi, quindi sono presentati come formalmente rispettosi della democrazia, ma sostanzialmente contrari alla comprensione pluralistica dello Stato costituzionale e democratico raggiunto[18].

---

breaching experiment, in *Global Constitutionalism*, 7(1), 2018, 1 ss.

[12] M. Barberis, *L'uomo della folla: la filosofia del diritto di Donald Trump*, in *Ragion Pratica*, 51, 2018, 411 ss.

[13] Nella sua formalizzazione, realizzazione e sviluppo, e dinanzi al suo ideale utopico e la limitata realtà del suo modo di esprimersi. V. G. Lipovetsky, *La sociedad de la decepción (Entrevista con Bertrand Richard)*, Barcellona, 2008. V. anche M. A. Presno linera, *Partidos políticos y movimientos ciudadanos en la sociedad del riesgo y la desconfianza*, *Fundamentos: Cuadernos monográficos de teoría del estado, derecho público e historia constitucional*, 8, 2014, 213 ss.; e O. Sánchez Muñoz, *Los partidos y la desafección política: propuestas desde el campo del Derecho constitucional*, in *Teoría y Realidad Constitucional*, 35, 2015, 413 ss.

[14] Cfr. J. F. Sánchez Barrilao, *Inteligencia y seguridad como objeto constitucional (El CNI y la comunidad de inteligencia ante los nuevos retos de la sociedad del riesgo)*, Madrid, 2019, spec. 324-325.

[15] Cfr. J. Alguacil Gómez, *Nuevos movimientos sociales: nuevas perspectivas, nuevas experiencias, nuevos desafíos*, in *Polis: Revista Latinoamericana*, 2007, 17.

[16] Come movimenti più interessati all'elitarismo e alla politica rappresentativa (in molti casi), che all'esposizione di proposte ideologiche. Di questo avviso, D. Vittori, *Re-conceptualizing populism: Bringing a multifaceted concept within stricter borders*, in *Revista Española de Ciencia Política*, 44, 2017, 43 ss.; o M. Manetti, *Costituzione, partecipazione democratica, populismo*, in *Rivista AIC*, 3, 2018, 377 ss.

[17] Distingue espressamente tra semplici populismi e altri movimenti contro le minoranze e le libertà S. Dion, *La democracia y los derechos universales frente al auge del populismo*, in *Cuadernos Electrónicos de Filosofía del Derecho*, 39, 2019, 26 ss.

[18] Sul punto, P. Ridola, *Il costituzionalismo e lo Estato costituzionale*, in Aa. Vv. *Passato, presente e futuro del*

Ai fini dello studio di questo fenomeno e della ricerca di risposte allo stesso da un punto di vista costituzionale, è necessario analizzare, in primo luogo, come la società si sia caratterizzata in funzione della paura, e soprattutto il ruolo che in questo contesto gioca la disinformazione attraverso Internet e i social network; in seguito, come la democrazia affronti al giorno d'oggi una politica compromessa da dette paure, post-verità e disinformazione, così come l'apparizione di nuovi conflitti e le risposte illiberali che sono state a lungo postulate; inoltre, come affrontare costituzionalmente, dalla prospettiva della Spagna, la difesa della democrazia pluralista di fronte alla paura e la sua manipolazione in relazione alla sicurezza, al patriottismo costituzionale, oltre ad altre forme di contenimento e promozione, tra cui la già citata "Procedura di azione contro la disinformazione"; e per finire, ovviamente, si proporranno alcune considerazioni conclusive che discendono da un'analisi critica di questa proposta.

2. Società della paura e post-verità

2.1. Dal mero rischio alla paura

Dalla seconda metà del secolo scorso, la società si è caratterizzata per la capacità dell'uomo di generare danni all'umanità tali che, al momento di realizzarsi, sembrano di difficile o impossibile rimedio. Rischi che agiscono congiuntamente e dialetticamente con altri, creandone così di nuovi; l'umanità convive con questi rischi e li gestisce, cercando di limitarli e/o contenerli[19]. Un rischio che a sua volta entra in contatto con il progresso tecnologico e la globalizzazione, finendo con l'assumere le sembianze di motore e di amplificatore. La tecnologia ha permesso di affrontare sfide e trovare soluzioni a problemi e bisogni dell'umanità, così mettendola, tuttavia, ancora più in pericolo[20]; e quindi il progresso (inteso come evoluzione, avanzamento, miglioramento, sviluppo e beneficio graduale), che prende forma grazie all'attività scientifica e tecnologica, si collega causalmente, e nonostante tutto, con lo stigma della generazione di rischi[21]. Non senza motivo, e molto prima della rivoluzione tecnologica, è stato quindi espresso timore o sospetto che, sotto forma di mito (Prometeo), arriva ai nostri giorni (il moderno Prometeo)[22]; un timore o sospetto che, al di là dei pregiudizi[23], adotta nuove forme come oggi richiedono l'intelligenza artificiale[24] e le trasformazioni che va

costituzionalismo e dell'Europa (Atti del Convegno, Roma 11-12 maggio 2018), Milano, 2019, 83 ss.

19 U. Beck, *La sociedad del riesgo (Hacia una nueva modernidad)*, Barcelona, 1998.

20 In generale, v. J. Esteve Pardo, *El desconcierto del Leviatán (Política y Derecho ante las incertidumbres de la Ciencia)*, Madrid, 2009.

21 J. Gray, *Nature Bites Back*, in Aa. Vv., *The Politics of Risk Society*, Cambridge, 1998, 44 ss.

22 F. Salmoni, *Le norme tecniche*, Milano, 2001, 8-15.

23 Anche, ma non solo, sulla questione tecnologica, L. Mumford, *El mito de la máquina I: Técnica y evolución humana*, La Rioja, 2010; e Id., *El mito de la máquina II: El pentágono del poder*, La Rioja, 2011. Sulla tecnologia come minaccia e opportunità, S. Rodotà, *El derecho a tener derechos*, Madrid, 2014, 69 ss.

24 Su tutti, N. Bostrom, *Superintelligence: Paths, Dangers, Strategies*, Oxford, 2014.

a determinare (ad esempio nel mercato del lavoro)[25], o si pensi ai big data e alla possibilità di controllo sociale che ne discende[26], per non parlare del cambiamento climatico e dell'emergenza ad esso connessa[27].

Il rischio e la paura della tecnologia acquistano quindi un certo grado di trascendenza dinanzi al potere pubblico e al diritto[28]. Vengono postulati principi che, di fronte al futuro e alla paura, cercano di evitare o mitigare rischi al fine di prevenire danni, conseguenze gravi di difficile, o impossibile e chissà inutile, soluzione (come quelli di responsabilità[29] e precauzione[30]); e infine limitare le attività che implicano una certa dimensione tecnologica, soprattutto per quanto riguarda le future garanzie dei diritti fondamentali e della dignità in caso di potenziali violazioni degli stessi[31].

Quanto alla globalizzazione, questa non solo amplifica il precedente rischio tecnologico (si pensi, ad esempio, al cambiamento climatico)[32], ma genera anche nuove dimensioni di rischio meno legate all'idea di disastro o catastrofe (anche se ciò non può escludersi, come è avvenuto nel caso della pandemia da COVID-19), così portando alla manifestazione di fenomeni che generano pericoli politici, economici e/o sociali[33]. Senza perdere di vista l'universalizzazione dei valori sociali, delle manifestazioni culturali e del Diritto (gli stessi diritti umani) che la globalizzazione ha comportato[34], quest'ultima ha finito per "stressare" la sovranità e il potere degli Stati (e dei loro cittadini) [35], in funzione dell'attività di quei soggetti privati che impongono i propri interessi all'ombra di un'economia e un mercato transnazionale[36]; questa tensione ha generato, a sua volta e in maniera contraddittoria[37], risposte endogene alla globalizza-

[25] J. F. Sánchez Barrilao, *Derecho constitucional, desarrollo informático e inteligencia artificial: aproximación a la propuesta del Parlamento Europeo a favor de una regulación sobre robótica*, in Aa. Vv. *Retos jurídicos por la sociedad digital*, Cizur Menor, 2018, 48-49.

[26] W. Hoffmann-Riem, *Big data. Desafíos también para el Derecho*, Cizur Menor, 2018.

[27] S. Borrás Pentinat, *La responsabilidad soberana para fortalecer la seguridad climática*, in Aa. Vv. *Retos del Derecho ante las nuevas amenazas*, Madrid, 2015, 327 ss.

[28] Persino cercando legittimità nel processo decisionale sulla definizione della tecnologia; cfr. J. F. Sánchez Barrilao, *Sobre la Constitución normativa y la tecnología*, in *Revista de la Facultad de Derecho de la Universidad de Granada*, 8, 2005, 257 ss.

[29] Cfr. J. Jonas, *El principio de responsabilidad (Ensayo de una ética para la civilización tecnológica)*, Barcellona, 2ª ed, 2004.

[30] Sul tema della paura, v. C. R. Sunstein, *Leyes de miedo (Más allá del principio de precaución)*, Buenos Aires, 2009.

[31] Cfr. S. Rodotà, *El derecho a tener derecho,* cit., 287 ss.

[32] U. Beck, *¿Qué es la globalización? (Falacias del globalismo, respuestas a la globalización)*, Barcellona, 2002, in particolare 141 ss.

[33] Cfr. M.L. Lanzillo, *Rischi sociali e domande di sicurezza*, in *Governare la paura. Journal of interdisciplinary studies*, 2015.

[34] V. A. De Julios Campuzano, *La globalización ilustrada: ciudadanía, derechos humanos y constitucionalismo*, Madrid, 2003.

[35] M. Stolles, *Trayectoria del Estado constitucional con la perspectiva de la globalización*, insieme a A. Paulus, *El Derecho constitucional de la globalización*, Madrid, Fundación Coloquio Jurídico Europeo, 2013, 23 ss.

[36] Tra gli altri, J. E. Faria, *El Derecho en la economía globalizada*, Madrid, Trotta, 2001; M. L. Salvadori, *Democrazie senza democrazia*, Roma-Bari, 2011; o M. R. Ferrarese, *Promesse mancate (Dove ci ha portato il capitalismo finanziario)*, Bologna, 2017.

[37] A. Giddens, *Un mundo desbocado*, Madrid, 2000.

zione rinvenendosi la sua dimostrazione nel fondamentalismo[38]. Tra le diverse forme di ciò, evidenziando quella nazionalista, invocando l'idea di tornare ad uno stato forte (e con esso, alla cittadinanza statale) come risposta "ri-sovrana" alla globalizzazione e all'impotenza che questa[39], insieme all'integrazione europea (più economica che sociale)[40], fa sì che ampi strati della popolazione si sentano lontano dal sistema democratico (e sociale)[41].

Ma è proprio in funzione di ciò che sorgono nuove frustrazioni e paure, che si esprimono nei conflitti tra alcune élite che, da un lato, prosperano grazie alla globalizzazione, e altre, dall'altro lato, che rimangono ancorate alla dimensione locale[42]; un conflitto diverso da quello tradizionale "tra classi", in quanto delocalizzato e irrisolvibile dalla tradizionale considerazione dello stato sociale (essendo per definizione delimitato territorialmente, e in crisi per effetto della globalizzazione)[43], per non parlare della graduale scomparsa della classe media (baluardo del precedente modello sociale) in questo contesto[44]. E anche rispetto agli "altri", gli immigrati, che hanno cessato di essere oggetto di promozione e riconoscimento[45], per diventare oggetto di paura, frustrazione, rabbia e odio in seguito ai menzionati processi di radicalizzazione e confronto sociale e identitario[46].

Ciò che avviene, infatti, è che la dimensione psicologica delle identità[47] valorizza proprio quelle che si fondano più su elementi soggettivi e sentimentali, che quelle che hanno carattere astratto e/o razionale; e così via per quanto riguarda sentimenti o percezioni di paura, frustrazione, incertezza, svalutazione e/o emarginazione. Non è solo, quindi, una conseguenza del fatto che questi sentimenti esaltino determinate identità, ma la circostanza che le rendano più facili da promuovere, raccogliere e manipolare, come la loro stessa radicalizzazione, poiché fanno appello più alla percezione e ai sentimenti (negativi), che alla ragione e alla riflessione, che risultano essere sempre scomodi e costosi. È così che la paura diviene una sorta di ariete per la radicalizzazione

---

38 Sul punto, P. Häberle, *El fundamentalismo como desafío del Estado constitucional: consideraciones desde la ciencia del Derecho y de la cultura*, in *Retos actuales del Estado constitucional*, Oñati, 1996, 133 ss.

39 V. G. Allegri – A. Sterpa – N. Viceconte (a cura di), *Questioni costituzionali al tempo del populismo e del sovranismo*, Napoli, 2019.

40 Per a, J. H. H. Weiler, *Descifrando el ADN político y jurídico de la integración europea: un estudio exploratorio*, in *Revista Española de Derecho Constitucional*, 96, 2012, 13 ss.

41 Cfr. J. F. Sánchez Barrilao, *Unión Europea y globalización: reivindicando una Europa de los ciudadanos*, in Aa. Vv. *Estudios en homenaje al Profesor y Magistrado Luis Ortega Álvarez*, Cizur Menor, 147 ss. 2016; e Id., *Constitucionalismo, (neo)crisis del Estado social e integración europea*, in Aa. Vv. *Constitución e Integración Europea. Forma política, gobernanza económica, organización territorial*, Madrid, 2017, 143 ss. V. anche M. G. Rodomonte, *¿Populismos y soberanismos versus Unión Europea?*, in *Revista de Derecho Político*, 106, 2019, 287 ss.

42 Z. Bauman, *La globalización (Consecuencias humanas)*, Madrid, 2017.

43 C. De Cabo Martín, *Constitucionalismo del Estado social y Unión Europea en el contexto globalizador*, in *Revista de Derecho Constitucional Europeo*, 11, 2009, 17 ss.

44 C. Guilluy, *No Society. El fin de la clase media occidental*, Barcellona, 2019.

45 Cfr. J. Habermas, *La inclusión del otro. Estudios de teoría política*, Barcellona, 1999.

46 V. A. Kaya, *Populismo e inmigración en la Unión Europea*, in *Anuario CIDOB de la Inmigración*, 2017, 52 ss.

47 Sull'identità come processo psichico (percezione) di appartenenza sociale, cfr. A. Von Bogdandy, *Identidad constitucional. Exploración de un fenómeno ambiguo con ocasión de la política de identidad europea de lege data y* lege ferenda, in *Revista Española de Derecho Constitucional*, 75, 2005, 13 ss.

culturale, sociale e politica di alcuni contro altri, specialmente per coloro più frustrati e sensibili rispetto alle incognite dei cambiamenti e all'insicurezza che oggi dilagano (alla perdita reale o potenziale, come indicato all'inizio di queste pagine); e alla sua ombra, la "viralizzazione" del confronto, l'"accelerazione" dell'odio e persino il dilagare della violenza[48].

2.2. Internet, post-verità e società della paura

Dal progresso innescato dalla Guerra Fredda è nato Internet[49] che, dopo uno sviluppo autonomo e fiducioso, al giorno d'oggi, ormai consolidato quale principale[50] rete di comunicazione, rivela il suo lato meno "amichevole". Certo, non perché prima questo lato non lo avesse; è proprio questo, e dopo una fase di scoperte (dovute al nuovo spazio virtuale di conoscenza, dibattito e riflessione collettiva)[51], ci viene ora presentato come un efficiente strumento di manipolazione e inganno attraverso bugie e disinformazione sotto forma di post-verità[52], oltre a paura, frustrazione, rabbia e odio[53]. Viene così mostrata la contraddittoria e complessa natura di Internet, che viene rivendicato come spazio virtuale e discreto di alterazione ideologica, così alterando artificialmente lo sviluppo libero e plurale dei processi democratici[54]; anche per promuovere la radicalizzazione più esecrabile e violenta (terrorismo, ma non solo)[55].
Esempi di quanto sopra, a livello politico e costituzionale, sono stati il referendum sulla Brexit o le elezioni americane del 2016 e del 2020 con Trump; non solo perché le rispettive campagne hanno sfruttato i social network come strumento di comunicazione politica diffondendo disinformazione, menzogne e rancore nei discorsi e

[48] V. F. Arteaga, *De las sociedades inseguras, sus miedos y sus odios*, in *Blog Análisis y Reflexiones sobre Política Internacional (Real Instituto Elcano)*, 2 ottobre 2017.

[49] Su tutti, K. Hafner – M. Lyon, *Where Wizards Stay Up Late (The Origins of the Internet)*, New York, Touchstone, 1998.

[50] Per esempio, A. Aguilar Calahorro, *El derecho fundamental a la comunicación 40 años después de su constitucionalización: expresión, televisión e internet*, in *Revista de Derecho Político*, 100, 2017, 405 ss.

[51] J. F. Sánchez Barrilao, *El futuro jurídico de internet: Una aproximación constitucional a la neutralidad de la red*, in *Revista de Derecho Constitucional Europeo*, 26, 2016.

[52] V. P. Valadier, *La posverdad, peligro para la democracia*, in *Revista de Fomento Social*, 72(2), 2017, 297 ss.; F. Aznar Fernández-Montesinos, *El mundo de la posverdad*, in *Cuaderno de Estrategia*, 197, 2018, 21 ss.; e G. Martínez Díaz, *La posverdad y el resquebrajamiento del orden liberal*, in *Documento de Opinión (ieee.es)*, 93, 2018, 441 ss.

[53] V. M. A. Moretón Toquero, *El «ciberodio», la nueva cara del mensaje de odio: entre la cibercriminalidad y la libertad de expresión*, in *Revista Jurídica de Castilla y León*, 27, 2012, 3 ss.; e F. Miró Llinares, *Taxonomía de la comunicación violenta y el discurso del odio en Internet*, in *IDP: Revista de Internet, Derecho y Política*, 22, 2016, 93 ss.

[54] V. E. Kaufman, *The social media, the mass media, violence and democracy. The arena for institutional weakening and citizens lack of confidence*, in *Derecom*, 25, 2018. V. anche P. Ciarlo, *Democrazia, partecipazione popolare e populismo al tempo della rete*, in *Rivista AIC*, 2, 2018, 6 ss.; G. Fioriglio, *Post-verità, paura e controllo dell'informazione: quale ruolo per il diritto?*, in *Governare la paura. Journal of interdisciplinary studies*, 2019, 105 ss.

[55] Per esempio, M. A. Cano Paños, *Odio e incitación a la violencia en el contexto del terrorismo islamista: Internet como elemento ambiental*, in *Indret: Revista para el Análisis del Derecho*, 4, 2016, 1 ss.; o M. R. Torres Soriano, *El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato*, in *Cuaderno de Estrategia*, 197, 2018, 197 ss.

nei messaggi elettorali, ma anche perché la tecnologia informatica è stata utilizzata al servizio della manipolazione psicologica dell'elettorato, e per farlo incitando (in modo personalizzato tramite l'identificazione dei profili) le fobie proprie degli utenti (Cambridge Analytica)[56]. Dalla rivendicazione di Internet come nuova dimensione del diritto nei sistemi costituzionali al fine di approfondire nuove possibilità partecipative e promozionali per la cittadinanza[57], si è materializzato un certo sospetto per le democrazie pluraliste in funzione della manipolazione e del dibattito che ne scaturisce[58]; ciò è dovuto alla ragionata implementazione da parte di terzi dei contenuti che circolano su Internet, nonché alla posizione predominante che alcune piattaforme occupano nel mercato digitale[59] che, in sostanza, beneficiano (almeno) del dibattito a livello sociale già menzionato[60].

La paura si estende così oltre il rischio tecnologico, connettendosi con altre realtà in cui crescono o sono sfruttate artificialmente dalle tecnologie digitali incertezze e perplessità; e questo al punto da arrivare a considerare la paura un vero e proprio fattore di caratterizzazione sociale[61]. Alle concezioni tecnocratiche di rischio che hanno predominato, e con le quali si è cercato di valutare e gestire oggettivamente paure, minacce e danni[62], ora corrisponde non solo l'angoscia e la frustrazione spontanea che esiste e si prova, ma anche l'alimentazione e la strumentalizzazione, in modo preciso e artificiale, della paura al fine di perseguire ulteriori fini economici, sociali e/o politici; oppure, che è lo stesso, la paura come mezzo di identificazione, cattura e controllo sociale[63].

Pur non potendosi considerare nuova, questa strumentalizzazione della paura[64], come rispetto alla sua funzione rispetto alla libertà (e cosa farne)[65], così come il grado, la trasversalità e il tecnicismo digitale con cui si manifestano paura, frustrazione, incertezza e progresso, consente una maggiore capacità di cattura, influenza e manipolazione da parte di terzi (pubblici o privati) sui cittadini spaventati e che domandano sicurezza.

---

[56] Cfr. A. Richterich, *How data-driven research fuelled the cambridge analytica controversy*, *Partecipazione e Conflitto*, 11(2), 2018, 528 ss.; S. Suárez Gonzalo, *Tus likes ¿tu voto? Explotación masiva de datos personales y manipulación informativa en la campaña electoral de Donald Trump a la presidencia de EEUU 2016*, in *Quaderons del CAC*, 44, 2018, 27 ss.; e M. Betzu – G. Coinu – G. Demuro, *Gobernanza de los macrodatos y democracia representativa*, in *Revista de Derecho Político*, 106, 2019, in particolare 261 ss.

[57] T. E. Frosini, *Liberté, Egalité, Internet*, Napoli, 2015.

[58] Cfr. A. D'Atena, *Democrazia illiberale e democrazia diretta nell'era digitale*, *Rivista AIC*, 2, 2019, 583 ss.

[59] V. A. Morelli - O. Pollicino, *Metaphors, Judicial Frames and Fundamental Rights in Cyberspace*, in *American Journal of Comparative Law*, 2020, 1 ss.

[60] F. Balaguer Callejón, *Redes sociales, compañías tecnológicas y democracia*, in *Revista de Derecho Constitucional Europeo*, 32, 2019.

[61] Definite espressamente "società della paura", H. Bude, *La sociedad del miedo*, Barcellona, 2017.

[62] Nonostante ciò, confinandoli e nascondendoli nei risultati economici e nel progresso sociale; cfr. J. A. López Cerezo - J. L. Luján, *Hacia un nuevo contrato social para la ciencia: evaluación del riesgo en contexto social*, in Aa. Vv. *Ciencia, tecnología, sociedad y cultura en el cambio de siglo*, Madrid, 2001, 135 ss.

[63] C. Formoso Araujo, *Miedo social en las sociedades de la comunicación. Poder, crisis económica y políticas en España (2008-2015)*, Madrid, 2019.

[64] Sulla paura, come strumento politico, cfr. C. Robin, *El miedo. Historia de una idea política*, México, 2009.

[65] E. Fromm, *El miedo a la libertad*, Barcelona, Paidós, 2009.

Da qui, ovviamente, la sua evidente dimensione costituzionale al giorno d'oggi.

3. Democrazia, post-verità e paura

3.1. Politica e paura

Come indicato, i social network (ma non solo) oggi canalizzano buona parte della paura e della frustrazione che si rinvengono nella vita politica; e ciò a partire dalle bugie, sotto forma di post-verità e disinformazione, così come attraverso la manipolazione psicologica dei cittadini. Ciò che è rilevante a livello costituzionale è il grado di paura, rabbia e odio che si raggiunge tramite tutto ciò[66], e in maniera combinata con: lo sviluppo tecnologico-informatico delle procedure manipolative della persona (già menzionato); la semplificazione e il carattere autoreferenziale e rialimentato per cui la comunicazione pubblica in rete si caratterizza ed offre, favorendo così posizioni contradditorie e sconnesse; la disaffezione che prolifera anche all'interno dei media tradizionali, come la loro progressiva digitalizzazione e l'adozione delle loro caratteristiche modalità di operare anche all'interno dei social network; e la dipendenza che dimostra la politica a vantaggio di Internet e dei social network, in quanto oggi sono intermediari fondamentali nella comunicazione tra cittadini, partiti e poteri pubblici, per non parlare delle sue conseguenze nei processi elettorali e per la democrazia diretta[67].

Ciò ha un impatto, infine, sul modo in cui si intende l'attività politica in democrazia, inclusa la democrazia stessa[68], secondo tre assi: uno, la pianificazione, la partecipazione e l'esercizio degli affari pubblici in relazione al governo delle risorse pubbliche secondo bisogni e scopi collettivi; due, la competizione elettorale, al fine di individuare i rappresentanti della cittadinanza nell'ambito di un certo governo e nell'esercizio dei loro diritti di partecipazione; e tre, la mera lotta e il confronto ideologico tra i consociati[69]. A seconda della combinazione e dell'equilibrio dialettico di questi assi, è possibile diagnosticare una maggiore o minore qualità democratica, e ciò soprattutto di fronte al riconoscimento e alla garanzia del pluralismo dato che è un valore insito al costituzionalismo contemporaneo; e cioè pluralismo da intendersi come fattore di governo, bilancio elettorale e limite al confronto, ma anche come rappresentatività, differenza e conflitto, nonché espressione dialettica di maggioranze e minoranze[70].

---

66 V. D. Zolo, *Miedo e inseguridad*, in *Anales de la Cátedra Francisco Suárez*, 43, 2009, 152 ss.

67 L. M. González De La Garza, *La crisis de la democracia representativa. Nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el microtargeting y el big data*, in *Revista de Derecho Político*, 103, 2018, 257 ss. Ma quanto affermato, inoltre, vale anche dal punto di vista della strumentazione politica digitale messa a disposizione dei poteri pubblici democratici e dei partiti rispetto alla cittadinanza e i processi elettorali; S. Rodotà, *Democracia y protección de datos*, in *Cuadernos de Derecho Público*, 19-20, 2003, 15 ss.

68 D. Palano, *La democrazia alla fine del «pubblico» sfiducia, frammentazione, polarizzazione: verso una «bubble democracy»?*, in *Governare la paura. Journal of interdisciplinary studies*, 2019, 35 ss.; v. anche F. Balaguer Callejón, *La crisis de la democracia representativa frente a la democracia digital*, 2021 (in corso di stampa).

69 E. Guillén López, *Repensando la forma de gobierno (Constitucionalismo, democracia y parlamentarismo en contextos posnacionales)*, Madrid, 2019, 25 ss.

70 V. F. R. De Martino, *L'attualità del principio pluralista come problema*, in *Rivista AIC*, 2, 2019, 569 ss.

Ma è proprio quando il confronto è alimentato dalla paura degli altri, dalla frustrazione e dalle insicurezze, che l'equilibrio si inclina pericolosamente a svantaggio del pluralismo. La democrazia come processo deliberativo[71] e forma di ricerca di compromesso[72] è sostituita dalla sfida e dalla lotta ideologico-identitaria, in cui alcuni cercano semplicemente di differenziarsi e imporre agli altri le proprie convinzioni. La politica si distacca dai problemi comuni e generali, rifugiandosi nella frammentazione e in interessi particolari e identitari ("impolitica")[73], mentre il popolo, in quanto corpo politico, finisce per essere invocato come unità affine e omogenea, anziché come un aggregato diversificato[74]; inoltre, gli stessi limiti costituzionali come garanzia del pluralismo e delle minoranze (diritti fondamentali) finiscono per essere visti come un ostacolo alle rivendicazioni delle maggioranze che si ricompongono attraverso il populismo[75], lasciando spazio alla disaffezione per i limiti costituzionali perché ne costituiscono un freno[76]. Anche la normatività e la supremazia costituzionale cessano di essere considerate come garanzia delle minoranze, per mettersi al servizio di nuove realtà politiche sorrette da mere maggioranze[77]; il relativismo del pluralismo è sostituito dall'assoluto costituzionale dei più, del popolo come totalità astratta.

3.2. Conflitti e democrazia illiberale

All'interno di questa crisi e disaffezione costituzionale, il conflitto, inteso quale espressione del pluralismo, è presentato artificialmente dalla post-verità e dalla disinformazione come causa di paura e frustrazione, mentre da alcuni è celebrato in virtù del perseguimento dei rispettivi (e rivendicati) vantaggi che porterebbe all'interno del dibattito politico. Se il diritto costituzionale dell'Ottocento riuscì ad instaurare il predominio della borghesia, il costituzionalismo del periodo tra le due guerre e soprattutto quello del secondo dopoguerra (quello della Germania Ovest e dell'Italia), attraverso la già menzionata concezione normativa della Costituzione, è venuto a promuovere un sistema pluralista democratico. Un sistema in cui le maggioranze erano giuridicamente limitate, al pari di un nuovo modello di Stato, in quanto: normativamente configurato da una Costituzione con supremazia giuridica; e garantito da una giurisdizione costituzionale, grazie alla quale le minoranze e il pluralismo sono effettivamente garantiti. Ma

[71] J. Elster, *La deliberación y los procesos de creación constitucional*, in Aa. Vv. *La democracia deliberativa*, Barcelona, 2000, 129 ss.

[72] J. Rawls, *El liberalismo político*, Barcellona, 1996.

[73] ss. P. Rosanvallon, *La contrademocracia (La política en la era de la desconfianza)*, Buenos Aires, 2007, 38, e 241

[74] Per esempio, v. P. Cossarini - R. García Alonso, *El papel de las emociones en la teoría democrática. Desafíos para un uso público de la razón en tiempos de populismo*, in *Revista de Estudios Políticos*, 168, 2015, 291 ss.

[75] Nonostante tali maggioranze risultino essere mere minoranze che si autoidentificano con un popolo come un tutto unitario e uniforme.; cfr. P. Ciarlo, *Democrazia, partecipazione popolare e populismo al tempo della rete*, cit., 1 ss.

[76] V. A. Morelli, *El reduccionismo populista y sus efectos en la representación política y en la jurisdicción*, in *Revista de Derecho Constitucional Europeo*, 31, 2019.

[77] Di questo avviso, in passato, G. Zagrebelsky, *La Ley, el Derecho y la Constitución*, in *Revista Española de Derecho Constitucional*, 72, 2004, spec. 17 ss.

parliamo, inoltre, di un modello che emerge non solo al fine di scoprire e riconoscere il conflitto di classe celato dal precedente sistema liberale, ma anche per configurare una nuova attenzione per l'uguaglianza sostanziale e farsi promotore di diritti e libertà, promuovendo la crescita della democrazia materialmente e "pluralisticamente" sociale[78]. Questo è il motivo per cui, in primo luogo, si è costituito un sistema di riequilibrio dialettico giuridico, politico ed economico tra le classi sociali e, successivamente, detto riequilibrio è stato esteso ad altri settori o gruppi sociali storicamente relegati[79]. Allo stesso tempo, lo sviluppo del costituzionalismo normativo ha coinciso con il riconoscimento e la garanzia, in non pochi casi, di un pluralismo territoriale con cui plasmare dialetticamente sia il centro che la periferia politica, nonché la stessa strutturazione del potere in relazione ai vari livelli territoriali di governo democratico e in risposta alle rispettive politiche (e di conseguenza potenzialmente diverse)[80].

Con ciò la Costituzione normativa, pur garantendo il suddetto pluralismo, avrebbe consentito l'emergere e l'esaltazione del conflitto politico, sociale e territoriale, cercando nel contempo di incanalarlo dal punto di vista giuridico ("pacificando" il conflitto); a differenza del precedente costituzionalismo (liberale) che nascondeva il conflitto, il diritto costituzionale del dopoguerra presuppone il confronto tra gli uni e gli altri, e allo stesso tempo predispone strumenti con cui raggiungere un certo equilibrio di fondo. Ma la perdita di capacità giuridica della Costituzione normativa all'ombra della globalizzazione[81], così come, soprattutto, la riduzione dello stato sociale e delle politiche sociali sotto l'azione del neoliberismo nel contesto globale[82], e anche lo stimolo di politiche di ricentralizzazione territoriale[83], hanno limitato la suddetta capacità costituzionale rispetto al conflitto; non invano, il dibattito politico è stato drasticamente ridotto rispetto a quello economico e commerciale[84].

Inoltre, nuovi conflitti emergono in funzione del rischio, della tecnologia e della globalizzazione (come indicato), in cui la paura è al centro della scena, mentre la lotta sociale e politica che coinvolge la società, amplificata anche dalla post-verità e dalla di-

[78] F. Balaguer Callejón, *El Estado social y democrático de Derecho. Significado, alcance y vinculación de la cláusula del Estado social*, in Aa. Vv. *Comentario a la Constitución socio-económica de España*, Granada, 2002, 89 ss.

[79] C. De Cabo Martín, *Conflicto y constitución desde el constitucionalismo crítico*, Madrid, 2019.

[80] E quindi, che la concezione normativa della Costituzione sarà essenziale come garanzia dei processi di decentralizzazione del potere nazionale (es. lo Stato *autonómico*), nonché della formazione di processi di integrazione sovranazionale (Unione europea). Cfr. P. Häberle, *Comparación constitucional y cultural de los modelos federales*, in *Revista de Derecho Constitucional Europeo*, 8, 2007, 171 ss.

[81] Oltre a quanto già indicato, J. F. Sánchez Barrilao, *Sobre la Constitución normativa y la globalización*, in *Revista de la Facultad de Derecho de la Universidad de Granada*, 7, 2004, 241 ss.; e ID., *Derecho europeo y globalización: mitos y retos en la construcción del Derecho Constitucional Europeo*, in *Revista de Derecho Constitucional Europeo*, 12, 2009, 115 ss.

[82] C. D. Cabo Martín, *Lo viejo y lo nuevo en la crisis económica actual: aspectos jurídico-políticos*, in Aa. Vv. *Pensamiento crítico y crisis capitalista: una perspectiva constitucional*, Granada, 2010, 11 ss.

[83] Per esempio, G. Massa Gallerano, *L'impatto della crisi economica sulla distribuzione territoriales del potere*, in Aa. Vv. *El impacto de la crisis económica en las instituciones de la UE y los Estados miembros*, Cizur Menor, Aranzadi, 2015, 551 ss.

[84] Tra gli altri, F. Balaguer Callejón, *Una interpretación constitucional de la crisis económica*, in *Revista de Derecho Constitucional Europeo*, 19, 2013, 449 ss.; e E. Guillén López, *La crisis económica y la dirección política: reflexiones sobre los conceptos de necesidad y de elección en la teoría constitucional*, in *Revista de Derecho Constitucional Europeo*, 20, 2013, 431 ss.

sinformazione, incita a nuovi confronti (genere, emergenza climatica, identità sessuale e di genere, animalismo, multiculturalismo, xenofobia, localismo, espansione urbana e svuotamento interno, ecc.), aumentando (alimentando) a sua volta movimenti reattivi come fattore di permanente tensione interna e di scontro nel quadro costituzionale pluralista, rispetto al quale le Costituzioni sono, in molti casi, anemiche. È con ciò che il ruolo pacificatore del costituzionalismo normativo si vede atomizzato di fronte a molteplici conflitti trasversali e in molti casi promosso artificialmente attraverso la post-verità e la disinformazione; e poi, che il modello democratico-pluralista sia messo alla prova da tendenze maggioritarie e illiberali che cercano di tornare a fasi passate (come un regime ibrido a metà strada tra quello autoritario e quello democratico)[85] in cui gruppi più o meno maggioritari e identità frustrate (con una base più o meno oggettiva, ma sempre caratterizzati da un sentimento di smarrimento) assumono, a partire dal rifiuto degli altri, nuove posizioni di leadership popolare (populisti) e di imposizione sociale, politica e giuridica (anche costituzionale).

Da questa prospettiva, i processi illiberali che guadagnano terreno di fronte alla democrazia pluralista si basano sulla già citata frustrazione nel contesto globalizzato, poiché la politica è soggetta a un pensiero economico egemonico (quello del mercato), mentre le masse popolari sono, in questo senso, lasciate fuori[86]. E così, facendo appello alla paura e alla frustrazione dei primi, non solo rifiutano *gli altri*, come cause ipotetiche della loro situazione deficitaria e instabile (le élite e/o gli immigrati, ad esempio), ma rinnegano, sulla base delle stesse garanzie offerte dal pluralismo, l'attuale modello costituzionale in quanto incapace di soddisfare le pretese di stabilità e sicurezza di cui avrebbero goduto fino a tempi recenti.

Inoltre, e all'ombra di una crisi come quella sanitaria da COVID-19, accade che il conflitto insito alle democrazie pluraliste e decentralizzate venga presentato come un ostacolo alla loro gestione; e non rispetto al sempre auspicabile accordo e sostegno dei "diversi" nel tentativo di superare la crisi, ma alla presunta efficienza dell'unità politica solamente di alcuni di fronte a tutti gli altri. Naturalmente, il diritto costituzionale sull'eccezione risponde a tale paradigma, ma lo fa senza negare il pluralismo; semmai sospenderlo temporaneamente[87]. Un'altra cosa è, come accade oggi, trarre vantaggio dalle crisi, e dalle loro difficoltà, per attaccare tramite la disinformazione il pluralismo, considerato che si presenta quale fonte del conflitto; o semplicemente presupponendo la maggiore efficienza di certi regimi che di fatto negano il pluralismo e il conflitto (come è stato il caso della Cina dinanzi al COVID-19).

[85] A. Di Gregorio, *I fenomeni di degenerazione delle democrazie contemporanee: qualche spunto di riflessione sullo sfondo delle contrapposizioni dottrinali*, in *Nuovi Autoritarismi e Democrazie: Diritto, Istituzioni, Società (NAD)*, 2, 2019, spec. 21 ss.

[86] J. Zielonka, *Contro-rivoluzione. La disfatta dell'Europa liberale*, Bari-Roma, 2018.

[87] P. Cruz Villalón, *Estados excepcionales y suspensión de garantías*, Madrid, 1984.

4. Affrontare la paura dalla prospettiva costituzionale dinanzi alla disinformazione

4.1. Sicurezza e democrazia pluralista

L'idea di sicurezza è implicita ad ogni comunità, ovvero il sentirsi protetti dal gruppo che la compone e in cui ci si trova[88]; e con essa l'evidenza soggettiva che della sicurezza emerge (dalla sua dimensione più liberale) e la connessione tra tale percezione e la paura, in modo tale che gestire la sicurezza significhi gestire la paura stessa[89]. Quindi questa sensazione di sicurezza (o insicurezza), al di là delle sue dimensioni più ovvie di fronte ai rischi effettivi, risulta manipolabile; la sicurezza, pertanto, deve essere ricostruita oggettivamente dalle molteplici sfaccettature in cui prosperano i rischi[90]: sicurezza nazionale (con l'integrazione di difesa, sicurezza pubblica, sicurezza economica e finanziaria, sicurezza informatica, ecc.), oltre alla sicurezza sanitaria, alimentare e farmaceutica, sicurezza ambientale, sicurezza sociale e sul lavoro, sicurezza umana, ecc.[91]. Ma ci si chiede anche come affrontare la sicurezza della stessa democrazia pluralista di fronte alla paura come catalizzatore della sua disaffezione, e soprattutto di fronte alla sua manipolazione sociale e politica da parte di gruppi che agiscono sotto l'ombrello del costituzionalismo democratico, soprattutto dall'esercizio dei diritti fondamentali come la libertà di espressione e di informazione. Non a caso, le libertà e la democrazia sono già protette in Spagna dalla suddetta sicurezza nazionale (art. 3, legge 28 settembre 2015, n. 36, "Sicurezza nazionale"), dove sono previsti i rischi e i fattori che possono comprometterli (quindi la strategia di sicurezza spagnola del 2011 e le successive strategie di sicurezza nazionale del 2013 e 2017 sono state aperte a fattori che aumentano il rischio sociale e politico come la povertà, la disuguaglianza, gli estremismi ideologici e la radicalizzazione violenta, gli squilibri demografici e l'uso nocivo, appunto, delle nuove tecnologie)[92]. Ma fino a che punto possiamo difendere la democrazia da sé stessa, senza metterla a rischio[93]?

Da tempo si percepisce come le disuguaglianze e gli estremismi ideologici siano fondamentali per un'adeguata conformazione sociale e democratica dello Stato, poiché si presentano quale presupposto della necessaria "normalità" utile ad una regolamenta-

[88] Z. Bauman, *Comunidad (En busca de seguridad en un mundo hostil)*, Madrid, 2006.

[89] V. M. L. Lanzillo, *Gouverner la peur (De la domination moderne de la peur au politiques de sécurité et au management du risque dans l'ère globale*), in *Governare la paura. Journal of interdisciplinary studies*, 2009.

[90] A proposito di sicurezza oltre il sentimento di insicurezza e politiche criminali, per tornare alla dimensione sociale dell'azione pubblica, cfr. D. Zolo, *Miedo e inseguridad*, cit., 158 ss.

[91] Sulla nozione di sicurezza in ambito costituzionale, E. Guillén López, *Repensando la forma de gobierno,* cit., 291 ss.

[92] Sulla radicalizzazione violenta, il Piano strategico nazionale per la lotta alla radicalizzazione violenta (PEN-LCRV), "Un quadro per il rispetto e la comprensione comune", del 2015; e più recentemente, la Strategia nazionale antiterrorismo (ed estremismo violento) del 2019.

[93] E soprattutto di fronte alle opzioni politiche che, democraticamente, implicano la negazione astratta e generalizzata di diritti e libertà per minoranze e gruppi di opposizione, e l'ovvia difficoltà di impedire a un popolo (soprattutto) di rinunciare alla propria libertà (poiché non può essere imposta); A. Ross, *¿Por qué Democracia?*, Madrid, 1989, 101-104.

zione costituzionale efficace ed efficiente[94]. Come indicato, i limiti che la globalizzazione determina per la democrazia pluralista, il conflitto interno e dialettico che sta alla base tra il tutto e l'identità con esso, e la fatale catalizzazione delle sue carenze si è raggiunta negli anni con la crisi economica (a cui oggi si può aggiungere quella nata a causa del COVID-19), hanno promosso movimenti sociali e politici poco rispettosi dei presupposti del costituzionalismo contemporaneo: dignità, libertà, uguaglianza materiale, pluralismo, ecc.. Tale radicalizzazione politica e sociale, senza essere nuova, si diffonde e si amplifica in maniera tecnologica ed esponenziale attraverso i social network, sotto forma di manipolazione, post-verità digitale, disinformazione e persino appello alla violenza[95]. Viene così messo a dura prova l'intero sistema democratico-costituzionale e i suoi valori[96], che finisce per essere oggetto del diritto costituzionale[97] e della stessa sicurezza, anche se pone problemi in quanto è contiguo allo stesso pluralismo: soprattutto quando si tratta di movimenti che, pur caratterizzati da un'intensa disaffezione nei confronti del sistema costituzionale pluralista, agiscono al suo interno, mentre detto sistema, anche presieduto da una Costituzione normativa e rigida, non vieta espressamente la riforma di alcuna parte o contenuto (come è appunto il caso Spagnolo)[98]; non trovandosi quindi nel quadro di una democrazia militante (e *ideologicamente non neutrale*, come quella tedesca)[99], qualsiasi opzione politica finalizzata a una riforma costituzionale conforme al quadro procedurale stabilito costituzionalmente rimarrebbe integrata nel pluralismo riconosciuto in Spagna. Tuttavia, sebbene questi gruppi rispettino i procedimenti democratici e costituzionali, e quindi aderiscano formalmente al principio di lealtà costituzionale[100], nella loro azione e nel loro linguaggio esprimono uno scarso patriottismo costituzionale[101] di fronte al pluralismo, ai diritti e alle libertà, in modo tale da generare sospetti fondati in merito alla futura rottura della suddetta lealtà al fine

94 H. Heller, *Teoría del Estado*, México, FCE, 6ª reimp., 1971, 256 ss. Anche in tema di politiche giuste come precondizione di legittimità dei regimi liberali, T. Khaitan, *Political insurance for the (relative) poor: How liberal constitutionalism could resist plutocracy*, in *Global Constitutionalism*, 8(3), 2019, 536 ss., spec. 569.

95 Si pensi ai gruppi terroristici, ma non solo, come quelli xenofobi e nazionalisti; cfr. A. P. Schmid, *Research on Radicalisation: Topics and Themes*, in *Perspectives on Terrorism*, 10(3), 2016, 26 ss.

96 A. D'Atena, *La conflictividad axiológica de la democracia liberal y el desafío de Internet*, in *Revista de Derecho Constitucional Europeo*, 30, 2018.

97 V. S. Choudhry, *Resisting democratic backsliding: An essay on Weimar, self-enforcing constitutions, and the Frankfurt School*, in *Global Constitutionalism*, 7(1), 2018, 54-55.

98 Art. 168 CE e STC 124/2017, 8 novembre (FJ núm. 5.d).

99 K. Von Beyme, *La protección del ordenamiento constitucional y del sistema democrático en la república federal de Alemania*, in *Revista de Estudios Políticos*, 35, 1983, 73 ss.; anche E. Denninger, *Democracia militante y defensa de la Constitución*, insieme a E. Benda, *Manual de Derecho Constitucional*, Madrid, 2001, 445 ss. Inoltre, sul carattere non "neutrale" della democrazia tedesca, cfr. K. Stern, *Derecho del Estado de la República Federal Alemana*, Madrid, 1987, 386-387.

100 V. L. Álvarez Álvarez, *Lealtad constitucional y partidos políticos*, in *Teoría y Realidad Constitucional*, 10-11, 2002-2003, 445 ss.; e R. Tur Ausina, *Lealtad constitucional y democracia*, in *Revista de Derecho Político*, 101, 2018, 503 ss.

101 J. Habermas, *Ciudadanía e identidad nacional*, in *Facticidad y validez (Sobre el Derecho y el Estado democrático de Derecho en términos de teoría del discurso)*, Madrid, 2005, 619 ss. E sull'origine della nozione "patriottismo costituzionale" in Sternberger, v. J. C. Velasco Arroyo, *Los contextos del patriotismo constitucional*, in *Cuadernos de Alzate*, 24, 2001, 63 ss.

di ottenere il potere[102]; ciò significa che la disaffezione costituzionale viene presentata come un fenomeno antagonista al patriottismo costituzionale, poiché è una messa in discussione ideologica del pluralismo, delle minoranze e delle libertà.

La storia permette di individuare, appunto, regimi autoritari che vantano un'iniziale legittimità democratica, di movimenti che lottano per il potere con evidenti derive autoritarie, e di quelli che vi arrivano riformandolo (ad esempio, attualmente, Viktor Orbán in Ungheria, Andrzej Duda in Polonia, o Recep Tayyip Erdoğan in Turchia). È così che sorge la sfida più difficile per gli Stati democratici, come quello spagnolo o quello italiano: garantire la democrazia pluralista dallo stesso principio democratico nel suo senso maggioritario e illiberale[103]; e con esso il paradosso di come e in che misura uno Stato, come la Spagna, possa controllare l'ontologica qualità democratica nell'esercizio di diritti e libertà che si presenti formalmente rispettoso dell'ordine costituzionale[104]. Se la democrazia costituzionale oggi non è solo un processo legato all'adozione di decisioni pubbliche, ma anche partecipazione e sviluppo di un sistema fondato, rispettoso e promotore della dignità umana[105], vuol dire che tale concezione della democrazia debba legittimare azioni volte alla sua protezione contro azioni formalmente democratiche, ma teleologicamente contrarie ad essa, anche se c'è chi presenta la democrazia come una semplice maggioranza rappresentativa (ovviamente, democrazie illiberali). Pertanto, sebbene in un sistema costituzionale come quello spagnolo non sia possibile riconoscere uno standard di democrazia militante, il patriottismo costituzionale accolto nell'Unione europea (art. 2 TUE) consente di trasmutarlo in un certo grado di democrazia militante sulla falsariga della limitazione del processo di integrazione europea, e soprattutto la riconosciuta capacità dell'Unione di sanzionare uno Stato in caso di torsione autoritaria (art. 7 TUE); in questo modo si parla di una certa "transnazionalizzazione" della democrazia militante (Wagrandl). Non si tratta tanto di affermare l'importanza, attraverso l'Europa, di una concezione di democrazia militante in grado di vietare legittimamente certe opzioni politiche, ma piuttosto accogliere una nozione di patriottismo costituzionale tale da giustificare misure con cui reagire alla disaffezione costituzionale, in generale, e ad una eventuale torsione autoritaria, in particolare.

---

[102] In Germania, distinguendo tra un movimento ideologico (partito politico) costituzionale, ma antidemocratico, e in vista della riforma costituzionale del 7 luglio 2017, v. P. Fernández De Casadevante Mayordomo, *La prohibición de partidos políticos en Alemania. Del nuevo criterio de la potencialidad y la reciente reforma constitucional para la no financiación de formaciones antidemocráticas pero constitucionales*, in *Revista de Derecho Político*, 102, 2018, 235 ss.

[103] E oltre la garanzia fornita dalle giurisdizioni costituzionali, come i tribunali ordinari (es. il divieto di associazioni e partiti ai sensi dell'art. 22.4 CE, Cap. VII LO 1/2002 e Cap. III LO 6/2002).

[104] Sui paradossi della democrazia militante, v. P. Macklem, *Militant democracy, legal pluralism, and the paradox of self-determination*, in *International Journal of Constitutional Law*, 4(3), 2006, 488 ss.; e U. Wagrandl, *Transnational militant democracy*, in *Global Constitutionalism*, 7(2), 2018, spec. 146-150.

[105] Cfr. E. Sciacca, *Interpretación de la democracia*, Madrid, 1994, spec. 159.

4.2. Misure per il contenimento della disinformazione e in promozione della democrazia: la "procedura di attuazione contro la disinformazione"

Quanto sopra sembrerebbe legittimare azioni pubbliche volte a contenere la paura che, ferma restando la loro necessità e proporzionalità (oltre alla loro copertura legale), tendono a ridurre l'impatto che del loro uso e manipolazione si finisca con il realizzare nell'ambito del dibattito e dei processi democratici[106]. In questo senso, la post-verità e la disinformazione rappresentano un pericolo per la democrazia pluralista (come è stato evidenziato), soprattutto se viene deliberatamente promossa per alterare il normale sviluppo delle istituzioni e dei processi democratici, destabilizzandoli; e ancor di più quando si tratta di manipolazioni nelle reti sociali, considerando l'influenza sociale, culturale, economica e politica che determinati gruppi e soggetti raggiungono effettivamente attraverso le stesse, oltre alla loro capacità molto limitata di comunicazione riflessiva[107]. È così che sorgono proposte per combattere tali azioni e contenuti in rete; proposte che, anche dalla più stretta proporzionalità, possono comportare restrizioni (anche legittime) alle libertà di espressione, comunicazione e informazione. È il caso della Germania, con il Network Enforcement Act (o NetzDG), del 30 giugno 2017, contro le *fake news* e l'inerzia della reta al riguardo, che costringe ad eliminare le false notizie a pena di multe elevatissime[108]; e della Francia, con una Legge sulla lotta alla manipolazione dell'informazione (Loi 2018-1202), del 22 dicembre 2018, che consente la sorveglianza sui social network e sui media stranieri, l'eliminazione delle false notizie durante il periodo elettorale e la sospensione di un canale se si ritiene che possa interferire con i risultati elettorali; o in Italia, la proposta di un'autorità indipendente della verità in rete che, sulla base di principi predefiniti, intervenga rapidamente[109].

A tal riguardo, nel caso della Spagna, parte della dottrina evidenzia il regio decreto legge 14/2019 del 31 ottobre (con il quale vengono adottate misure urgenti per motivi di sicurezza pubblica in materia di amministrazione digitale, appalti pubblici e telecomunicazioni)[110], in quanto ha evidenziato la possibilità di un intervento governativo in materia di rete e servizi di comunicazione elettronica in casi eccezionali di cui risultino compromesse l'ordine pubblico, la pubblica sicurezza e la sicurezza nazionale (art. 6.1, che modifica l'art. 4.6 della legge 9 maggio 2014, n. 9, *General de Telecomunicaciones*). Tut-

[106] E ciò, senza pregiudizio per la persecuzione di messaggi di odio e radicalizzazione violenta; persino reclutamento e addestramento di terroristi sui social network, come già accade.

[107] Di questo avviso C. Pinelli, *"Postverità", verità e libertà di manifestazione del pensiero*, in *questa Rivista,* 1, 2017, 41 ss.

[108] G. De Gregorio, *The market place of ideas nell'era della post-verità: quali responsabilità per gli attori pubblici e privati online?*, in *questa Rivista*, 1, 2017, 97 ss.; e V. Claussen, *Fighting Hate Speech and Fake News. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation*, ivi, 3, 2018, 110 ss.

[109] G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *questa Rivista*, 1, 2018, 26 ss.; in senso contrario, N. Zanon, *Fake news e diffusione dei social media: abbiamo bisogno di un"Autorità Pubblica della Verità"?*, ivi, 1, 2018, 87 ss.

[110] Per esempio, e contro questa possibilità, v. G. M. Teruel Lozano, *¿'Estado de excepción' digital?*, in *Agenda Pública*, 2019; L. Cotino Hueso, *ONLINE-OFFLINE. Las garantías para el acceso a Internet y para la desconexión, bloqueo, filtrado y otras restricciones de la red y sus contenidos*, in *Revista de Derecho Político*, 198, 2020, 13 ss.

tavia, senza considerare la mancanza di precisione della regola in questione, si intende come l'obiettivo non sembri quello di controllare i contenuti sui social network, ma garantire il funzionamento delle infrastrutture, delle risorse ad esse associate o di un elemento o livello della rete o del servizio di comunicazione elettronica in situazioni di grave rischio per la sicurezza nazionale[111]; in altre parole, ciò che la norma apre è una possibilità di intervento del governo nella gestione dell'accesso e della fornitura di rete Internet, non dei contenuti che circolano attraverso di essa (fermo restando, ovviamente, che il legislatore potrebbe avere mostrato maggiore chiarezza nella redazione della norma, insistiamo, soprattutto vista la sensibilità e la rilevanza della materia).

Altra cosa è, dalla stessa portata e struttura della sicurezza nazionale spagnola, considerare la manipolazione delle informazioni che circolano attraverso le reti come il suo principale obiettivo (Strategia nazionale per la sicurezza informatica del 2019, cap. 3, *in fine*)[112]; e in questo senso, appunto, la previsione all'interno dell'organizzazione di *cybersecurity* e *cyberintelligence* (all'interno del National Cryptological Center, e come organismo dipendente dal Centro Nacional de Intelligencia o CNI)[113] di un "Osservatorio Digitale" con ELISA come strumento digitale e con funzioni specifiche di emergenza, valutazione e compilazione di campagne di disinformazione e destabilizzazione del sistema. D'altra parte, nel marzo 2020, nel contesto caratterizzato dalla pandemia da COVID-19, il Ministero dell'Interno ha pubblicamente ed espressamente riconosciuto il monitoraggio dei social network[114]; e, infine, la pubblicazione ufficiale in data 5 novembre 2020 da parte del *Ministerio de la Presidencia, Relaciones con la Cortes y Memoria Democrática* (Ordinanza PCM/1030/2020, del 30 ottobre, come indicato all'inizio di queste pagine), della "Procedura per l'azione contro la disinformazione", con la quale il Governo spagnolo intende, sotto la protezione e lo sviluppo del "Piano d'azione per la lotta alla disinformazione" della Commissione europea e del Servizio europeo per l'azione esterna (Consiglio europeo, 13 e 14 dicembre 2018), per realizzare un'azione più coordinata in materia di disinformazione (riadattando il precedente quadro di azione)[115] sia a livello organizzativo che funzionale.

---

[111] Contro la possibilità di sequestro dei contenuti, E. Ramos Carvajal, *Comentario crítico sobre el Real Decreto-Ley 14/2019*, *Diario La Ley*, 9531, 2019. L'ambito di applicazione della norma sembra più opportuno rispetto al controllo del cyberspazio da parte dello Stato; dalla dipendenza tecnologica dalle reti e dalle infrastrutture di comunicazione e dall'interesse dei poteri pubblici a controllarle per ragioni di sicurezza, v. J. F. Sánchez Barrilao, *Sobre la Constitución normativa y la globalización*, cit., 295 ss.

[112] Per un approccio in diritto comparato e in Europa sulla regolamentazione della disinformazione, v. R. Magallón Rosa, *La (no) regulación de la desinformación en la Unión Europea. Una perspectiva comparada*, in *Revista de Derecho Político*, 106, 2019, 319 ss.

[113] Ancora J. F. Sánchez Barrilao, *La constitucionalización de la integración regional europea*, cit., 104-105, e *Sobre la Constitución normativa y la globalización*, cit., 257 ss.

[114] Il ministro dell'Interno, Fernando Grande-Marlaska Gómez, in una conferenza stampa il 16 marzo 2020, quando ha letteralmente affermato che si stavano "monitorando tutti i *social network*"; *cfr.* J. F. Sánchez Barrilao, *Riesgos y seguridad a comienzos del siglo XXI (y una coda al respecto de la crisis del COVID-19)*, in Aa. Vv., *Los derechos fundamentales ante las crisis económicas y de seguridad en un marco constitucional fragmentado,* cit., spec. 333 (N.P. 125).

[115] E con cui preparare le basi per la creazione di un autentico Sistema Nazionale di prevenzione, rilevazione, allerta, monitoraggio e risposta alle cause, ai mezzi e/o alle conseguenze legate alla disinformazione. In questo senso, inoltre, si rileva la necessità di preparare una proposta per una Strategia Nazionale per combattere la Disinformazione.

Per quanto riguarda la prima, viene definita l'organizzazione per la lotta alla disinformazione, evidenziando al suo interno una "Commissione Permanente contro la disinformazione"[116]. Quanto alla seconda, ne vengono definiti gli obiettivi essenziali: identificare e definire organi, enti e autorità competenti; stabilire livelli di prevenzione, rilevamento, preallarme, analisi, risposta e valutazione[117]; descrivere ruoli specifici per i vari livelli di lotta alla disinformazione; definire meccanismi per lo scambio di informazioni a livello strategico, operativo e tecnico; determinare le modalità di valutazione dell'attuazione e del funzionamento della procedura; e definire una metodologia per l'identificazione, l'analisi e la gestione dei fenomeni di disinformazione. Pertanto, come si può vedere, non è altro, sostanzialmente, che un insieme di misure di natura politica e gestionale che si articolano in questo piano relative alla sicurezza, e senza impatto giuridico sui diritti e le libertà di espressione e informazione, almeno in principio[118].

Proprio per questo, la Sicurezza Nazionale, piuttosto che tentare di reagire a quei gravi attacchi perpetrati contro il sistema politico che possono addirittura configurare fattispecie tipiche di reato (per questo c'è la sicurezza pubblica e i Tribunali, e senza pregiudizio del fatto che determinate azioni possano essere oggetto di alternative forme di sicurezza, come al giorno d'oggi il caso del terrorismo), tenta di impedire la materializzazione di questi rischi, difendendo il sistema nel suo complesso; è per questo che gli strumenti che si rinvengono in questo procedimento sono di carattere politico (come si è già anticipato), in quanto sostanzialmente diretti all'acquisizione di conoscenze (per esempio, monitoraggio, vigilanza e ricerca di contenuti pubblici che circolano su Internet) e alla loro valutazione (intelligenza), al fine di poter adottare, successivamente, altri tipi di strumenti (secondo quanto indicato, prendere decisioni e definire obiettivi di carattere politico-strategico davanti alle campagne di disinformazione).

E tutto questo, a sua volta, in accordo con l'Unione europea, e non più perché questa "Procedura per l'azione contro la disinformazione" è adottata in linea con il già citato

[116] Oltre al Consiglio di Sicurezza Nazionale, il Comitato di Situazione (e al suo interno, una Cellula di Coordinamento per combattere la disinformazione), il Segretario di Stato per la Comunicazione, altre autorità pubbliche competenti, nonché il settore privato e la società civile. Quanto alla cosiddetta "Commissione permanente contro la disinformazione", è composta da: Segretario di Stato per la Comunicazione, coordinandola; la Presidenza del Governo, attraverso il Dipartimento della Sicurezza Nazionale, presieduta dal suo Direttore; il Ministero della Difesa, tramite il CNI; il Ministero dell'Interno, con la Segreteria di Stato per la Sicurezza e l'Ufficio di coordinamento e studi; il Ministero degli Affari Esteri, UE e Cooperazione, attraverso la Direzione Generale Comunicazione, Diplomazia Pubblica e Reti; il Ministero dell'Economia e della Trasformazione Digitale, con il Segretario di Stato per la Trasformazione Digitale e l'Intelligenza Artificiale; Possono essere convocati in qualità di esperti anche altri rappresentanti dell'Amministrazione generale dello Stato, Comunità autonome, Città autonome ed enti locali, nonché rappresentanti del settore privato e altri esperti.

[117] La procedura stabilisce quattro diversi livelli di attivazione nel rilevamento di campagne di disinformazione, analisi dei possibili impatti sulla sicurezza nazionale spagnola e gestione delle situazioni di crisi: livello 1, rilevamento, realizzazione di allarmi e notifiche precoci (evidenziando le azioni nel monitoraggio, sorveglianza e investigazione); Livello 2, nel coordinamento, sincronizzazione e definizione delle priorità degli sforzi nella lotta alla disinformazione; Livello 3, prendere decisioni e fissare obiettivi di natura politico-strategica per affrontare le campagne di disinformazione; e Livello 4, di gestione politica nell'ambito del sistema di sicurezza nazionale in caso di campagne da Stati terzi.

[118] Diciamo "in linea di principio", perché in vista del sopracitato monitoraggio e rilevazione di una campagna di disinformazione, è possibile attivare specifiche azioni di sicurezza nazionale e di carattere più intenso, anche se, ovviamente, sempre nel rispetto della Legge.

"Piano d'azione per la lotta alla disinformazione" della Commissione e del Servizio europeo per l'azione esterna, ma perché oggi buona parte della pianificazione della sicurezza (e dell'attività di intelligence) è realizzata e sviluppata trasversalmente con l'Europa; la maggior parte dei rischi, come quello posto dalla disinformazione per la democrazia, non sono esclusivi o caratterizzanti di singoli Stati, ma sono minacce che, dall'interno e dall'esterno, si diffondono orizzontalmente e verticalmente in Europa, richiedendo quindi un alto grado di collaborazione e cooperazione tra Stati e con/dall'Unione[119].

Le precedenti contestazioni sono sollevate anche dagli stessi fornitori di applicazioni, in considerazione dell'autoregolamentazione da questi progressivamente costruita[120], senza pregiudicare la loro natura, capacità, rischi e limitazioni[121]; e da questa prospettiva privata, la promozione di codici di *best practices* in reti verificabili successivamente da terzi, così come la citata proposta della Commissione Europea dell'aprile del 2018 di un codice in tal senso (Code of Practice on Disinformation)[122] e rete europea indipendente di verificatori dell'informazione[123], o l'approvazione di taluni autocontrolli da parte degli stessi utenti di Internet attraverso strumenti discorsivi (come la First Draft Coalition)[124].

Una maggiore complessità e difficoltà ha fatto sì che l'Executive Order firmato da Trump il 28 maggio 2020[125], revocasse l'immunità dei social network contro le rivendicazioni per i contenuti che si trovano su di essi quando sviluppano un qualche tipo di meccanismo di controllo per tali contenuti (da considerarsi, quindi, come editori di contenuti e non semplici fornitori di servizi); e ciò, precisamente e repressivamente, si presenta quale reazione ai controlli da loro esercitati su di lui, sui suoi seguaci e alleati politici[126].

Ma la post-verità, la disinformazione e la paura non sono solo un problema di contenuto, e della forma e dei mezzi con cui vengono presentati e proiettati[127]. Lo stesso vale

---

119 J. F. Sánchez Barrilao, *Inteligencia y seguridad como objeto constitucional*, cit., 427 ss.

120 Già come condizioni generali di contratto, o semplici codici di condotta e meccanismi extragiudiziali per la risoluzione dei conflitti; e da una tale lungimiranza, che i provider di applicazioni social prevedono sempre più limitazioni sui contenuti, come strumenti specifici contro le fake news. Di interesse, sul regime di responsabilità degli intermediari Internet in relazione ai contenuti, v. A. Sigüenza Flórez, *La libertad de expresión en Internet*, in Aa. Vv., in *El Derecho de Internet*, Barcellona, 2016, 66-68.

121 In questo senso, J. F. Sánchez Barrilao, *El internet en la era Trump*, cit., 58-59. Altra cosa è la linea pericolosa che la proposta di Trump suppone per monitorare, attraverso un decreto esecutivo (Proteggere gli americani dalla censura online), i controlli effettuati dalle reti quando ciò interessa comunicazioni soggette a settori o gruppi politici legati al Presidente)

122 Cfr. *Code of practice on disinformation,* in *digital-strategy.ec.europa.eu.*

123 V. il primo *annual self-assessment of the signatories to the Code of Practice on Disinformation*, in *ec.europa.eu.*

124 Cfr. *firstdraftnews.org.*

125 E modificando la sezione 230 di quella che è nota come *Communications Decency Act* (1996). A tal riguardo, e in modo critico, v. T. Wu, *Trump's Response to Twitter Is Unconstitutional Harassment (His executive order aimed at social media companies should be ignored)*, in *The New York Times*, 4 giugno 2020.

126 Sul progetto di questa *executive order*, come *Protecting Americans from Online Censorship*, e i controlli che le reti stavano sviluppando in merito alle comunicazioni inclini a settori o gruppi politici legati da tempo al Presidente (e quindi al di là dei conflitti tra Trump e Twitter dall'inizio del 2020), v. B. Fung, *White House proposal would have FCC and FTC police alleged social media censorship*, 10 agosto 2019.

127 In questo ambito, R. M. García Sanz, *La difícil relación del instituto de la opinión pública y los procesos de*

per la facoltà intellettuale e l'attitudine civica dei cittadini a interagire nel nuovo spazio virtuale che Internet e le reti rappresentano quando si tratta di valutare adeguatamente e criticamente tali contenuti, oltre che di contribuire ad essi. Si tratta principalmente di una questione culturale ed educativa, poiché la post-verità e la manipolazione della paura non possono essere risolte solo tramite le limitazioni all'esercizio dei diritti e delle libertà, ma anche promuovendo politiche pubbliche volte a configurare una cultura e un'educazione digitale responsabile che permetta di fondare una cittadinanza critica e politicamente attiva di fronte alla nuova realtà democratica digitale che abbiamo di fronte[128]. Ciò è stato evidenziato nell'Unione europea quando, in linea con il rapporto secondo cui nel gennaio 2018 la Commissione ha creato un gruppo di esperti di alto livello in materia di *fake news* e disinformazione (dando origine al citato Codice di buone pratiche sulla disinformazione), si osserva (tra le altre misure)[129] la necessità di promuovere una cittadinanza attiva e critica di fronte alle nuove tecnologie digitali[130].
Infine, un altro aspetto da sottolineare è che, come già evidenziato (Cambridge Analytica), le nuove tecnologie digitali possono operare come strumenti di manipolazione psicologica diretta della paura dei cittadini, quindi, senza pregiudicare i meccanismi informatici destinati ad avvertirli e neutralizzarli (soprattutto, attraverso l'Intelligenza Artificiale)[131], come di un'adeguata formazione cittadino-digitale, il suo utilizzo è da considerarsi del tutto illegittimo in quanto lede in maniera chiara la coscienza e la libera formazione della volontà dei cittadini, soprattutto nei processi elettorali (e questo senza considerare il già illegittimo trattamento dei dati personali che ciò implica)[132].

5. Considerazioni conclusive

Al fine di contenere la disinformazione, il Governo, in quanto principale responsabile della sicurezza in Spagna (artt. 97 CE e 4.1, l. 36/2015), deve sempre intervenire partendo dalla considerazione politica più neutra e oggettiva possibile, evitando comun-

comunicación pública en Internet: la desinformación desafiando las garantías constitucionales, *Revista de Derecho Político*, 106, 2019, 77 ss.

128 Cfr. F. Pizzetti, Fake news *e allarme sociale: responsabilità, non censura*, in *questa Rivista,* 1, 2017, 58-59. Anche, v. D. Frau-Meigs, *Contra la información falsa, espíritu crítico*, in *El Correo de la UNESCO*, 2, 2017, 12 ss.; e M. L. Lanzillo, *Cittadinanza democratica, scienza, educazione nel tempo della post-verità*, in *valuenews.invalsi.it*, 2018. Sulla realtà democratica digitale, v. J. Castellanos Claramunt, *Las imbricaciones políticas entre la participación ciudadana e Internet*, in *Revista de Derecho Político*, 106, 2019, 167 ss.

129 *Final report of the High Level Expert Group on Fake News and Online Disinformation*, 12 marzo 2018.

130 T. Casadei, *L'irruzione della post-verità*, *Governare la paura. Journal of interdisciplinary studies,* 2019, 1 ss. Non bisogna neanche dimenticare che il conflitto identitario che determina la globalizzazione, proprio come i movimenti populisti o illiberali, si alimentano della paura, la frustrazione e il conflitto, per cui si rimanda a C. Delsol, *Democracias iliberales*, in *Anales de la Cátedra Francisco Suárez*, 53, 2019, 339 ss. La cultura e l'educazione dovrebbero quindi proporre anche nuove modalità di ricostruzione delle identità collettive che legittimano non solo il rispettivo sistema attuale, ma i valori costituzionali su cui si è basata la convivenza di solidarietà tra i consociati; J. F. Sáchez Barrilao, *Fundamentalismos, identidades e integración europea*, in Aa. Vv. *Perspectivas actuales del proceso de integración europea*, Zaragoza, 2019, spec. 131-134.

131 V. J. M. Flores Vivar, *Inteligencia artificial y periodismo: diluyendo el impacto de la desinformación y las noticias falsas a través de los bots*, in *Doxa Comunicación*, 29, 2019, 197 ss.

132 F. Balaguer Callejón, *Redes sociales, compañías tecnológicas y democracia*… cit.

que di confondere (per lo meno) l'interesse generale che la garanzia del sistema costituzionale e democratico implica con quello più particolare e politico-partigiano che può manifestarsi in funzione dell'alternativa portata ideologica espressa dai consociati; e ciò per l'innato rischio che tali attività pubbliche comportano per il pluralismo ideologico costituzionalmente riconosciuto, nonché per la libertà di espressione e di informazione (art. 1.1 CE, oltre 20).

Quanto precede richiede, in cambio, un reale controllo su tale azione pubblica al fine di garantirne l'effettiva soggezione ai fondamenti dello Stato di diritto sociale e democratico; e ciò anche considerando il rischio di politicizzazione che tale attività può comportare senza un adeguato esame degli scopi a cui serve. In questo senso, al di là della necessaria riservatezza che è richiesta da parte dell'attività di sicurezza nazionale per essere efficace (artt. 103.1 e 105.b CE), il suo sviluppo normativo, ancora incentrato sulla Legge precostituzionale 9/1968, del 5 aprile, in materia di segreti ufficiali[133], impedisce drasticamente una declassificazione automatica con la quale raggiungere una maggiore legittimità e controllo democratico almeno negli anni (a titolo di responsabilità differita), che riteniamo essenziale rispetto al potenziale intervento pubblico in relazione alla disinformazione e alla disaffezione costituzionale e democratica (come già sottolineato). Non si tratta solo del fatto che oggi sia necessario un nuovo regime giuridico sulla segretezza che si presenti più in linea con l'estensione della sicurezza (e in stretto equilibrio e rispetto con il necessario controllo giuridico, politico e sociale con cui rendere effettivo lo stato di diritto democratico), ma è anche necessario approfondire l'effettiva trasparenza di un'azione pubblica che, pur garantendo la democrazia, rischi di metterla a rischio[134]. In tal senso, non sarebbe un male una maggiore collaborazione istituzionalizzata a livello pubblico con i rappresentanti dei social network e dei media, in modo che, sulla base del pluralismo che ispira sia il sistema democratico spagnolo, sia la libertà di espressione e informazione (artt. 1.1 e 20 CE, ancora) si sono resi partner nel delicato compito di garantire la sicurezza della democrazia dinanzi alla disinformazione (in base agli articoli 5 e 8 della citata l. 36/2015).

È inoltre necessaria una regolamentazione più adeguata dell'attività di sicurezza nazionale in Spagna dinanzi ai diritti fondamentali e alle libertà pubbliche in generale; in molti casi, tale azione (come l'intelligence) resta in un quadro anomico e silenzioso contrario allo sviluppo costituzionale raggiunto tramite la garanzia della riserva di legge e il contenuto essenziale dei diritti fondamentali (art. 53.1 CE)[135], che genera anche logiche di sfiducia politiche e sociali, anche paura (la limitazione stessa dei diritti), in relazione all'azione dei poteri pubblici al fine di garantire proprio la democrazia di fronte ad attacchi esterni ed interni ad essa.

Ma una concezione di democrazia che si propone in queste pagine, non dimentichiamolo, dal pluralismo e dalle minoranze, e della cui garanzia e sicurezza sono diretta-

[133] Sebbene in conformità con la sua successiva riforma con legge 7 ottobre 1978, n. 48, mentre è integrata dalla legge 11 maggio 1995, n. 11, che regola l'uso e il controllo dei crediti destinati a spese riservate. Al respecto, v. J. F. Sánchez Barrilao, *Servicios de inteligencia, secreto y garantía judicial de los derechos*, in *Teoría y Realidad Constitucional*, 44, 2019, spec. 319-320.

[134] J. F. Sánchez Barrilao, *Democracia, desafección constitucional y seguridad*, in *Revista de Derecho Constitucional Europeo*, núm. 33, 2020.

[135] Cfr. J. F. Sánchez Barrilao, *Inteligencia y seguridad como objeto constitucional,* cit., 423 ss.

mente responsabili i poteri pubblici in quanto democratici e costituiti (art. 1.2 e 9.1 CE), nonché promotori e protettori dei diritti e delle libertà fondamentali degli individui, nonché delle stesse minoranze (Tít. I CE). Una concezione della democrazia, dunque, nella cui difesa siamo tutti coinvolti di fronte alla sua disaffezione e potenziale regressione, e alla quale devono partecipare gli stessi *social network* come mezzo qualificato di comunicazione e relazione sociale e politica; ciò perché Internet continua ad essere uno spazio aperto in cui scoprire e approfondire forme nuove e positive di interazione collettiva[136]. Una concezione di democrazia, infine, capace di affrontare adeguatamente le nuove sfide e problemi posti dalla globalizzazione e dal progresso tecnologico a livello sociale (come è stato evidenziato), evitando così l'impotenza della persona che li precede; non invano, qui sta il vero carburante della disinformazione, della paura e del populismo oggi[137].

[136] J. F. Sánchez Barrilao, *Sobre youtubers y la neutralidad de la red*, in Aa. Vv. *Desafíos de la protección de menores en la sociedad digital: Internet, redes sociales y comunicación*, Valencia, 2018, 195.

[137] J. F. Sánchez Barrilao, *Sociedad del miedo y desafección constitucional*, in *Revista de Derecho Político*, 108, 2020, 97 ss.

Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*

Marco Bassini

Abstract

Il saggio propone una panoramica di diritto comparato sulla più recente giurisprudenza statunitense ed europea relativa alla qualificazione giuridica dei social network, alla vigilia di importanti riforme che riguarderanno la disciplina dei servizi digitali a livello dell'Unione europea. L'obiettivo del contributo è mettere in evidenza come la frequente assimilazione di tali soggetti e dei relativi servizi ai caratteri di pubblicità possa comportare conseguenze non necessariamente favorevoli sul piano della tutela della libertà di espressione.

The paper draws a comparative overview on recent case law developments in the US and Europe concerning the legal status of social networks, which stands out as a hot topic in light of the upcoming reform that European Union institutions are planning in the field of digital services. The goal of the paper is to bring to light how the frequent claim that social networks should be equalized to public fora or state actors and that the relevant services should be treated likewise may trigger unintended consequences for freedom of expression.

Sommario

1. Introduzione. – 2. L'alba di un mondo nuovo: genesi ed evoluzione delle piattaforme nel cyberspazio. - 3. Internet come *digital marketplace of ideas*? Le ricadute del nuovo ecosistema digitale sulla tutela della libertà di espressione. – 4. La giurisprudenza statunitense e i limiti alla equiparazione tra social network e forum pubblici. - 5. *PragerU* e la dimensione "prettamente orizzontale". Il possibile ricorso alla *state action doctrine*. – 6. Dall'altra sponda dell'Atlantico: il dibattito in Europa e in Italia. – 7. Conclusioni

Keywords

social network – libertà di espressione – Internet service provider – poteri privati – deplatforming

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1. Introduzione

Un social network privato che offre ai suoi utenti, sulla base di un contratto, uno spazio virtuale per la condivisione di manifestazioni di pensiero può censurare il politico forse più potente al mondo? Una decisione di tale natura, perfettamente lecita sulla base delle condizioni contrattuali, può essere comunque ritenuta foriera di un'effrazione sul piano costituzionale? Sono domande complesse, per rispondere alle quali occorre fare luce sulla tenuta di alcune categorie del mondo "reale" nell'ambito digitale. L'obiettivo di questo scritto è di indagare la dimensione di conflitto tra potere e libertà, nonché tra potere pubblico e potere privato che si dà sulla rete Internet e che, tra le altre, sembra emergere dalle più recenti vicende relative alla sorte degli account ospitati dai più importanti social network appartenuti all'ex presidente degli Stati Uniti d'America Donald Trump[1].

In questo contributo, provando a fare tesoro di riflessioni già maturate analizzando il mutamento di paradigma che la libertà di espressione conosce in ambito digitale[2], tenterò di rispondere, con l'ausilio della prospettiva comparata, ad alcuni quesiti che esigono risposta in merito alla qualificazione giuridica dei social network.

Mi domanderò, in particolare, se la metafora che descrive Internet e soprattutto i social network come spazio e/o luogo pubblico obbedisca a una finalità meramente descrittiva, che intercetta la moltitudine variegata di interazioni che intercorrono al giorno d'oggi in rete, ovvero sottenda una qualche valenza o pretesa di carattere normativo[3].

In correlazione a quest'ultima opzione, tenterò di appurare se la giustificazione delle scelte di moderazione operate da social network come Twitter o Facebook in un caso come quello che vede per protagonista Trump (c.d. *deplatforming*) possa riposare sulla natura squisitamente privatistica della relazione che avvince contrattualmente utenti e prestatori di servizi[4]. Agli occhi del costituzionalista, infatti, il richiamo alla natura contrattuale e pattizia del rapporto tra le parti quale fondamento del potere di esercitare una "censura privata"[5] potrebbe non sembrare del tutto appagante. Questa giustifica-

---

[1] Si v. il comunicato di Twitter, *Permanent suspension of @realDonaldTrump,* in ***blog.twitter.com,*** 8 gennaio 2021 e quello di Facebook, in G. Rosen-M. Bickert, *Our Response to the Violence in Washington*, in ***facebook.com***, 6 gennaio 2021. Cfr. anche il post Facebook pubblicato a questo url da Mark Zuckerberg il 7 gennaio 2021. Per una ricostruzione accurata della vicenda, si v. anche M. Isaac-K. Conger, *Facebook Bars Trump Through End of His Term*, in ***nytimes.com,*** 7 gennaio 2021. Nella dottrina statunitense, tra gli altri, v. D. Keller, *Who decides what stays on the Internet,* in ***theverge.com,*** 12 gennaio 2021.

[2] Sia consentito il richiamo, volendo, alle riflessioni già esposte in M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali,* Roma, 2019.

[3] Sulla molteplice valenza delle metafore nel linguaggio giuridico si v. A. Morelli-O. Pollicino, *Le metafore della rete. Linguaggio figurato, judicial frame e tutela dei diritti fondamentali nel cyberspazio: modelli a confronto,* in *Rivista AIC,* 1, 2018.

[4] In termini generali, cfr. D. Keller, *Who Do You Sue? State and Platform Hybrid Power Over Online Speech,* Aegis Series Paper No. 1902; D. Hudson, *In the Age of Social Media, Expand the Reach of the First Amendment,* in *American Bar,* 43(4).

[5] Cfr. in particolare M. Monti, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale*, in *Rivista italiana di informatica e diritto*, 1, 2019, 35 ss. Volendo, si rinvia anche a M. Bassini, *Fundamental Rights and Private Enforcement in the Digital Age*, in *European Law Journal,* 25(2), 2019, 182 ss.

zione, formalmente inattaccabile, pare infatti trascurare una componente significativa del problema in discorso dal punto di vista sostanziale, perdendo di vista la crescente attitudine delle piattaforme digitali ad atteggiarsi nei confronti degli individui come veri e propri "poteri"[6] che entrano perciò in competizione con gli attori pubblici statali[7]. Proprio quest'ultima dimensione acquisisce particolare evidenza nella vicenda relativa alla sospensione degli account di Donald Trump[8]; e, come tenterò di affermare, la tematica si mantiene di cogente attualità anche a voler considerare la reazione di Twitter e Facebook un esercizio censorio che ha fatto corretta applicazione dei limiti alla libertà di espressione negli Stati Uniti[9]; sembrerebbe esserne riprova, del resto, la recente approvazione di una discussa legge dello Stato della Florida volta a contrastare le pratiche di *deplatforming*[10].

---

[6] Nella dottrina italiana, questa categoria è stata esaminata *in primis* da G. Lombardi, *Potere privato e diritti fondamentali,* Torino, 1970, soprattutto in relazione alla idoneità a determinare limitazioni e compressioni dei diritti degli individui alla luce della posizione di dominanza occupata degli attori privati. Cfr. anche, da una prospettiva di diritto private, C.M. Bianca*, Le autorità private*, Napoli, 1977, recentemente "riletto", anche alla luce delle evoluzioni tecnologiche, da P. Sirena-A. Zoppini (a cura di), *I poteri privati e il diritto della regolazione*, Roma, 2018 (in cui si v. nello specifico, con riferimento ai prestatori di servizi Internet, S. Martinelli, *L'autorità privata del provider,* ivi, 555 ss.). Riferimenti utili, seppur in via generale, con riguardo alla posizione del privato a livello costituzionale anche in P. Barile, *Il soggetto privato nella Costituzione italiana*, Padova, 1953. Sulla specifica rilevanza del ruolo delle piattaforme digitali per la democrazia, con riguardo al loro impatto sulla libertà di espressione, si v. M. Monti, *Le* Internet platforms, *il discorso pubblico e la democrazia,* in *Quaderni costituzionali,* 4, 2019, 811 ss.

[7] Per alcune riflessioni su questi temi da una prospettiva diversa da quella giuridica, cfr. S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019; T. Gillespie, *Custodians of the Internet,* New Haven-London, 2018. Da un diverso angolo visuale ancora, si v. M. Sorice, *La «piattaformizzazione» della sfera pubblica,* in *Comunicazione Politica,* 3, 2020, 371 ss.

[8] Si tratta di una dimensione ben visibile, peraltro, nella *concurring opinion* consegnata lo scorso 5 aprile 2021 da Justice Thomas in occasione della decisione della Corte Suprema in *Knight Institute v. Trump,* ora *Joseph Biden, Jr., President of the United States, et al., v. Knight First Amendment Institute at Columbia University, et al.,* 593 U. S. ____ (2021), no. 20-197, ultimo tassello della vicenda giurisprudenziale che si descriverà con maggior dettaglio nel par. 3. La Corte Suprema ha accolto il ricorso avanzato da Trump volto a ottenere che fosse dichiarata priva di oggetto la causa precedentemente intentata nei suoi confronti (e conclusasi con una pronuncia della Court of Appeals per il Second Circuit) per effetto del venir meno, *medio tempore,* della carica presidenziale che aveva costituito il presupposto della decisione. Senza anticipare quanto più compiutamente esposto *infra,* la *concurring opinion* rileva come, al di là dell'inquadramento giuridico delle limitazioni imposte agli utenti da account appartenenti a *state officials*, il nodo centrale è rappresentato dal potere concentrato nelle mani di piattaforme private di condizionare il *free speech,* per esempio sospendendo o cancellando gli account di queste stesse *public figures.* Proprio per questo motivo Justice Thomas propone di elaborare un inquadramento di questi attori alla stregua di *common carriers* o, in alternativa, come *places of public accommodation*, opzioni che consentirebbero di sottoporli a una regolazione più stringente, escludendo così per via legislativa il potere di rimuovere gli account dei propri utenti.

[9] In tal senso si argomenterà oltre, ma merita anticipare la lettura di C. Melzi d'Eril-G.E. Vigevani, *Assalto al Congresso: perché non è colpa della rete ma di Trump,* in *Il Sole 24 Ore,* 8 gennaio 2021; O. Pollicino, *Odio e rabbia in rete, così il presidente ha nutrito i suoi sostenitori*, ivi, 8 gennaio 2021; A. Morelli, *Non scomodiamo Voltaire a proposito di Trump e dei social,* in *lacostituzione.info,* 10 gennaio 2021. Si v. anche F. Paolucci, *Il blocco dei social di Trump e la libertà di espressione online,* in *Ius in Itinere,* 15 febbraio 2021. Oltre i profili strettamente giuridici, merita attenzione l'indagine di M. Carone, *Trump e i social media,* in *Rivista Il Mulino,* 14 gennaio 2021. Con specifico riguardo alle tematiche della disinformazione e dell'odio online, si rinvia all'approfondita analisi offerta nel volume di G. Pitruzzella-O. Pollicino, *Disinformation and Hate Speech. A European Constitutional Perspective,* Milano, 2020. Da una prospettiva ancora diversa A. Palmieri, *Social è responsabilità!,* Milano, 2021.

[10] Lo scorso 24 maggio 2021 il governatore dello Stato della Florida ha firmato una legge denominata

Se queste suggestioni presentano un qualche fondamento, allora la domanda sullo statuto giuridico dei social network non può essere sbrigativamente liquidata facendo appello alla pur incontestabile natura contrattuale del rapporto con gli utenti (una prospettiva che rischia di non fotografare parte importante del problema); e può essere ulteriormente sviluppata cercando di comprendere se e in quale misura si possa assistere a una "compenetrazione" con effetti orizzontali della libertà di espressione[11]. Queste domande nascono peraltro all'indomani di quella che si preannuncia come una svolta a livello europeo, segnata dalla presentazione, lo scorso 15 dicembre 2020, di una proposta di regolamento relativa a un mercato unico dei servizi digitali[12] (c.d.

"Stop Social Media Censorship Act" (Senate Bill 7072), disponibile in *flsenate.gov,* che prevede, tra le altre, sanzioni di natura pecuniaria a carico delle piattaforme (fino a 250.000 $ al giorno) nel caso di disattivazione dell'account (*deplatforming*) di candidati a cariche politiche. La norma contenuta nel par. 2 della Section 2 – Section 106.072, Florida Statues, dispone segnatamente che: «*A social media platform may not willfully deplatform a candidate for office who is known by the social media platform to be a candidate, beginning on the date of qualification and ending on the date of the election or the date the candidate ceases to be a candidate. A social media platform must provide each user a method by which the user may be identified as a qualified candidate and which provides sufficient information to allow the social media platform to confirm the user's qualification by reviewing the website of the Division of Elections or the website of the local supervisor of elections*». Questa legge è stata presentata dalle stesse autorità della Florida come una reazione al *political bias* che soprattutto i sostenitori repubblicani denunciano da tempo da parte delle piattaforme digitali, a loro dire particolarmente inclini a silenziare le voci di esponenti conservatori. La legge, unico tra i vari progetti elaborati in materia a giungere a maturazione, è stata già oggetto di impugnazione davanti alla District Court for the Northern District of Florida – Tallahssee Division, con un *complaint for declaratory and injunctive relief* presentato il 27 maggio da Netchoice e CCIA (Computer & Communications Industry Association), Case 4:21-cv-00220-RH-MAF, disponibile in *ccianet.org*. La legge pare *ictu oculi* di difficile tenuta costituzionale, alla luce sia del possibile contrasto con il Primo Emendamento sia della manifesta difformità di queste previsioni rispetto alla Section 230 del Communications Decency Act, legge federale approvata dal Congresso nel 1996 che esclude in via generale (salvo limitate eccezioni) la responsabilità delle piattaforme digitali per la moderazione di contenuti, come si dirà meglio *infra* nel par. 2. Cfr. G. Edelman, *Florida's New Social Media Law Will Be Laughed Out of Court,* in *wired.com,* 24 maggio 2021, che riporta tra l'altro l'autorevole opinione, nel senso sopra descritto, di Michael Froomkin.

[11] Sul tema dell'efficacia con effetti orizzontali dei diritti fondamentali in ambito digitale si v. G. Resta, *Diritti fondamentali e diritto privato nel contesto digitale,* in G. Resta-F. Caggia (a cura di), *I diritti fondamentali in Europa e il diritto privato,* Roma, 2019, 117 ss., spec. 118, il quale evidenzia, tra i fattori di discontinuità rispetto al passato, un capovolgimento del rapporto tra potere pubblico e potere privato, in quanto «il governo delle relazioni digitali in rete è prevalentemente esercitato da soggetti privati, anche per il tramite degli strumenti tecnologici». In tema cfr. anche O. Gerstenberg, *Private Law and the New European Constitutional Settlement,* in *European Law Journal*, 10(6), 2004, 766 ss. e R. Van Loo, *The Corporation as Courthouse,* in *Yale Journal on Regulation*, 33(2), 2016, 547 ss. Per una rassegna in chiave storica dei mutamenti che hanno caratterizzato la dialettica tra diritto pubblico e diritto privato, cfr. anche B. Sordi, *Diritto pubblico e diritto privato. Una genealogia storica,* Bologna, 2020.

[12] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, Bruxelles, 15.12.2020, COM(2020) 825 final, 2020/0361(COD). Per una panoramica di contributi "a caldo" sulla proposta della Commissione si rinvia al simposio online "Verso il Digital Services Act" in *medialaws.eu*, in cui tra gli altri v. l'introduzione di O. Pollicino-M. Bassini-G. De Gregorio, *Verso il Digital Services Act: problemi e prospettive. Presentazione del simposio,* ivi, 23 novembre 2020. Cfr. anche M. Bassini-G. Finocchiaro-O. Pollicino, *L'Ue verso il Digital Services Act: quale equilibrio tra democrazia e potere,* in *agendadigitale.eu,* 15 febbraio 2021; G.M. Ruotolo, *Le proposte di disciplina di* digital services *e* digital markets *della Commissione del 15 dicembre 2020*, in *DPCE on line,* 4, 2020, 5419 ss., nonché M. Bassini, *L'Unione europea al grande passo: verso una regolazione di mercati e servizi digitali*, in *Quaderni costituzionali*, 1, 2021, 224 ss. Più in dettaglio, sul contenuto della proposta, cfr. G. Caggiano, *La proposta di Digital Service Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea,* in *Annali AISDUE,* 3, 2021, "Forum Servizi e piattaforme digitali", n. 1, 18 febbraio 2021.

"Digital Services Act"). Questo passaggio dovrebbe condurre a una riforma complessiva che modificherà l'impianto della Direttiva E-Commerce (direttiva 2000/31/CE), che nell'Unione europea rappresenta l'unico atto di respiro generale specificamente dedicato ai servizi digitali e contiene una scarna disciplina sulla responsabilità dei prestatori, ormai "imbozzolata" da più di un decennio di giurisprudenza quantomeno creativa[13].

Le risposte che cercherò di trarre da questa analisi dovrebbero consentire di comprendere meglio lo *status quo* e valutare, così, con cognizione di causa, le scelte che saranno compiute dal legislatore.

Per addivenire ad alcune, pur provvisorie e forse incomplete risultanze, il saggio procederà anzitutto da una sintetica analisi del ruolo delle piattaforme online e dell'intimo collegamento che lo stesso presentava alle origini e mantiene tuttora con la libertà di espressione. Una volta illustrato il punto di saldatura tra i due ambiti in parola, il paragrafo successivo metterà in luce le dinamiche di sovrapposizione tra sfera pubblica per la manifestazione del pensiero e dimensione privata del rapporto tra utenti e social network. Il saggio procederà, quindi, operando una ricognizione e una disamina critica della giurisprudenza statunitense che ha preso in considerazione la posizione dei social network alla luce della *public forum doctrine* e della *state action doctrine*. Si produrrà, quindi, in una comparazione con lo scenario domestico, paradigmatico dell'attitudine europea, esaminando gli spunti problematici della recente giurisprudenza formatasi in merito alla disattivazione delle pagine social di associazioni politiche di estrema destra. Così articolato il quadro comparato, il saggio tenterà di illustrare i motivi per cui appare preferibile resistere a ogni velleità di qualificazione in senso pubblicistico dei social network.

2. L'alba di un mondo nuovo: genesi ed evoluzione delle piattaforme nel cyberspazio

Alle origini di Internet, il cyberspazio era stato immaginato da alcuni dei commentatori più vicini alla sensibilità libertaria e "cyberanarcoide"[14] come il terreno di una possibile competizione "privata" tra comunità virtuali aliene dall'interferenza dei poteri statali. Ciascuna una piattaforma di libertà, caratterizzata da un novero di (poche

[13] Ci si riferisce, in particolare, alla creazione giurisprudenziale del c.d. *provider* attivo, su cui ci si soffermerà più diffusamente oltre, recentemente sdoganata anche dalla Cassazione italiana nella sentenza della sez. I civile, 21 febbraio 2019, n. 7708. Pesanti riserve su questa figura sono esposte in M. Bassini, *La Cassazione e il simulacro del provider attivo:* mala tempora currunt, in *questa Rivista,* 2, 2019, 248 ss. e altresì in L. Tormen, *La linea dura della Cassazione in materia di responsabilità* dell'hosting provider (attivo e passivo), in *La nuova giurisprudenza civile commentata*, 5, 2019, 1039 ss. A un giudizio positivo sulla configurazione di tale figura perviene invece R. Panetta, *Il ruolo attivo degli intermediari di Internet e la conseguente responsabilità civile*, in *Diritto di Internet*, 2, 2019, 273 ss. Il tema ha trovato spazio, originariamente, nella giurisprudenza della Corte di giustizia: cfr. CGUE, cause riunite da C-236/08 a C-238/08, *Google France e Google Inc. c. Louis Vuitton et. al.* (2010); C-324/09, *L'Oréal et al. c. eBay* (2011); ma si v. anche la recentissima sentenza CGUE, cause riunite C-682/18 e C-683/18, *Peterson c. Google LLC, YouTube Inc. et al.; Elsevier c. Cyando* (2021).

[14] Su tutti, cfr. D.G. Post, *Anarchy State and the Internet,* in *Journal of Online Law*, article 3, 1995.

e semplici) regole definite dagli amministratori e condivise dagli aderenti: in sostanza, il rispetto di limiti di contenuto e di continenza verbale, pena l'esclusione[15]. Nessuna sanzione ulteriore, semmai la possibilità di transitare a una comunità diversa. Un sistema parallelo dominato da una sorta di "arbitraggio regolamentare", dove gli utenti avrebbero potuto "disporsi" e collocarsi a seconda delle rispettive inclinazioni e degli interessi coltivati. Per gli Stati, apparentemente, nessun ruolo e nessun potere: gli Stati, in questa ricostruzione, sono l'altrove, impossibilitati a predicare la propria sovranità e a estendere l'*enforcement* delle norme giuridiche entro uno spazio idealizzato come territorio separato[16].

Questa ricostruzione dai toni idealistici si fondava su due illusioni che si sarebbero di lì a breve disvelate. In primo luogo, l'assunto che questa compartimentazione in comunità private non avrebbe generato posizioni di potere favorite dall'accumulo di risorse economiche, con un condizionamento sull'organizzazione, sulla mole, e conseguentemente sulla genuina circolazione dei contenuti condivisi dagli utenti, condizionamento costituente un diretto precipitato del dischiudersi di strutture oligopolistiche nel mercato dei servizi (a tacitazione di quella pretesa concorrenza perfetta tra comunità virtuali). In secondo luogo, la ferrea convinzione inerente non soltanto all'impossibilità degli Stati di regolare il web ma anche alla non necessità di un loro intervento in un campo dove l'autonomia privata prometteva una *governance* efficiente, ridondando quel rifiuto della sovranità statale già predicato metaforicamente da John Perry Barlow nella Dichiarazione d'indipendenza del cyberspazio[17] e fatto oggetto di un *claim* normativo.

L'affermazione prepotente del ruolo degli intermediari e in particolare dei prestatori di servizi della società dell'informazione non ha soltanto segnato il superamento delle ricostruzioni che idealizzavano la rete come luogo d'elezione e di massima espressione della libertà, impermeabile ai poteri economici[18], ma ha altresì profondamente modificato, con l'evoluzione che questi servizi ha caratterizzato, le dinamiche di esercizio della libertà forse di più immediata percezione sul web[19]. Non si è trattato, però, di un percorso connotato da fratture o momenti traumatici; al contrario, si è assistito a una graduale crescita del potere delle piattaforme, favorita da un quadro regolamentare

[15] Per una accurata ricostruzione delle prime questioni sorte con l'avvento della rete, si v. T. Wu-J.L. Goldsmith, *Who Controls the Internet? Illusions of a Borderless World,* Oxford, 2006.

[16] D.R. Johnson-D.G. Post, *Law and Borders-The Rise of Law in Cyberspace*, in *Stanford Law Review*, 48, 1996, 1367 ss.; *contra* v. J.L. Goldsmith, *Against Cyberanarchy*, in *University of Chicago Law Review*, 65, 1998, 1199 ss. e la replica di D.G. Post, *Against "Against Cyberanarchy",* in *Berkeley Technology Law Journal,* 17, 2002, 1363 ss.

[17] J.P. Barlow, *A Declaration of the Independence of Cyberspace,* in *eff.org*, 8 febbraio 1996.

[18] Sul tema della possibile "costituzionalizzazione" di Internet, proposta al fine di mettere al "riparo" gli individui e i loro diritti a fronte dell'erompere di nuovi attori privati, cfr. G. Azzariti, *Internet e Costituzione*, in *Politica del diritto.*, 3, 2011, 367 ss.; S. Rodotà, *Una Costituzione per Internet*?, ivi, 3, 2010, 337 ss.; F. Gallo, *Democrazia 2.0. La Costituzione, i cittadini e la partecipazione*, Conversano, 15 settembre 2013, *in cortecostituzionale.it*.

[19] Cfr. F. Pasquale, *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*, in *Theoretical Inquiries in Law*, 17, 2015, 487 ss.; J.M. Balkin, *The Future of Free Expression in a Digital Age*, in *Pepperdine Law Review*, 36, 2009, 427 ss.

volutamente minimalista[20].

Proprio scelta di non regolamentare l'ecosistema digitale se non nei suoi pilastri essenziali (ossia la responsabilità dei prestatori di servizi) e secondo un approccio "minimo" e incentivante risponde probabilmente, in Europa come negli Stati Uniti (anche se non esattamente al pari degli Stati Uniti) alla percezione del valore strategico di queste infrastrutture per la circolazione di contenuti nel cyberspazio e dunque, indirettamente, alla centrale rilevanza delle piattaforme per la libertà di espressione[21]. In altri termini, l'opzione di non interferire da subito e secondo "scelte forti" nella regolazione di Internet reagirebbe alla rilevanza strategica di queste piattaforme per favorire un'ampia circolazione di contenuti. Non è un caso che a confortare tali rilievi depongano le ricostruzioni dottrinali che negli Stati Uniti hanno discettato sulla natura di *First Amendment rule* della Section 230 CDA[22], la prima norma introdotta dal Congresso nel 1996 per regolare il ruolo dei prestatori di servizi Internet[23], giungendo a esaltarne le virtù con l'icastica formula "*The Twenty-Six Words that Created the Internet"*[24]*,* ove non a discutere se questa norma non munisse invero, agli effetti pratici, la libertà di espressione di una copertura finanche più ampia di quella imposta dal Primo Emendamento[25]. L'intima connessione che segna la nascita dalla prima (e per certo tempo unica) regola su Internet nell'ordinamento statunitense sembra cogliersi, del resto, anche nello spirito della giurisprudenza della Corte Suprema, protesa ad affermare la vocazione libertaria della rete come piattaforma di inveramento del libero mercato delle idee[26], che sotto-

[20] In tema v. O. Lynskey, *Regulating 'Platform Power'*, LSE Law, Society and Economy Working Papers, 1, 2017.

[21] Sempre con riferimento al ruolo dei "poteri privati" che si affermano in rete e al loro impatto sul diritto alla manifestazione del pensiero cfr. M. Manetti, *Regolare Internet,* in *questa Rivista,* 2, 2020, 35 ss.; M. Betzu, *Libertà di espressione e poteri privati nel cyberspazio*, in *Diritto Costituzionale - Rivista quadrimestrale,* 1, 2020, 117 ss.; M. Cuniberti*, Potere e libertà nella rete,* in *questa Rivista*, 3, 2018, 39 ss.

[22] Cfr. nella dottrina statunitense C. Glynn, *Section 230 as First Amendment Rule*, in *Harvard Law Review*, 131, 2018, 2027 ss.; E. Goldman, *Why Section 230 Is Better Than the First Amendment*, in *Notre Dame Law Review Reflection*, 95(1), 2019, 33 ss.*;* ma v. anche K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in *Harvard Law Review*, 131, 2018, 1598 ss.; J.M. Balkin, *The Future of Free Expression in a Digital Age,* cit.; D.K. Citron-B. Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, in *Fordham Law Review*, 86, 2017, 401 ss.; R. Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, in *George Washington Law Review*, 76, 2008, 101 ss.

[23] Sulle origini della disciplina sulla responsabilità dei prestatori di servizi in Europa e negli Stati Uniti, si v. l'approfondita disamina di R. Petruso, *Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a raffronto*, Torino, 2019. Merita ricordare, già in questa sede, come l'introduzione della Section 230 del Communications Decency Act costituì il frutto di una scelta bipartisan volta a evitare possibili salti in avanti da parte della giurisprudenza in merito a una equiparazione in senso editoriale delle piattaforme online. Negli stessi lavori preparatori si scorgono, infatti, plurimi riferimenti alla volontà di prevenire esiti assai discutibili come quelli cui la Corte suprema dello Stato di New York era giunta nel caso *Stratton Oakmont v. Prodigy Services Company,* 1995 WL 323710 (N.Y. Sup. Ct. 1995), ritenendo che, per il solo fatto di aver implementato linee guida per la pubblicazione di contenuti e di aver incaricato un team di moderatori, la piattaforma dovesse essere qualificata alla stregua di un editore e così soggiacere al relativo standard di responsabilità, anziché a quello, più permissivo, per i distributori, già assecondato invece da una precedente, celebre decisione nel caso *Compuserve,* 776 F. Supp. 135 (S.D.N.Y. 1991).

[24] Cfr. J. Kosseff, *The Twenty-Six Words That Created the Internet*, Ithaca-London, 2019.

[25] V. per esempio E. Goldman, *Why Section 230 Is Better Than the First Amendment*, cit.

[26] Metafora elaborata nella fortunata quanto celebre *dissenting opinion* di Justice Holmes nel caso *Abrams*

porre a regolazione avrebbe perciò provocato più rischi che benefici[27].
Questi motivi non hanno in realtà impedito che si instaurasse, anche negli Stati Uniti (così come del resto in Europa[28]) un partecipato dibattito incentrato sulla possibilità di mitigare l'ampia forbice di immunità garantita ai prestatori di servizi dalla Section 230[29], segno della percezione di una ormai compiuta sofisticazione delle caratteristiche dei servizi cui non ha fatto seguito, per il momento, una parallela evoluzione del paradigma normativo[30].
La scelta di non corrispondere a quella sofisticazione nelle caratteristiche dei servizi sotto il profilo normativo riflette il prevalere del timore che una regolazione potesse tradursi in costringimenti eccessivi, forieri di conseguenze negative per la libertà di espressione. Ma a distanza di oltre vent'anni, i tempi paiono maturi per un intervento che sappia opportunamente coniugare il ruolo di "volano della libertà di espressione" con l'esigenza di ricondurre a un pur minimo set di regole il dispiegarsi della libertà di iniziativa economica[31], incanalando servizi tra loro diversi entro binari normativi altrettanto eterogenei secondo una logica di modularità[32].
Tuttavia, proprio per valutare la bontà dei propositi di riforma e dei futuri esiti di

v. United States, 250 U.S. 616, 630 (1919): «*the best test of truth is the power of the thought to get itself accepted in the competition of the market*». Sui pericoli di una ricezione supina di tale metafora nell'ambito digitale, cfr. O. Pollicino, *Fake news, Internet and metaphors (to be handled carefully),* in *Italian Journal of Public Law,* 1, 2017, 1 ss.

27 *Reno v. ACLU,* 521 U.S. 844, 885 (1997): «*As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship*».

28 In Europa molti tribunali nazionali, in Italia in particolare, anche sulla scorta di alcune pronunce della Corte di giustizia, hanno fatto emergere la figura, già ricordata *supra,* del prestatore di servizi "attivo" (c.d. *provider* attivo) onde applicare in modo più rigoroso e restrittivo il regime giuridico di favore previsto dalla direttiva 2000/31/CE. Il tentativo è stato percorso onde attribuire rilievo a caratteristiche nella gestione del servizio tali da denotare, ad avviso dei giudici, la sussistenza di un controllo. Si tratta, però, di una figura priva di un chiaro fondamento normativo, se si eccettua il considerando 42 della direttiva medesima (che esige dagli intermediari la prestazione di un servizio meramente tecnico, automatico e passivo). Su questi temi cfr. il volume di O. Pollicino-E. Apa, *Modelling the liability of internet service providers: Google vs. Vivi down. A constitutional perspective,* Milano, 2013.

29 Nella giurisprudenza, tuttavia, questo argomento non sembra aver fatto breccia, specialmente nelle decisioni più recenti e rilevanti; si v., per esempio, la causa *Caraccioli v. Facebook,* 167 F. Supp. 3d 1056 (N.D. Cal. 2016) poi decisa anche dalla Corte d'appello per il Ninth Circuit (0:17-cv-15443).

30 Va da sé che domande più generali si sono poste, a fronte dell'avvento di Internet, anche in relazione alla adeguatezza del parametro rappresentato dal Primo Emendamento. V. in tal senso T. Wu, *Is the First Amendment Obsolete?,* in *Michigan Law Review,* 117, 2018, 547 ss.

31 Sul cambio di paradigma che sembra "respirarsi" a livello dell'Unione europea nel campo della regolazione delle tecnologie digitali, si v. le ponderate riflessioni di G. De Gregorio, *The rise of digital constitutionalism in the European Union,* in *International Journal of Constitutional Law,* 2021, 1-30. Sulla rilevanza del formante giurisprudenziale in questo processo di alienazione dell'Unione europea da una matrice di liberalismo economico, cfr. O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?,* Oxford, 2021.

32 Questo sembra essere, perlomeno, l'atteggiamento sotteso alla proposta di regolamento, già menzionata, nota come Digital Services Act, che distingue tra quattro categorie, articolandole dal generale al particolare e prevedendo obblighi sempre più stringenti tanto più specifica risulta la tipologia considerata: il primo genere è quello dei servizi intermediari, all'interno dei quali si individua la specie dei servizi di *hosting*; all'interno di quest'ultima si differenziano poi le piattaforme online; da ultimo, la proposta isola, tra le piattaforme online, le c.d. piattaforme di grandi dimensioni.

questo processo occorre affrontare un nodo inevitabilmente connesso e ancora da districare, quello relativo allo statuto costituzionale dei social network, sempre più luogo di condivisione e scambio di idee e opinioni. E, infatti, attribuire ai prestatori di servizi che gestiscono social network la qualifica di servizio pubblico o comunque equiparare tali spazi di libertà, per esempio, a un *public forum* può determinare implicazioni di assoluto momento sul piano costituzionale. Occorre dunque comprendere se si tratti di velleità ben fondate sul piano giuridico onde calcolarne le eventuali conseguenze.

3. Internet come *digital marketplace of ideas*? Le ricadute del nuovo ecosistema digitale sulla tutela della libertà di espressione

Dato atto del legame che unisce il regime giuridico dei prestatori di servizi e la tutela della libertà di espressione, occorre valutare all'atto pratico quali sfide il nuovo ecosistema digitale popolato da "poteri privati" abbia provocato rispetto alla tutela di questo diritto[33].

Si è già tentato altrove[34] di argomentare come l'avvento di Internet abbia senz'altro prodotto un incremento "quantitativamente apprezzabile" della misura della libertà di espressione di cui gli individui godono online, mettendo nondimeno in discussione che a tale ampliamento meramente "quantitativo" corrisponda anche un maggior spazio di libertà sotto un profilo "qualitativo"[35]. Tale interrogativo reagisce alla constatata presenza, nell'ecosistema digitale, di prestatori di servizi che interpongono dinamiche di moderazione di contenuti fondate su proprie regole (incorporate nei termini e nelle condizioni d'uso)[36] all'interno della tradizionale direttrice verticale tra Stato e cittadino, ove il primo definisce tramite la legge (e cioè qualificando alcune fattispecie come illecite) i limiti alla libertà del secondo. Questa sofisticazione è già stata attentamente teorizzata ed esplorata nelle sue implicazioni pratiche in dottrina, soprattutto da Jack Balkin[37], e illustra la sovrapposizione che giunge a determinarsi tra una dimensione prettamente privata (quella che vede utenti e prestatori di servizi avvinti da una relazione contrattuale) e la sfera pubblica ove fluiscono le manifestazioni di pensiero, sempre più digitale e dunque dominata dalla presenza di intermediari.

Il problema al centro del presente saggio si collega esattamente a quest'ultima carat-

[33] In tema v. A. Koltay, *New Media and Freedom of Expression. Rethinking the Constitutional Foundations of the Public Sphere,* Oxford, 2019.

[34] Cfr., volendo, M. Bassini, *Internet e libertà di espressione,* cit., nonché O. Pollicino-M. Bassini, *Free speech, defamation and the limits to freedom of expression in the EU: a comparative analysis*, in A. Savin-J. Trzaskowski (eds.), *Research handbook on EU Internet law*, Cheltenham-Northampton, 2014, 508 ss.

[35] A ben vedere, l'incremento in senso "quantitativo" riflette la disintermediazione della libertà di parola dai media tradizionali; ma dal punto di vista qualitativo sembra scorgersi una nuova intermediazione (e quindi una re-intermediazione) frutto del ruolo nevralgico delle piattaforme online per la scambio e la condivisione di contenuti.

[36] Sul significato e sulle implicazioni della *content moderation,* v. G. De Gregorio, *Democratising Online Content Moderation: A Constitutional Framework,* in *Computer Law & Security Report,* 36, 2020.

[37] Cfr. J.M. Balkin, *Free Speech is a Triangle*, *in Columbia Law Review*, 118(7), 2018, 2011 ss.

terizzazione: si può ritenere (e se sì, fino a che punto) che la presenza di prestatori di servizi che forniscono gli spazi virtuali - gli ideali contenitori digitali di idee e opinioni - rappresenti un requisito essenziale e indefettibile perché possa ritenersi garantita agli individui la possibilità di manifestare il proprio pensiero? In altri termini, occorre chiedersi, ragionando *a contrario*, se la privazione della disponibilità di utilizzo (comunque venutasi a determinare) dei social network (il già ricordato *deplatforming*) possa configurare una menomazione della libertà di espressione costituzionalmente tutelata. Sottesa a questi interrogativi è dunque la ricerca di una possibile efficacia con effetti orizzontali dei diritti in gioco.

La domanda nasce da una osservazione di carattere empirico ma intercetta (e ambisce a rappresentare) un *claim* normativo: la privazione della possibilità di accesso ai social network determina inevitabilmente, nell'odierna società dell'informazione, quantomeno un depotenziamento (ma anche un vero e proprio impedimento, a seconda dei casi) nell'esercizio della libertà di espressione. Poiché la decisione di sospendere il servizio (ovvero di rimuovere un contenuto) potrebbe dipendere dall'*enforcement* del regolamento contrattuale in essere tra le parti e non necessariamente da una previa decisione giurisdizionale (espressione delle tradizionali garanzie che assistono le incisioni di matrice pubblica delle libertà costituzionali), è giocoforza interrogarsi se questi servizi si possano configurare alla stregua di *essential facilities* o, come recentemente si è proposto[38], di servizi erogati da *common carrier,* assumendo una connotazione di "pubblicità" che potrebbe giustificarne l'assoggettamento a un particolare statuto giuridico e introietterebbe nella relazione prettamente privata e orizzontale tra utente e social network riflessi di natura costituzionalistica legati alla possibile limitazione "per via privata" della libertà di espressione.

Guardando all'esperienza statunitense, senz'altro più vicina a queste problematiche, una prima opzione, di carattere oggettivo, potrebbe condurre a considerare i social network[39] alla stregua di *public forum*, assimilandoli cioè a quegli spazi aperti tradizio-

[38] In tal senso si v. la *concurring opinion* di Justice Thomas, cit., del 5 aprile 2021, in *Joseph Biden, Jr., President of the United States, et al., v. Knight First Amendment Institute at Columbia University, et al.,* 593 U. S. ____ (2021), cit.

[39] Si badi che l'indagine verte segnatamente non già sulla qualificazione giuridica della rete Internet nel suo complesso, bensì dei social network intesi come spazi privati su cui i gestori del servizio fanno *enforcement* delle condizioni d'uso sancite nel regolamento contrattuale. Su questi temi cfr. M.R. Allegri, *Ubi social Ibi ius. Fondamenti costituzionali dei social network e profili giuridici della responsabilità dei provider,* Milano, 2018, spec. 29 ss., la quale ipotizza una riconducibilità delle sole c.d. *social network communities* al novero delle formazioni sociali tutelate dall'art. 2 Cost. richiamandosi alle riflessioni elaborate pionieristicamente da P. Passaglia, *Internet nella Costituzione italiana: considerazioni introduttive,* in *ConsultaOnline,* 4, 2014, ove l'Autore ragionava di una possibile qualificazione a questa stregua della intera comunità degli utenti (prendendo le mosse dalla concettualizzazione a suo tempo operata da E. Rossi, *Le formazioni sociali nella Costituzione italiana,* Padova, 1989), con considerazioni poi riprese anche in Id., *Le formazioni sociali e Internet,* in T.E. Frosini-O. Pollicino-E. Apa-M. Bassini (a cura di), *Diritti e libertà in Internet,* Milano, 2017, 50 ss. Contesta recisamente questa opzione, invece, rifiutando il riconoscimento di una comunità di utenti di Internet, M. Cuniberti, *Tecnologie digitali e libertà politiche,* in *Diritto dell'informazione e dell'informatica,* 2, 2015, 273 ss., spec. 280. In particolare Allegri, op. ult. cit., spec. 37 ss. e 44 ss., accedendo a una risposta possibilista in merito, si interroga altresì se la configurazione delle comunità di utenti dei social network come formazioni sociali *ex* art. 2 (che comporterebbe per i pubblici poteri l'obbligo di garantire la tutela dei diritti inviolabili degli appartenenti alle comunità) possa comportare l'adesione a uno dei paradigmi costituzionali particolari delineati dall'art. 17 o dall'art. 18 con riferimento alla libertà di riunione e alla libertà di associazione. Con riguardo a quest'ultima, l'Autrice sembra non ritenere necessariamente di

nalmente deputati all'incontro tra persone e dunque allo scambio di manifestazioni di pensiero. Proprio per via della loro naturale destinazione, questi spazi sono tendenzialmente compatibili soltanto con restrizioni contenutisticamente neutrali alla libertà di espressione, con la conseguenza che risultano vietate le discriminazioni fondate unicamente sul merito delle opinioni e idee (c.d. *viewpoint discrimination*)[40].

A un risultato sostanzialmente analogo si potrebbe poi addivenire, secondo una diversa opzione, operando una qualificazione in senso soggettivo dei prestatori di servizi come "attori pubblici" ai sensi della *state action doctrine,* oppure come *common carriers,* come suggerito da una recente *concurring opinion* di Justice Thomas.

Occorre, però, affermare con fermezza il significato profondamente e intimamente normativo di ogni ri-qualificazione in questo senso delle piattaforme social. Spesso, infatti, nel linguaggio comune (ma anche in quello tecnico, come si dirà a breve…), pare diffuso il ricorso a semplificazioni che legano a queste infrastrutture un valore e un significato di "agorà digitale" senza un pieno intendimento delle conseguenze giuridiche che da tale opzione, inevitabilmente normativa (ancorché frutto di una valutazione politica), scaturirebbero. Non è un caso che proprio su queste sottili ma dirimenti qualificazioni si sia aperta una garbata disputa in seno alla Corte Suprema tra Justice Kennedy e Justice Alito in una delle più interessanti pronunce su questo tema ossia

ostacolo il problema, da alcuni già puntualmente affrontato (in specie da S. Sassi, *La libertà di associazione nel "nuovo ecosistema mediatico": spunti problematici sull'applicazione dell'art. 18 della Costituzione. Il (recente) caso dell'associazione xenofoba on-line,* in *Rivista AIC,* 2, 2013), della pretesa all'anonimato degli utenti. In merito all'applicazione dello statuto della libertà di riunione, invece, l'Autrice individua quale principale ostacolo il tradizionale intendimento in senso fisico del luogo entro cui occorre si realizzi una compresenza di individuo, che parrebbe nondimeno superabile alla luce di alcune aperture giurisprudenziali rispetto alla considerazione dei social network come luogo aperto al pubblico (così Cass. pen., sez. I, 12 settembre 2014, n. 37596; su cui si v. M. Mezzanotte, *Facebook come "luogo aperto al pubblico",* in *federalismi.it,* 2, 2016). Sul possibile ricorso al paradigma dell'art. 17 cfr. anche M. Betzu, *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio,* in *Rivista AIC,* 4, 2012; A. Pirozzoli, *La libertà di riunione in Internet*, in *Diritto dell'informazione e dell'informatica*, 4-5, 2004, 595 ss.; e P. Marsocci, *Lo spazio di Internet nel costituzionalismo*, in *costituzionalismo.it,* 2, 2011. Rispetto allo statuto costituzionale della rete, rimangono naturalmente insuperate le considerazioni di P. Costanzo, (voce) *Internet (Diritto pubblico)*, in *Digesto delle discipline pubblicistiche*, Agg., Torino, 2000, 347 ss.

[40] La Corte Suprema ebbe modo di formulare compiutamente questa dottrina nel caso *Hague v. Committee for Industrial Organization*, 307 U.S. 496 (1939), riprendendo gli spunti già elaborati in *Davis v. Massachussets*, 167 U.S. 43 (1897). Nel caso *Hague* fu teorizzato che compito dello Stato è di evitare ogni discriminazione e di riconoscere la più ampia latitudine all'esercizio della libertà di parola in quegli spazi che sono «*immemorially been held in trust for the use of the public […] for purposes of assembly, communicating thought between citizens, and discussing public questions*». Si può affermare che tale dottrina corrisponda a una declinazione sostanziale della libertà di espressione: tale diritto non deve essere riconosciuto soltanto "sulla carta" ma deve essere concretizzato da parte dei poteri pubblici con la garanzia di spazi entro cui i cittadini possano confidare nell'indisturbato e incensurato fluire delle loro opinioni, funzionale ad assicurare il carattere democratico dello Stato. La Corte Suprema ha confermato questo indirizzo nella pronuncia di poco successiva *Schneider v. State*, 308 U.S. 147 (1939) per poi sofisticare ulteriormente, nel corso degli anni, la sua elaborazione, distinguendo diverse ipotesi: spazi che costituiscono *traditional public forum* e che, secondo *Hague*, hanno "tradizionalmente" rivestito questa funzione nel corso del tempo (parchi, marciapiedi, strade); spazi che costituiscono *designated public forum*, ossia spazi di proprietà pubblica o di proprietà privata comunque soggetti a controllo pubblico (per esempio, aule seminariali all'interno delle università) che, pur non costituendo oggetto di una consolidata associazione con l'esercizio della libertà di espressione, sono stati aperti e destinati a questo scopo dallo Stato. Nell'ambito dei *traditional* e *designated public forum,* lo Stato può introdurre limitazioni inerenti esclusivamente a circostanze di tempo, luogo e modo.

Packingham v. North Carolina[41].

La sentenza ha dichiarato incostituzionale, per violazione del Primo Emendamento, una legge statale che aveva imposto un divieto di accedere a tutte le piattaforme di social networking a carico indiscriminatamente di coloro che fossero stati giudicati colpevoli di reati a sfondo sessuale[42]. La Corte Suprema ha evidenziato come la misura in questione fosse carente di proporzionalità, estendendosi anche a siti Internet che avrebbero potuto favorire il percorso di reinserimento sociale e di emenda dei condannati. Ciò che tuttavia merita segnalare in questa pronuncia è il linguaggio adoperato dalla Corte e dall'*opinion* di Justice Kennedy in particolare, in cui ridonda un parallelismo tra Internet, definita la moderna piazza pubblica, e una categoria, quella del *public forum*, che possiede un preciso significato nell'interpretazione data dalla giurisprudenza al Primo Emendamento[43]. Proprio questa correlazione è stata oggetto delle critiche esposte nella sua *concurring opinion* da Justice Alito, ad avviso del quale questa analogia con luoghi e spazi fisici sarebbe stata tracciata con eccessiva disinvoltura e tra concetti e categorie invero differenti tramite una serie di *undisciplined dicta* suggestivi di una corrispondenza non scevra da importanti implicazioni giuridiche. Particolarmente indicativa di questa critica è l'affermazione secondo cui «*if the entirety of the internet or even just 'social media' sites are the 21st century equivalent of public streets and parks, then States may have little ability to restrict the sites that may be visited by even the most dangerous sex offenders*». Nell'opinione di Alito sembra scorgersi la preoccupazione di evitare che la Corte suprema possa involontariamente, mediante una *loose rethoric*, cadere in quello che ritiene un errore, ossia equiparare indiscriminatamente Internet e i social network a un *public forum*. Questa non pare, per vero, essere stata la conclusione della Corte Suprema; che però si è fatta portatrice, a distanza di vent'anni, di una ideale continuità con il suo storico precedente nel caso *Reno v. ACLU,* con una esaltazione del cyberspazio (allora non ancora popolato dalle piattaforme e dai social network oggi ormai affermati) quale "luogo" di inveramento del libero mercato delle idee profetizzato da Justice Holmes nella celebre *dissenting opinion* del 1919.

Proprio la sentenza del 1997 aveva inaugurato un trittico di pronunce assai paradigmatiche dell'attitudine della Corte Suprema rispetto alla portata del Primo Emendamento nell'era di Internet. In quella sentenza, la Corte, oltre a esaltare le potenzialità irripetibili del mezzo, aveva evidenziato l'esigenza di preservarne l'immunità da una

---

[41] *Packingham v. State of North Carolina*, 582 U.S. ___ (2017). Nella fattispecie, la Corte suprema ha ritenuto che le limitazioni previste dal General Statute 14-202.5 della North Carolina, approvato nel 2008, non superassero il vaglio del c.d. *intermediate scrutiny*, ossia il test impiegato per vagliare la legittimità di restrizioni contenutisticamente neutrali alla libertà di espressione, che richiede che le misure siano *narrowly tailored* al fine di soddifare un *significant governmental interest*. Cfr. anche il commento per la sezione "The Supreme Court - Leading Cases", *First Amendment – Freedom of Speech – Public Forum Doctrine – Packingham v. North Carolina,* in *Harvard Law Review,* 131, 2018, 233 ss.

[42] Cfr. i commenti di O. Soldatov, *The Transformative Effect of Social Media: Preliminary Lessons from the Supreme Court Argument in Packingham v. North Carolina,* in *DPCE on line*, 2, 2017, 417 ss. ed E. Celeste, *Packingham v North Carolina: A Constitutional Right to Social Media?*, in *Cork Online Law Review*, 2018, 116 ss.

[43] Si v. le notazioni in tema di D.C. Nunziato, *From Town Square to Twittersphere: The Public Forum Doctrine Goes Digital,* in *Boston University Journal of Science and Technology Law,* 25(1), 2019, 1 ss. Cfr. anche, in generale, A. Ardito, *Social Media, Administrative Agencies, and the First Amendment,* in *Administrative Law Review,* 65(2), 2013, 301 ss.

regolazione che avrebbe potuto produrre più svantaggi che benefici[44]. Non a caso, la Corte aveva dichiarato incostituzionali disposizioni che perseguivano senz'altro uno scopo meritevole di tutela quale la protezione dei minori da contenuti nocivi; ma che, come nella vicenda più recente *Packingham,* risultavano sproporzionate alla luce della definizione eccessivamente ampia di contenuti "*indecent*" e "*patently offensive*". La legge finiva così per determinare una compressione oltre misura della circolazione di materiali che formavano oggetto di un diritto costituzionalmente tutelato da parte della popolazione adulta.

È evidente che, in un terreno dominato da un così ampio fervore libertario[45], il ruolo dei social network riveste un rilievo cruciale e la loro qualificazione giuridica costituisce pertanto un nodo da cui dipende l'effettività della tutela garantita dal Primo Emendamento.

Guardando oltreoceano, invece, l'Europa pare aver interpretato l'avvento di Internet come una conquista di sicuro valore, mantenendo tuttavia un approccio più temperato. E questo non soltanto, forse, per via del diverso valore assiologico che la libertà di espressione occupa nel costituzionalismo americano[46] e della differenza nella formulazione del contenuto di questa libertà che si ritrova nei rispettivi parametri costituzionali, ma anche per effetto della diversa attitudine delle corti europee, e della Corte di giustizia in particolare, verso un diritto concorrente della libertà di parola: il diritto alla privacy e alla protezione dei dati, vera e propria "ossessione europea"[47]. La stessa Corte europea dei diritti dell'uomo è parsa fare un uso abbastanza prudente dell'art. 10 rispetto ai casi che riguardavano possibili interferenze nell'esercizio di questa libertà perpetrate dagli Stati contraenti rispetto all'utilizzo di Internet[48]. Ne sono riprova, per esempio, le ondivaghe decisioni adottate con riferimento alla conformità all'art. 10, par. 2, CEDU di sanzioni irrogate nei confronti dei prestatori di servizi per aver omesso o ritardato la rimozione di contenuti anonimi[49] così come il tono tutt'altro che

---

[44] «*The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship*». 521 U. S. 844, 885 (1997)

[45] Senza dimenticare, però, che lo stesso Justice Alito aveva osservato, nella sua *opinion* (in parte *concurring,* in parte *dissenting*) nel caso *Elonis v. United States,* 575 US ___ (2015), spec. 6, i possibili risvolti problematici connessi all'utilizzo dei social network rispetto all'esercizio della libertà di parola e ai suoi confini: «*"Taken in context," lyrics in songs that are performed for an audience or sold in recorded form are unlikely to be interpreted as a real threat to a real person. Watts, supra, at 708. Statements on social media that are pointedly directed at their victims, by contrast, are much more likely to be taken seriously*».

[46] Si v. su tutti G. Bognetti, *La libertà di espressione nella giurisprudenza americana. Contributo allo studio dei processi dell'interpretazione giuridica,* Milano, 1958; Id., *Lo spirito del costituzionalismo americano: breve profilo del diritto costituzionale degli Stati Uniti,* Torino, 2000.

[47] Volendo, cfr. O. Pollicino-M. Bassini, *The Luxembourg Sense of the Internet: Towards a Right to Digital Privacy*, in *The Global Community Yearbook of International Law and Jurisprudence 2014,* Oxford, 2015, 223 ss.

[48] Su quest'intima connessione si v. in particolare i commenti alla giurisprudenza della Corte europea di M. Husovec, *Editorial: Intermediary Liability as a Human Rights,* in *JIPITEC,* 8, 2017, 181, § 1, e di R. Spano, *Intermediary Liability for Online User Comments under the European Convention on Human Rights*, in *Human Rights Law Review*, 17(4), 2017, 665 ss.

[49] Corte EDU, *Delfi c. Estonia*, ric. 64569/09 (2015); *Magyar Tartalomszolgáltatók Egyesülete (MTE), Index.*

enfatico proprio di quelle pronunce che avevano condannato gli Stati contraenti per violazioni manifeste della libertà di espressione costituite dall'oscuramento di intere categorie di siti Internet[50], al pari forse della relativa prudenza con cui si è affermata la rilevanza dell'utilizzo di Internet come strumento informativo a beneficio dei detenuti nel censurare misure statali che ne limitavano l'accesso[51].

Sebbene il contesto europeo non presenti apparenti convergenze rispetto al sentire proprio del costituzionalismo statunitense in relazione alla libertà di espressione, esso offre spunti di sicuro interesse per una comparazione transatlantica in rapporto soprattutto al tema dell'applicazione nei rapporti orizzontali dei diritti fondamentali in gioco, cui è inevitabilmente collegata la qualificazione giuridica (soggettiva ovvero oggettiva) dei social network[52].

4. La giurisprudenza statunitense e i limiti alla equiparazione tra social network e forum pubblici

Per comprendere la portata della discussione che finora si è animata sul tema della qualificazione dei social network e degli spazi virtuali da questi amministrati, e dunque della possibile rilevanza costituzionale dell'attività di moderazione "privata" di contenuti, occorre muovere dall'analisi della giurisprudenza statunitense. La casistica prodotta dalle corti d'oltreoceano, vuoi per una maggiore sensibilità libertaria del relativo contesto costituzionale, vuoi per una maggiore prossimità (anche meramente geografica) alle *big tech* e alle problematiche giuridiche che vi sono connesse, ha fornito interessanti chiavi di lettura utili a ordinare il dibattito secondo alcune preliminari coordinate.

Va detto, anzitutto, che i timori (giustamente) paventati da Justice Alito nella sua ricordata *concurring opinion* nel caso *Packingham* non sembrano, almeno per il momento, aver trovato seguito. Infatti, le corti che si sono pronunciate nelle vicende in cui era in questione una possibile equiparazione di Internet (e dei social network in particolare) a un *public forum*, hanno opportunamente delimitato il campo di applicazione di questa analogia, evitando di trarne conseguenze che avrebbero verosimilmente presentato riflessi "di sistema" ben più invasivi.

hu Zrt c. Ungheria, ric. 22947/13 (2016); *Rolf Anders Daniel Pihl c. Svezia*, ric. 74742/14 (2017). A riprova dell'assenza di una particolare armonia tra questa casistica, si v. il commento di P. Costanzo, *Quando in internet la Corte di Strasburgo continua a navigare a vista,* in *DPCE on line*, 3, 2017, 767 ss. Su questa giurisprudenza cfr. anche G.E. Vigevani, *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano,* in *Diritto dell'informazione e dell'informatica,* 2, 2014, 207 ss.; Id., *La responsabilità civile dei siti per gli scritti anonimi: il caso Delfi c. Estonia*, in *Forum di Quaderni costituzionali*, 4 febbraio 2014; L. Nannipieri, *L'aggiunta di commenti offensivi in calce ad un articolo di un portale informativo online in una recente sentenza della Corte Europea dei Diritti dell'Uomo*, in *medialaws.eu*, 13 gennaio 2014.

[50] Si v. per esempio Corte EDU, *Ahmet Yildirim c. Turchia,* ric. 3111/10, (2012).

[51] Si v. Corte EDU, *Kalda c. Estonia,* ric. 17429/10 (2016) e *Jankovskis c. Lituania*, ric. 21575/08 (2017). Su queste pronunce cfr. D. Galliani, *Internet e la funzione costituzionale rieducativa della pena*, in O. Pollicino-T.E. Frosini-E. Apa-M. Bassini (a cura di), *Diritti e libertà in Internet,* cit., 329 ss.

[52] Spiega il punto, evidenziando le differenze di approccio tra *state action doctrine* statunitense e *Drittwirkung* alla luce del diverso grado di sensibilità del costituzionalismo nordamericano ed europeo, O. Pollicino, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato,* in *questa Rivista,* 2, 2019, 138 ss.

L'occasione di affrontare questi nodi è sorta a seguito di alcune controversie aventi a oggetto la legittimità delle limitazioni attuate da account appartenenti a figure pubbliche rispetto alla possibilità di interazione con i propri utenti-*constituents*.

Il caso giudiziario forse più noto è quello che ha visto per protagonista l'ex presidente degli Stati Uniti Donald Trump (prima che i fatti di Capitol Hill suscitassero un nuovo capitolo della vicenda[53]), che era stato citato in giudizio per aver impedito ad alcuni utenti di interagire con il suo account @realDonalTrump (dunque non l'account "ufficiale" del presidente degli Stati Uniti @POTUS, migrato invece nei mesi successivi nella disponibilità del neo-presidente Biden), poi ingloriosamente sospeso in modo permanente, nei mesi successivi, da Twitter. Invero, è la stessa sentenza della Court of Appeals for the Second Circuit, che ha confermato il precedente della Corte distrettuale[54], a stabilire sin dall'inizio importanti limiti alla sua possibile portata innovativa: «*We do not consider or decide whether an elected official violates the Constitution by excluding persons from a wholly private social media account. Nor do we consider or decide whether private social media companies are bound by the First Amendment when policing their platforms. We do conclude, however, that the First Amendment does not permit a public official who utilizes a social media account for all manner of official purposes to exclude persons from an otherwise-open online dialogue because they expressed views with which the official disagrees*». Sgombrando così subito il terreno da possibili equivoci, i giudici d'appello hanno inteso delimitare puntualmente il perimetro della propria decisione, esclusivamente inerente alla possibilità per un account ospitato da una piattaforma privata ma utilizzato in un dato momento da uno *state official*[55]

[53] In merito a questa vicenda, è opportuno segnalare la recente decisione del Facebook Oversight Board che ha confermato la correttezza della decisione del social network di sospendere l'account di Trump, dal quale erano stati pubblicati contenuti di implicita approvazione in occasione dell'attacco al Campidoglio, richiamando però l'esigenza di una maggiore proporzionalità delle misure in questione con riferimento alla relativa durata (nella fattispecie, indefinita) e di maggiore trasparenza in relazione all'iter e ai criteri di adozione. Cfr. il comunicato *Il Comitato per il controllo conferma la sospensione per l'ex Presidente Trump e sostiene l'incapacità da parte di Facebook di imporre una sanzione adeguata,* in *oversightboard.com,* maggio 2021, nonché il testo integrale della decisione nel caso 2021-001-FB-FBR. In merito alla vicenda, cfr. il commento di M. Manetti, *Facebook, Trump e la fedeltà alla Costituzione,* in *Forum di Quaderni costituzionali,* 1, 2021, 195 ss.; ma v. anche l'editoriale di B. Caravita, *Davanti ad un mondo che cambia chi è più pericoloso tra Trump e Zuckerberg? Alla ricerca di una risposta che penetri nei meccanismi che governano la nostra vita in rete,* in *federalismi.it,* 1, 2021, 13 gennaio 2021. In merito alla decisione del Facebook Oversight Board si v. O. Pollicino-M. Bassini-G. De Gregorio, *Trump's Indefinite Ban. Shifting the Facebook Oversight Board away from the First Amendment Doctrine*, in *verfassungsblog.de*, 11 maggio 2021; A. Gerosa, *La tutela della libertà di manifestazione del pensiero nella rete tra Independent Oversight Board e ruolo dei pubblici poteri. Commenti a margine della decisione n. 2021-001-FB-FBR,* in *Forum di Quaderni costituzionali,* 2, 2021, 427 ss. In generale, sul ruolo dell'Oversight Board di Facebook, cfr. soprattutto K. Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, in *The Yale Law Journal,* 129, 2020, 2418 ss.; nonché A. Jr Golia, *Beyond Oversight. Advancing Societal Constitutionalism in the Age of Surveillance Capitalism*, in *Int'l J. Const. L. Blog*, 5 marzo 2021; P. Bianchi, Pieszczek *e l'Indipendent Oversight Board di FB: piccoli passi verso la censura collaterale,* in *Liber Amicorum Pasquale Costanzo – ConsultaOnline,* 10 febbraio 2020.

[54] *Knight First Amendment Inst. at Columbia Univ. v. Trump*, 302 F. Supp. 3d 541 (S.D.N.Y. 2018).

[55] La Corte d'appello ha puntualmente motivato la propria decisione evidenziando che, ancorché l'account in questione fosse intestato alla persona di Donald Trump e non riconducibile in quanto tale all'istituzione rappresentata dal presidente degli Stati Uniti d'America, inevitabilmente l'utilizzo da questi effettuato in costanza di carica fosse del tutto idoneo ad attrarlo nel campo degli *official, state-run account.* Nel motivare su tale qualificazione, i giudici hanno messo in luce che non vi è dubbio alcuno sul fatto che lo stesso account potesse configurarsi come uno spazio prettamente privato prima dell'elezione di Donald Trump a presidente e come lo stesso sarebbe verosimilmente "degradato" a tale originario status

di porre in essere limitazioni che costituiscono *viewpoint discrimination* tendenzialmente vietate. Non si tratta, dunque, di una vicenda dalla quale possono essere tratte chiavi di lettura "di sistema", le quali verosimilmente mal si attaglierebbero alla generalità dei casi. Tuttavia, la sentenza della Corte d'appello documenta in modo assai visibile quanto il discrimine tra forum pubblico e forum privato costituisca un crinale denso di implicazioni. Non è un caso che la difesa di Trump sia stata improntata principalmente sull'affermazione della natura meramente privata dello spazio creato da Twitter: nonostante quest'ultimo «*facilitates robust public debate on the Account*»[56], secondo l'ex presidente «*it is simply the means through which he participates in a forum and not a public forum in and of itself*»[57]. Nessuna di queste difese ha fatto tuttavia breccia nelle argomentazioni della Corte d'appello, che ha recisamente respinto questa impostazione per affermare che «*the President is a governmental actor with respect to his use of the Account*», circostanza da cui discende il divieto di effettuare *viewpoint discrimination,* in quanto tali contrarie al Primo Emendamento[58]. E il blocco di un account, secondo la decisione della Corte, integra senz'altro questa fattispecie, nella misura in cui impedisce agli utenti cui sono generalmente rivolte le esternazioni (di fatto, nella loro veste di *constituency*) di accedere e di interagire con le stesse (senza che ciò implichi, naturalmente, alcun obbligo, per converso, in capo al presidente o a qualsiasi *state official* di darvi ascolto o attribuirvi rilevanza): le reazioni degli utenti, sia in forma di replica sia in forma di condivisione (*retweet*) o di apprezzamento (*like*) sono del resto, esse stesse, *speech* costituzionalmente tutelato[59].

Cercando di decodificare la decisione, il messaggio che se ne ricava appare nitido e non sembra frutto di particolari forzature determinate dal contesto tecnologico di riferimento: sul web, e sui social network in particolare, le garanzie che contraddistinguono la libertà di espressione, nelle sue molteplici declinazioni, nel rapporto tra potere pubblico e individuo rimangono inalterate. Internet finisce, in questo frangente, per atteggiarsi analogamente ad altri media, imponendo che i pubblici poteri siano sottoposti alle rigorose limitazioni che il Primo Emendamento racchiude. Si assiste, semmai,

alla cessazione della carica. Tuttavia, le modalità di utilizzo e le connotazioni dell'account personale nel periodo dell'esercizio della carica erano tali da suffragare la qualificazione come spazio utilizzato da uno *state official*. La stessa Corte distrettuale aveva rilevato, con riguardo al requisito del *government control* ai fini della configurazione di un *public forum,* che: «*the President presents the @realDonaldTrump account as being a presidential account as opposed to a personal account and* […] *uses the account to take actions that can be taken only by the President as President*». 302 F. Supp. 3d 541, 567. Anche la Corte d'appello ha confermato, anzi rafforzato il punto, evidenziando come non vi fosse dubbio alcuno circa l'esistenza di un «*substantial and pervasive government involvement with, and control over, the Account*» (Case 18-1691, p. 17), confermato anche dal fatto che l'account fosse adoperato «*as a channel for communicating and interacting with the public about his administration*» (ivi, p. 18)

[56] Case 18-1691, p. 16.

[57] *Ibidem.*

[58] Si coglie in questa sede un interessante richiamo alla recente pronuncia della Corte Suprema nel caso *Manhattan Community Access Corp. et al. v. Halleck et al.*, 587 U.S. __ (2019), in cui la Corte aveva spiegato che: «*When the government provides a forum for speech (known as a public forum), the government may be constrained by the First Amendment, meaning that the government ordinarily may not exclude speech or speakers from the forum on the basis of viewpoint*».

[59] A commento di queste vicende, peraltro, v. anche P.L. Morris-S.H. Sarapin, *You can't block me: When social media spaces are public forums,* in *First Amendment Studies,* 54(1), 2020, 52 ss.

a un adattamento delle categorie rilevanti, con una riconduzione all'alveo delle attività espressive delle variegate modalità di interazione disponibili agli utenti. Non entrano così in gioco, in questa vicenda, eventuali obblighi "ulteriori" e "particolari" che si impongono alla piattaforma in quanto tale, in ragione della sua eccezionalità e della capacità pressoché unica e irripetibile di tradurre in pratica il libero mercato delle idee. La dialettica, del resto, non insiste nel rapporto tra utente e piattaforma ma tra utente e potere pubblico. La giurisprudenza sembra così riconoscere che di *public forum* possa parlarsi, nel contesto di Internet, solo in presenza di uno *state actor* vincolato al rispetto del Primo Emendamento.

Pur non profondendo un'argomentazione particolarmente dettagliata sui profili "di sistema", relativi alle connotazioni generali delle piattaforme social, le sentenze nella vicenda che ha riguardato Trump paiono sottendere che entro questo ecosistema non si ponga un problema di generalizzata applicazione della dottrina del *public forum*[60]. È questo un messaggio che esce confermato anche da un'altra vicenda per larghi tratti analoga: il caso *Davison v. Randall*, in cui la Corte d'appello per il Fourth Circuit[61], con una decisione di poco precedente a quella resa dal Second Circuit in *Knight First Amendment Institute v. Trump,* ha confermato la pronuncia della Corte distrettuale dell'Eastern District della Virginia[62]. Analogo, come detto, l'esito: la Corte ha ritenuto che sussistessero *viewpoint discrimination* in ragione della riconosciuta natura di forum pubblico della pagina Facebook della Chair Randall del Board of Supervisors della Contea di Loudoun dalla quale erano stati rimossi commenti e sospesi account riconducibili alla paternità di utenti non graditi.

La pronuncia della Corte d'appello si segnala però per un interessante inciso che potrebbe prestarsi per ragionare su implicazioni di sistema, un nodo che viene affrontato per respingere l'eccezione secondo cui, a dispetto della natura pubblica del suo utilizzo la pagina fosse ospitata da una piattaforma privata. Secondo i giudici, ferma restando l'assenza di una chiara connotazione in senso del tutto privato o pubblico di Facebook (un punto che sarebbe stato assai interessante esplorare[63]), la circostanza che una *property* sia privata, differenziandosi dalle *government-owned property,* non vale necessariamente a escluderla dalla possibile applicazione della dottrina del *public forum*, che la giurispru-

[60] Il che appare pienamente coerente con il contenuto della Section 230 del CDA che, come detto, esonera da responsabilità i prestatori di servizi per le attività di moderazione dei contenuti condotte in buona fede.

[61] No. 17-2002.

[62] 267 F. Supp. 3d 702 (E.D. Va. May 10, 2017). Le sentenze si sono appuntate, in questa vicenda, sulla rimozione di commenti e sospensione di account da parte della pagina pubblica Facebook gestita dalla Chair del Board of Supervisors della Contea di Loudoun, che veniva espressamente qualificata e connotata come appartenente a una figura pubblica che rivestiva un incarico politico e indubbiamente si poneva, in quella sfera, come uno *state official.*

[63] In realtà la Corte d'appello si è posta questo interrogativo (relegandolo però a un nota a piè di pagina…) in relazione non tanto al complessivo statuto giuridico applicabile ai social network in funzione del loro ruolo e della loro possibile connotazione come *public forum*, quanto invece in rapporto alla possibile natura proprietaria dei post e commenti pubblicati dagli utenti, argomento che, se applicato alle attività social di una pagina riconducibile a uno *state official,* sembrerebbe deporre a favore di una qualificazione come *government property.*

denza ha esteso anche a casi di proprietà private adibite a un uso pubblico[64]. Nel caso specifico, la pagina pubblica Facebook era stata creata appositamente da Chair Randall e così giungeva a costituire un *designated public forum*, in quanto soggetta, a dispetto della natura privata della piattaforma ospitante, al potere di controllo del suo amministratore, appunto uno *state official*.

Le argomentazioni sviluppate dalla Corte d'appello si sono senz'altro avvicinate al nucleo del problema che in questa sede si vuole indagare, senza però affrontarlo direttamente e anzi, forse, eludendolo. Vi è però un dato fondamentale che sembra potersi guadagnare anche da questa vicenda: la natura privata delle piattaforme non è, di per sé, circostanza necessariamente ostativa alla possibilità di scorgere nel relativo utilizzo le connotazioni di un *public forum*. In sospeso rimane, inoltre, il nodo relativo alla definizione delle circostanze che potrebbero giustificare una siffatta equiparazione: la domanda, in altri termini, è se sia dato immaginare che anche in presenza di soggetti che non rivestono qualità di *state official* possa realizzarsi un'analogia che dipenda da circostanze oggettive, legate alla peculiarità dello strumento. In altri termini: i social network sono *public forum* soltanto quando a utilizzarli sono figure che rivestono cariche pubbliche, sulle quali è attratto "l'obbligo costituzionale" di tutelare la libertà di espressione? Oppure esistono elementi in grado di supportare, ancorché in via di fatto, una conclusione analoga anche quando si controverta di una dinamica prettamente inter-privata, non riducibile al rapporto tra poteri pubblici e cittadini?

Sgombrando il campo da ogni equivoco, nelle due vicende appena commentate[65] gli account di Twitter e Facebook interessati paiono essere un "simulacro del potere": essi rappresentano e si identificano con attori statali, poteri pubblici indubbiamente tenuti a garantire la libertà di espressione senza operare discriminazioni di sorta fondate sul semplice contenuto delle manifestazioni di pensiero. La presenza di Facebook e Twitter rischia di equivocare, dunque, il vero nodo problematico da sciogliere, ossia se piattaforme online di natura privata possano attuare scelte di moderazione dei contenuti che potrebbero non essere consentite ai pubblici poteri, in quanto direttamente vincolati dal Primo Emendamento. Se quest'ultimo "filtra", superando la barriera legata alla natura privata dei social network, laddove i profili rilevanti appartengano ad attori statali, vi è da chiedersi se abbia eguale possibilità di penetrare nell'alveo delle relazioni

[64] *Cornelius v. NAACP Leg. Def. Fund,* 473 U.S. 788 (1985).

[65] Invero, non si tratta delle uniche occasioni in cui la giurisprudenza si è occupata, in terra statunitense, di questa tematica, addivenendo a conclusioni non sempre convergenti. Tra le altre, merita ricordare: *Morgan et al v. Bevin*, 298 F. Supp. 3d 1003 (E.D. Ky. 2018), decisione della Corte distrettuale dell'Eastern District del Kentucky che è approdata a conclusione opposta, sostenendo che sulle piattaforme online i *public officers* possono limitare il proprio uditorio senza per questo violare il Primo Emendamento; *Campbell v. Reisch*, No. 19-2994 (8th Cir. 2021), sentenza della Corte d'appello dell'Eight Circuit che ha stabilito che la scelta di una deputata dello stato del Missouri di bloccare un utente da Twitter non fosse contraria al Primo Emendamento, sull'assunto che l'account adoperato non fosse utilizzato per *governmental activity* (e che, pertanto, essa non lo utilizzasse *under the color of state law*), a differenza dei casi *Trump* e *Davison,* e non fosse pertanto inteso a funzionare come un *public forum*; la pronuncia *Robinson v. Hunt County*, 2019 WL 1594319 (5th Cir Apr. 15, 2019), in cui la Corte d'appello per il Fifth Circuit ha giudicato contraria al Primo Emendamento la "censura" operata su alcuni contenuti pubblicati sulla pagina ufficiale Facebook dello sceriffo della contea di Hunt, nonostante un *disclaimer* secondo il quale gli utenti erano invitati a pubblicare input e commenti positivi in relazione a temi di pubblico interesse ma la pagina non costituiva un *public forum*.

prettamente private che intercorrono non più tra pubblici poteri e cittadini bensì tra cittadini e soggetti privati che sembrano sempre più atteggiarsi e agire, tuttavia, alla stregua di poteri.

5. *PragerU* e la dimensione "prettamente orizzontale". Il possibile ricorso alla *state action doctrine*

Nel tentativo di formulare un giudizio sulla giurisprudenza delle corti statunitensi che si è illustrata nel paragrafo che precede, si può rilevare che le decisioni finora prodotte appaiono portatrici di una impostazione fortemente formalistica rispetto alla verifica e all'interpretazione delle condizioni che fanno di un account di un social network un *public forum*. Tale ricerca è imperniata, come si è messo in evidenza, sull'accertamento di un controllo riconducibile a un soggetto pubblico anche in presenza di una piattaforma di natura privata. Occorre però domandarsi se non si tratti di una lettura eccessivamente "notarile", che rischia di trascurare il fatto che le odierne piattaforme digitali non sono state create da attori pubblici ma, pur nate per scopi commerciali, rispondono comunque alle stesse finalità ultime per le quali i pubblici poteri hanno creato o designato *public forum*: consentire lo scambio di idee, opinioni e contenuti.
Sebbene l'assimilazione tra social network e *public forum,* proprio per la diversa matrice "storica" di queste categorie, non rappresenti necessariamente un risultato desiderabile (anzi, agli occhi di chi scrive si tratterebbe di un esito denso di criticità), sembrerebbe che, se si pone mente alla *ratio* sottostante a tale ultima categoria, l'esigenza di limitare la possibilità per i pubblici poteri di praticare delle *viewpoint discrimination* sia collegata alla particolare apertura garantita "per vocazione" da quei luoghi che sono qualificati per l'appunto come *public forum* e che assicurano per la natura loro propria degli spazi di libertà. L'interrogativo che sorge da queste considerazioni è se la mera circostanza che si tratti di spazi privati basti a privare gli individui delle tutele di cui gli stessi invece godono, in via generale e indifferentemente dal mezzo utilizzato, nel rapporto con i pubblici poteri. In altri termini, è possibile "traslare" le garanzie che tutelano l'individuo da possibili *viewpoint discrimination* dal rapporto con i poteri pubblici per proiettarle e introiettarle in quello che li avvince con i nuovi "poteri privati"?
Questa domanda impone di considerare la misura entro cui la definizione di poteri privati racchiuda un significato genuinamente normativo, a dispetto del diffuso e forse disinvolto ricorso a questa metafora, che simboleggerebbe la disponibilità di un potere di mercato così significativo da poter influenzare in misura apprezzabile anche i diritti e le libertà individuali[66].

[66] Il tema è particolarmente dibattuto nell'ambito della letteratura che si è occupata di trasparenza algoritmica, anche in relazione all'art. 22 del regolamento (UE) 2016/679 (GDPR). Solo per alcune coordinate, si rinvia a C. Casonato, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *DPCE*, fascicolo speciale, maggio 2019, 101 ss.; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 1, 2019, 63 ss.; F. Pasquale, *The Black Box Society. The Secret Algorithms that Control Money and Information*, Cambridge (MA), 2015; T. Zarsky, *The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making*, in *Science, Technology & Human Values,* 41(1), 2016, 118 ss.; D.K. Citron-F. Pasquale, *The Scored Society: Due Process For Automated Predictions,* in *Washington Law Review*, 89, 2014, 1 ss; D.K. Citron, *Technological Due Process*,

Indicazioni utili, in questa prospettiva, sembrano potersi cogliere nella sentenza *Prager University v. Google LLC* (oltre, "*PragerU v. Google*")[67] ove, a differenza della giurisprudenza già citata *supra,* la Corte d'appello del Ninth Circuit ha avuto la possibilità di esprimersi su un quadro spurio della presenza di soggetti riconducibili a *state officials*, in quanto tali vincolati dal Primo Emendamento. In questa vicenda il nodo non riguarda la conformità alla *free speech clause* delle condotte poste in essere da attori pubblici, ma si innesta direttamente sul rapporto privato tra utente (in questo caso, una persona giuridica, la Prager University) e piattaforma. La categoria che è stata chiamata in causa in questa sede allo scopo di verificare la possibile estensione a soggetti privati dei vincoli costituzionali (e in particolare del Primo Emendamento), nel tentativo di "normativizzare" quel richiamo ai "poteri privati", è quella della *state action*.

La dottrina in parola vanta origini antiche e affonda le sue radici nel costituzionalismo statunitense, nella profonda matrice libertaria che caratterizza questo ordinamento, che si è giuridicamente tradotta nell'intendimento del *bill of rights* come un predicato della forma di stato, codificante situazioni giuridiche azionabili nei confronti dell'autorità pubblica, non anche al cospetto di altri attori privati. Non sono tuttavia mancate, sul piano dottrinale, ricostruzioni inclini a riconoscere un'efficacia orizzontale indiretta ai diritti costituzionalmente tutelati[68]; così come, del resto, sembra temperare il rigore di questa impostazione il fatto che la giurisprudenza abbia riconosciuto la possibilità di estendere il novero degli *state actor* anche a soggetti privati, ancorché in via di eccezione e laddove investiti da funzioni tradizionalmente ed esclusivamente affidate ad attori pubblici[69].

Dunque, la qualificazione come *state actor,* ipotizzabile per via del collegamento con l'assolvimento di funzioni tipicamente riservate ai poteri pubblici, diventa il "grimaldello" per cercare di "forzare" le resistenze a una estensione della *free speech clause* nei rapporti tra privati, e segnatamente tra social network e utenti.

Questa è stata la via, almeno in prima battuta, sperimentata anche in *PragerU v. Google*[70]*,* anche se le difficoltà a fare breccia erano immaginabili alla luce delle conclusioni che la Corte Suprema aveva raggiunto pochi mesi prima, nel giugno 2019, nel caso *Manhattan*

in *Washington University Law Review*, 85(6), 2008, 1249 ss.; G. De Gregorio, *From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society*, in *European Journal of Legal Studies*, 11(2), 2019, 65 ss.

Merita inoltre una segnalazione la recente proposta della Commissione europea, del 21 aprile 2021, per l'adozione di un regolamento che definisce un approccio europeo sull'Intelligenza Artificiale.

[67] Case No. 18-15712.

[68] Si legga in proposito S. Gardbaum, *The Horizontal Effect of Constitutional Rights,* in *Michigan Law Review,* 102, 2003, 387 ss.

[69] Cfr. per esempio *Jackson v. Metropolitan Edison Co.*, 419 U.S. 345 (1974).

[70] Per una disamina accurata della rilevanza della *state action doctrine* nel caso in commento cfr. D. Zecca, *Soluzioni tradizionali per piattaforme moderne: la* state action *(non) mostra i segni del tempo,* in *questa Rivista,* 2, 2020, 340 ss.

Community Access Corp. v. Halleck[71], seppure in una vicenda non del tutto analoga[72]. In questa sentenza, la Corte Suprema ha stabilito che l'operatore di televisione via cavo cui sia stata affidata per legge la gestione del servizio con l'obbligo di trasmettere canali ad accesso pubblico non è soggetto al vincolo del Primo Emendamento. Secondo la Corte, «*merely hosting speech by others is not a traditional, exclusive public function and does not alone transform private entities into state actors subject to First Amendment constraints*»[73]. Per quanto si trattasse di un caso non direttamente inerente al ruolo delle piattaforme online, il principio di diritto e l'affermazione da ultimo ricordata sembrano segnare un atteggiamento di netta chiusura a una troppo disinvolta estensione della nozione di *state actor,* anche se la circostanza che la decisione sia stata assai combattuta (adottata con un solo voto favorevole in più dei contrari) potrebbe lasciare presupporre futuri margini di discussione sul tema.

Con questa pesante ipoteca della Corte Suprema, però, era difficile immaginare che la Corte d'appello del Ninth Circuit potesse sposare un risultato di segno opposto. E non a caso l'esito, forse scontato, della controversia ha visto rigettare il tentativo di far qualificare YouTube alla stregua di uno *state actor* onde ottenere una pronuncia che dichiarasse contraria al Primo Emendamento la scelta da questi operata di collocare alcuni contenuti pubblicati dalla Prager University sul proprio canale in un'area ad accesso riservato, in modo da impedirne la visualizzazione nell'ambito delle ricerche "pubbliche" effettuate dagli utenti.

La Corte d'appello si diffonde in una serrata critica alle argomentazioni svolte a questo scopo, ricordando come la storica sentenza *Marsh v. Alabama,* evocata da Prager University, non avesse affermato che «*any private property owner "who operates its property as a public forum for speech" automatically becomes a state actor who must comply with the First Amendment*»[74]. Nel caso *Marsh v. Alabama*[75], infatti, il soggetto privato titolare della *company town* risultava proprietario di tutte le strutture ed esercitava tutte le funzioni tipiche di un ente pubblico. In ogni caso, la stessa Corte Suprema, con alcune pronunce successive[76] si è adoperata per mantenere un'interpretazione restrittiva onde evitare che la nozione di *state actor* potesse essere applicata con eccessiva generosità anche rispetto all'ambito

[71] 587 U.S. ___ (2019). In tema cfr., volendo, la ricostruzione operata in M. Bassini, *Internet e libertà di espressione,* cit., 235 ss.; nonché il commento di D. Zecca, *I canali a pubblico accesso non sono un* public forum: *i perché di un'occasione persa,* in *questa Rivista,* 1, 2020, 270 ss. Nella dottrina statunitense, tra gli altri, si v. E. Goldman, *Private Publishers Aren't State Actors–Manhattan Community Access v. Halleck*, in *ericgoldman.org,* 26 giugno 2019; A. Howe, *Opinion analysis: Court holds that First Amendment does not apply to private operator of public-access channels*, in *SCOTUSblog,* 17 giugno 2019.

[72] La sentenza ha comunque avuto il merito di rinvigorire il dibattito in materia; prima che i commentatori tornassero a occuparsene più di recente (si v. K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech,* cit.; J. Peters, *The "Sovereigns of Cyberspace" and State Action: The First Amendment's Application (or Lack Thereof) to Third-Party Platforms*, in *Berkeley Tech. L.J.*, 32, 2017, 989 ss.) sul tema si era soffermato, in tempi non sospetti, anche P.S. Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to 'Private' Regulation,* in *U. Colo. L. Rev.,* 71, 2000, 1263 ss.

[73] 587 U.S. ___ (2019), spec. 10.

[74] Case 5:17-cv-06064-LHK, p. 18.

[75] 326 U.S. 501 (1946).

[76] Cfr. *Amalgamated Food Employees Union Local v. Logan Valley Plaza, Inc.*, 391 U.S. 308 (1968); *Hudgens v. N.L.R.B.*, 424 U.S. 507, 513 (1976); *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972); *Flagg Bros., Inc. v. Brook*s, 436 U.S. 149, 158 (1978).

privato.

Il passaggio forse più significativo si coglie però nella affermazione per cui nemmeno la sentenza della Corte Suprema nel caso *Packingham* giova alla causa dell'estensione della *state action doctrine*. Così, i timori di Alito sembrano finalmente dissipati: secondo la Corte d'appello, «*[a]lthough Packingham spoke of "cyberspace" and "social media in particular" as "the most important places … for the exchange of views" in modern society, […] Packingham did not, and had no occasion to, address whether private social media corporations like YouTube are state actors that must regulate the content of their websites according to the strictures of the First Amendment*»: metaforicamente, si tratta di un colpo di grazia rispetto a ogni velleità di equiparazione che potesse sorreggersi su quella pur importantissima sentenza, il cui significato non deve essere perciò travisato[77]. Gli *obiter dicta* tanto temuti da Justice Alito non sembrano così aver mietuto vittime.

Nell'interpretazione della Corte d'appello, mancano totalmente possibili punti di contatto tra un prestatore di servizi come YouTube e ciò che nel diritto costituzionale statunitense rappresenta uno *state actor*: non vi sarebbe alcuna partecipazione a quel novero limitato di funzioni che sono tradizionalmente riservate in via esclusiva allo Stato; al contrario, queste piattaforme non sono altro che soggetti privati che adottano decisioni in merito alla pubblicazione di contenuti di terzi sul proprio sito. A supporto di questa netta chiusura, la Corte d'appello menziona anche una serie di decisioni di varie corti distrettuali che hanno negato la qualificazione dei prestatori di servizi come *state actors*, a partire dal celebre caso *Cyber Promotions v. AOL*[78].

Se questo è il quadro di riferimento, la decisione di Twitter e di Facebook di sospendere l'account personale di Donald Trump dopo i fatti di Capitol Hill offre senz'altro nuovi spunti di riflessione. Quella in parola è una vicenda ancora diversa, in cui il "silenziamento" non segue la logica delle decisioni *Knight Institute v. Trump* e *Randall v. Davison*, dove era uno *state official* ad aver interferito arbitrariamente con la libertà di espressione degli individui; né tantomeno può ricondursi alle decisioni appena ricordate, incentrate sulla possibilità di ridurre il margine di moderazione dei contenuti di un "potere privato" alla luce della sua pretesa (ma smentita) natura quasi-pubblicistica. Nel caso più recente, invece, il problema concerne la possibilità per un soggetto privato di incidere su uno dei canali di esercizio della libertà di espressione di un attore pubblico. Come si è visto, la giurisprudenza statunitense sembra essere giunta ad approdi alquanto saldi, per quanto la Corte Suprema non abbia ancora avuto modo di pronunciarsi direttamente sul punto (con l'eccezione, già ridimensionata, del caso *Packingham*): se il Primo Emendamento è una tutela a garanzia dei cittadini nel rapporto con i pubblici poteri, nessuna pretesa potrà essere avanzata rispetto alle scelte compiute da operatori privati

[77] Peraltro già la sentenza della Corte distrettuale del Southern District del Texas nel caso *Nyabwa v. Facebook*, 2018 WL 585467 (S.D. Tex. Jan. 26, 2018) aveva colto esattamente questo punto, smentendo il valore normativo della metafora enunciata dalla Corte Suprema e sottolineando che: «*the Court did not declare a cause of action against a private entity such as Facebook for a violation of the free speech rights protected by the First Amendment*».

[78] 948 F. Supp. 436 (E.D. Pa. 1996). Ma si v. anche *Howard v. Am. Online, Inc.*, 208 F.3d 741 (3d Cir. 2000) e le più recenti *Nyabwa v. Facebook*, cit.; *Shulman v. Facebook.com*, 2017 WL 5129885 (D.N.J. Nov. 6, 2017); *Kinderstart.com LLC v. Google, Inc.*, 2007 WL 831806 (N.D. Cal. Mar. 16, 2007); *Langdon v. Google, Inc.,* 474 F. Supp. 2d 622 (D. Del. 2007).

che non si qualificano come *state actor* né danno vita a un *public forum*.

Questo fermento non sembra però esser sfuggito a Justice Thomas che, nel redigere una *concurring opinion* all'*order* con cui, a seguito dell'investitura di Biden come nuovo Presidente degli Stati Uniti d'America, la Corte Suprema si è spogliata della materia del contendere nel caso *Knight Institute v. Trump,* ha messo in luce come la vicenda dell'oscuramento degli account appartenuti a Donald Trump, se letta in controluce con la pronuncia da ultimo citata, riveli una trama più complessa; essa indica, infatti, l'esistenza di uno sbilanciamento di potere tra la posizione di Twitter e Facebook, in grado di paralizzare l'attività social dell'allora Presidente, e quella di quest'ultimo, impossibilitato a condizionare con eguale efficacia i propri *followers*. Nella ricostruzione di Thomas[79], proprio la concentrazione di un potere così rilevante come quello di *deplatforming* in capo a operatori privati motiverebbe la ricerca di categorie in forza delle quali riqualificare questi soggetti ed escluderne la possibilità di incidere unilateralmente sulla libertà di espressione. Tra le opzioni a suo dire praticabili, Justice Thomas individua il ricorso alla categoria dei *common carrier* e a quella, alternativa, dei *places of public accommodation*[80]. Entrambe le dottrine permetterebbero di stabilire per via legislativa quel *right to exclude* che tanto pare sbilanciare i rapporti di forza nell'ecosistema digitale[81]. Questa lettura sembra però svalutare l'importanza che la Section 230 CDA ha avuto nel corso del tempo come leva normativa per esonerare da conseguenze i prestatori di servizi rispetto all'attività di moderazione.

Allo stato attuale, però, soprassedendo sulla *concurring opinion* (non vincolante) di Justice Thomas, lo scenario giurisprudenziale descritto in premessa sembrerebbe lasciare uno spazio pressoché nullo per ogni pretesa che Trump dovesse avanzare nei confronti di Twitter o Facebook, tanto più ora che egli è tornato (ma è un passaggio davvero scontato?) a essere un privato cittadino "qualunque"[82].

Peraltro, anche a voler prescindere dal dibattito sulla qualificazione giuridica dei social network, autorevole dottrina[83] ha argomentato in modo senz'altro condivisibile che nel caso di specie le esternazioni di Trump travalicassero i limiti del Primo Emendamento,

---

[79] A commento della *concurring opinion* di Justice Thomas si v. M. Monti, *La Corte Suprema Statunitense e il potere delle piattaforme digitali: considerazioni sulla privatizzazione della censura a partire da una* concurring opinion, in *DPCE on line,* in corso di pubblicazione. Si v. anche R. Krishnan, *The Pitfalls of Platform Analogies in Reconsidering the Shape of the First Amendment,* in *knightcolumbia.org,* 19 maggio 2021.

[80] Infatti, nella visione di Justice Thomas, 593 U. S. ____ (2021), spec. 4: «*If part of the problem is private, concentrated control over online content and platforms available to the public, then part of the solution may be found in doctrines that limit the right of a private company to exclude*».

[81] In particolare, la categoria dei *common carriers* indica quegli operatori di servizi essenziali rispetto ai quali storicamente si è imposto per via legislativa un obbligo di servizio universale (*to serve all comers*), scelta che sottrae l'attività dei soggetti rilevanti a logiche di mercato e dunque all'equilibrio economico ma che contempla una remunerazione del sacrificio occasionato dalla necessità di operare in condizioni anche anti-economiche a carico del pubblico. La somiglianza tra le piattaforme digitali e questi operatori sarebbe, ad avviso di Justice Thomas, particolarmente visibile, soprattutto avendo riguardo a quei soggetti che agiscono in condizioni pressoché di monopolio o di oligopolio, data l'assenza di alternative comparabili a causa anche della forte concentrazione di potere di mercato.

[82] Qualche dubbio potrebbe nascere dalla recente costituzione di un ufficio ad hoc (si v. il sito www.45office.com), The Office of Donald J. Trump…

[83] Così M. Manetti, *Facebook, Trump e la fedeltà alla Costituzione,* cit.

costituendo *fighting words* incitanti all'odio e alla violenza[84]. Sicché, a rigore, neppure potrebbe porsi un problema di tutela della libertà di espressione. Ad analoga conclusione si potrebbe pervenire esaltando la dimensione privatistica delle piattaforme online e reclamando la loro libertà, assicurata dalla Section 230 CDA nell'ordinamento statunitense[85], di effettuare una moderazione (in buona fede) dei contenuti di terzi; o ancora evidenziando come resterebbero comunque disponibili, per l'esercizio di questa libertà, canali alternativi a quelli oggetto del *ban*.

Se tutto questo è vero, non può però sfuggire al giurista l'eccezionalità di questa situazione, in cui a un soggetto privato sia rimesso un potere così importante come quello di limitare (financo, volendo, a propria discrezione) la capacità di esternare manifestazioni di pensiero di attori pubblici: al di là di ogni giudizio di valore, è questo un enorme *elephant in the room* che non può non interrogare per primi i costituzionalisti, in Europa come negli Stati Uniti, a fronte delle importanti riforme che potranno prendere corpo nei mesi a venire in questo campo. Una questione, invero, che sembra porsi in ogni caso, anche a voler prescindere dalla possibile configurazione di quello che è stato efficacemente descritto come "un diritto di *post*"[86].

6. Dall'altra sponda dell'Atlantico: il dibattito in Europa e in Italia

Se la giurisprudenza statunitense è apparsa opporre una netta chiusura rispetto a una possibile estensione con effetti orizzontali del Primo Emendamento, complice soprattutto un'interpretazione restrittiva della *state action doctrine*, l'Europa non pare aver compiuto particolari avanzamenti nonostante sia stata la "culla" della teoria della *Drittwirkung*[87], che acconsente a riconoscere un'efficacia con effetti indiretti orizzontali alle norme costituzionali[88]; e a dispetto del fatto che le disposizioni convenzionali e costi-

[84] *Amplius* in tema cfr. M. Rosenfeld, *Hate Speech in Constitutional Jurisprudence: A Comparative Analysis*, in *Cardozo Law Review,* 24, 2003, 1523 ss. Per una disamina comparata in tema di *hate speech*, si v. L. Scaffardi, *Oltre i confini della libertà di espressione: l'istigazione all'odio razziale,* Padova, 2009.

[85] Non va peraltro dimenticato che la decisione di Twitter e Facebook è giunta dopo che mesi addietro Trump aveva adottato un discusso Executive Order che mirava a riformare la disciplina sulla responsabilità dei prestatori di servizi affidato alla *Good Samaritan clause* della Section 230 CDA. Al di là del merito delle proposte di riforma, già ampiamente dibattute da tempo in dottrina, deve essere evidenziato come tale proposta non fosse estranea a una forte contrapposizione di carattere anche personalistico tra l'allora presidente e i social network. Sulle varie sfaccettature di questa vicenda cfr., tra gli altri, i commenti di M. Monti-A. Venanzoni, *Il tramonto della frontiera digitale? Note a prima lettura dell'executive order del 28 maggio 2020 emanato per prevenire la censura online da parte dei social media,* in *Diritti Comparati,* 8 giugno 2020; G. De Gregorio-R. Radu, *Trump's Executive Order: Another Tile in the Mosaic of Governing Online Speech*, in *medialaws.eu,* 6 giugno 2020 nonché G. Casavola, *L'executive order di Trump e l'Internet che nessuno vorrebbe,* ivi, 22 giugno 2020. Cfr. anche G.F. Ferrari, *L'*executive order *sulla prevenzione della censura online: quali effetti sull'autonomia dei social network?,* in *DPCE on line,* 2, 2020, 1145 ss.; V. Azzollini, *Cosa ci dice il caso Trump sulla natura di Internet e dei social media,* in *Il Sole 24 Ore,* 23 giugno 2020.

[86] Così C. Melzi d'Eril-G.E. Vigevani, *Facebook vs. Casapound: un social network è davvero un servizio pubblico?,* in *Il Sole 24 Ore,* 15 dicembre 2019.

[87] Per una comparazione tra Europa (e in particolare Germania) e Stati Uniti, cfr. P. Quint, *Free Speech and Private Law in German Constitutional Theory*, in *Maryland Law Review*, 48, 1989, 247 ss.

[88] A partire dal celeberrimo caso *Lüth* deciso dal Tribunale costituzionale federale tedesco, BverfGE

tuzionali di riferimento lascino un margine più ampio, utilizzando una formulazione improntata al riconoscimento di diritti e non solo al divieto di interferenze[89]. Se è vero che anche la giurisprudenza della Corte europea dei diritti dell'uomo che si è esercitata sull'art. 10 CEDU ha riconosciuto, in alcuni casi, la sussistenza di *positive obligations* in capo agli Stati contraenti, con risultati pratici in parte analoghi, sostanzialmente, a quelli propri di un'efficacia orizzontale dei diritti fondamentali, è soprattutto la Corte di giustizia ad aver dimostrato una sensibilità più spiccata rispetto all'*enforcement* con effetti orizzontali di alcuni diritti, privacy su tutti. Il caso forse più noto e al contempo evidente di questo processo è quello del diritto alla deindicizzazione dai motori di ricerca, che risale alla celeberrima pronuncia *Google Spain*[90]. Questa vicenda rivela un tentativo[91] di estendere orizzontalmente l'applicazione delle norme a tutela dei dati personali. L'elemento di particolare innovatività ma al contempo anche di criticità di questa decisione riguarda però la scelta di affidare il compito di bilanciare i contrapposti interessi (la tutela della privacy e dei dati personali, da un lato; la libertà di informazione, dall'altro) a un operatore privato, tema che dischiude, come è stato notato, l'assunzione di un ruolo paracostituzionale da parte del motore di ricerca[92].

Svolta questa premessa, è importante evidenziare come il quadro normativo vigente nell'Unione europea, ormai prossimo a un processo di riforma, ponga inevitabilmente una maggiore pressione in capo ai prestatori di servizi rispetto all'attività di moderazione di contenuti. Se, infatti, la Section 230 CDA ha tradotto la scelta di una esenzione pressoché generale (che soffre di limitate eccezioni) che mette al riparo gli operatori da qualsiasi conseguenza connessa alla scelta di moderare in buona fede determinati contenuti rimuovendoli ovvero mantenendoli online (la c.d. *Good Samaritan clause*), analogo "scudo" non trova corrispondenza in Europa dove la disciplina in materia si conforma al ben più temperato paradigma *notice and take down* ispirato dalla normativa statunitense in materia di tutela del diritto d'autore. Nell'attribuire ai prestatori una responsabilità, ancorché soltanto in via mediata, per il caso di mancata rimozione di contenuti illeciti di cui si abbia avuta conoscenza effettiva, sembra sfumare quella neutralità di fondo che caratterizza il sistema statunitense[93] e che poteva fondare un atteggiamento di sostanziale indifferenza rispetto all'esercizio dell'attività di moderazione, purché svolta in buona fede: in Europa esistono, innegabilmente, maggiori incentivi alla rimozione di contenuti, che può diventare finanche doverosa per i prestatori di servizi. Questa diffe-

7, 198 (1958).

89 In tal senso sembra deporre anche M. Betzu, *Libertà di espressione e poteri privati nel cyberspazio,* cit., 131, richiamando peraltro C. Esposito, *La libertà di manifestazione del pensiero nell'ordinamento italiano,* Milano, 1958, nt. 61.

90 CGUE, C-131/12 (2014).

91 Era la direttiva 95/46/CE, allora vigente, ed è ora il regolamento (UE) 2016/679 (GDPR) a stabilire in capo all'interessato i cui dati personali siano oggetto di trattamento da parte del titolare il diritto alla cancellazione. Si può dire che la Corte di giustizia, nella sentenza appena ricordata, è stata in grado di applicare a soggetti diversi da quelli che trattano direttamente i dati sui loro siti sorgente in quanto editori, ossia ai motori di ricerca, regole istitutive di diritti in capo agli interessati già per vero vigenti ma mai ritenute suscettibili di *enforcement* in quella direzione.

92 Così O. Pollicino, *Google rischia di «vestire» un ruolo para-costituzionale,* in *Il Sole 24 Ore,* 14 maggio 2014.

93 A tacere, peraltro, delle forzature giurisprudenziali che hanno portato alla luce la figura "ibrida", non oggetto di codificazione normativa, del c.d. *provider* attivo.

renza nei meccanismi che governano la responsabilità delle piattaforme pare costituire un riflesso del diverso sentire proprio dei rispettivi ordinamenti con riguardo alla tutela della libertà di espressione[94]. Ciò non toglie che anche in Europa i prestatori di servizi non sono formalmente vincolati dalle previsioni costituzionali rilevanti, potendo così ipoteticamente introdurre policy di moderazione dei contenuti più stringenti rispetto alle regole previste dall'ordinamento che identificano i contenuti illeciti. Viene così preservata, sembra, la possibilità che si determini un "differenziale" legato alla eventuale divergenza tra policy di moderazione (più restrittive) e regole ordinamentali[95].

Nonostante la differenza tra i meccanismi insiti nella disciplina di riferimento, il problema che sembra porsi in Europa e negli Stati Uniti è analogo: possono i social network "censurare" ciò che non sarebbe (necessariamente) vietato dalla legge dello Stato?

Per rispondere a questa domanda è necessario, ancora una volta, verificare la sensibilità dimostrata dalla giurisprudenza in relazione allo statuto giuridico dei social network, da cui discendono rilevanti implicazioni sull'estensione dei "poteri censori" di cui sono muniti.

A livello comparato, prima di entrare nel merito della casistica nazionale, merita segnalare una importante presa di posizione del Bundesverfassungsgericht che, nel maggio 2019, ha ordinato a Facebook di ripristinare l'accesso alla pagina di un partito politico di estrema destra che era stata oggetto di oscuramento pochi mesi prima che si tenessero le elezioni del Parlamento europeo[96]. I giudici di prime cure investiti delle istanze cautelari, pur riconoscendo la possibilità per i diritti costituzionali di spiegare entro certe condizioni effetti indiretti orizzontali, avevano respinto il ricorso e affermato che la libertà di espressione non conoscesse comunque una protezione assoluta[97]. Il Tribunale

---

[94] In questi termini, volendo, M. Bassini, *Internet e libertà di espressione,* cit., 107 ss.

[95] Si pensi, per esempio, all'ipotesi in cui all'interno delle condizioni di servizio, e dunque sul piano contrattuale, si faccia ricorso a una terminologia eccessivamente aperta e generica per delimitare fattispecie (che pur potrebbero avere un corrispondente normativo) che legittimano la rimozione di contenuti o ancora la disattivazione del servizio, come per esempio quella, già di per sé problematica, di *hate speech*.

[96] 1 BvQ 42/19, ord. 22 maggio 2019. Per un commento, cfr. E. Tuchtfeld, *Marktplätze, soziale Netzwerke und die BVerfG-Entscheidung zum „III. Weg"*, in *verfassungsblog.de*, 26 maggio 2019.

[97] La vicenda aveva tratto origine dalla decisione di Facebook di rimuovere un articolo che era stato pubblicato il 21 gennaio 2019 sulla pagina appartenente al movimento politico Der Dritte Weg. L'articolo era infatti stato ritenuto dal social network una forma di *hate speech* contraria alle condizioni di servizio e agli standard della comunità. Contestualmente, veniva limitata la possibilità per la pagina in questione di pubblicare contenuti per un periodo di trenta giorni. In seguito, l'account veniva invece sospeso. Il partito ricorreva in sede cautelare contro la misura adottata da Facebook, eccependo la violazione dell'art. 5 della Legge fondamentale tedesca, che garantisce la libertà di espressione, anche in combinazione con altre previsioni a tutela del pluralismo politico. Si invocava, dunque, una efficacia indiretta con effetti orizzontali di tali norme costituzionali nel rapporto interprivato tra Facebook e il partito politico. Tale efficacia non è stata messa in discussione nemmeno dai giudici che hanno rigettato la domanda cautelare, i quali hanno però ritenuto che il social network avesse correttamente fatto applicazione degli obblighi scaturenti dal NetzDG (*Netzwerkdurchsetzungsgesetz*), ossia la legge tedesca per migliorare la tutela dei diritti sui social network entrata in vigore il 1 ottobre 2017 (di cui è disponibile la traduzione italiana a cura di G. Giannone Codiglione in *questa Rivista,* 1, 2017, 185 ss.), in quanto il contenuto apparso sul sito era stato giudicato integrare la fattispecie di istigazione all'odio punita dalla § 130 del StGB (il codice penale tedesco, *Strafgesetzbuch*). A proposito del NetzDG, si v. tra gli altri i commenti di S. Theil, *The German NetzDG: A Risk Worth Taking?*, in *verfassungsblog.de*, 8 febbraio 2018 e M. Hong, *The German Network Enforcement Act and the Presumption in Favour of Freedom of Speech,* ivi,

costituzionale federale, successivamente investito della questione, accoglieva invece le doglianze dei ricorrenti, evidenziando come l'opzione di ripristinare temporaneamente una pagina che un successivo giudizio di merito a cognizione piena avrebbe potuto ribaltare fosse senz'altro meno rischiosa di quella di confermare sommariamente uno *stay down* che avrebbe potuto poi essere giudicato illegittimo[98]. Il Bundesverfassungsgericht giungeva a questa conclusione non senza aver osservato come Facebook, in funzione delle sue caratteristiche di mercato, costituisse uno spazio di particolare importanza per il mutuo scambio di espressioni; così da evincere che negarne l'accesso a un partito politico, soprattutto nel contesto di una campagna elettorale, avrebbe significato privare quest'ultimo di una *essential facility* per la divulgazione delle proprie idee.
In tempi recenti, anche la giurisprudenza italiana si è espressa sul tema, soprattutto in un trittico di pronunce del Tribunale di Roma[99] che sembrano timidamente affrontare il nodo legato alla pretesa qualificazione meramente privatistica del rapporto tra utenti e social network ma che hanno partorito esiti tra loro differenti[100]. Al centro di queste controversie si colloca la decisione di Facebook di disattivare le pagine appartenenti alle associazioni di stampo politico di estrema destra Forza Nuova e CasaPound (e quelle personali dei relativi amministratori). Il nucleo critico comune a questi provvedimenti riguarda la rilevanza delle condizioni d'uso e dunque del regolamento contrattuale in essere tra gli utenti e Facebook e il rapporto tra i predetti termini di servizio e le norme dell'ordinamento interno e sovranazionale. Ai fini che qui rilevano, è importante mettere in luce come le pronunce in parola falliscano nell'obiettivo di consegnare una ricostruzione coerente non solo dello statuto giuridico dei social network ma anche del

22 gennaio 2018. Cfr. anche V. Claussen, *Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation*, in *questa Rivista,* 3, 2018, 110 ss.

98 Il ragionamento del Tribunale costituzionale federale pare così maggiormente incentrato sul *periculum* che un atto di censura privata come quello messo in atto da Facebook avrebbe potuto determinare rispetto all'esercizio della libertà di espressione ma anche (e forse soprattutto) in relazione al regolare svolgersi dell'allora imminente competizione elettorale in condizioni di garanzia del pluralismo politico. Vale peraltro la pena precisare che l'ordine del Bundesverfassungsgericht ha riguardato esclusivamente il ripristino della pagina Facebook, mentre il Tribunale non ha messo in discussione la correttezza della rimozione dell'articolo.

99 Trib. Roma, sez. impresa, ord. 12 dicembre 2019, confermata poi, in sede di reclamo cautelare, dall'ordinanza collegiale Trib. Roma, sez. impresa, 29 aprile 2020 (caso *CasaPound c. Facebook*); Trib. Roma, sez. diritti della persona e immigrazione, ord. 23 febbraio 2020 (caso *Forza Nuova c. Facebook*). Per un'accurata disamina delle sentenze e dei loro vari profili si v. O. Grandinetti, *Facebook vs. CasaPound e Forza Nuova, ovvero la disattivazione di pagine social e le insidie della disciplina multilivello dei diritti fondamentali,* in *questa Rivista,* 1, 2021, 173 ss. Cfr. anche
Cfr. anche P. Falletta, *Controlli e responsabilità dei social network sui discorsi d'odio online,* in *questa Rivista*, 1, 2020, 146 ss.; C. Caruso, C. Caruso, *La libertà di espressione presa sul serio. CasaPound c. Facebook, Atto I,* in *sidiblog.it,* 20 gennaio 2020 e la "replica" di P. De Sena-M. Castellaneta, *La libertà di espressione e le norme internazionali ed europee prese sul serio: sempre su CasaPound c. Facebook,* ivi, 20 gennaio 2020. Cfr. ancora P. Zicchittu, *La libertà di espressione dei partiti politici nello spazio pubblico digitale: alcuni spunti di attualità,* in *questa Rivista,* 2, 2020, 81 ss.; R. Bin, *Casa Pound vs. Facebook: un'ordinanza che farà discutere,* in *lacostituzione.info,* 15 dicembre 2019; A. Venanzoni, *Pluralismo politico e valore di spazio pubblico della piattaforma social Facebook: la vicenda CasaPound,* in *Diritto di Internet,* 12 dicembre 2019; P. Villaschi, *Facebook come la RAI? Note a margine dell'ordinanza del Tribunale di Roma del 12.12.2019 sul caso CasaPound c. Facebook*, in *Osservatorio costituzionale,* 2, 2020, 430 ss.

100 Evidenziano l'assenza completa di sintonia tra le decisioni in commento C. Melzi d'Eril-G.E. Vigevani, *Odio in rete e rimozione delle pagine Facebook: giudice che vai, soluzione che trovi,* in *Il Sole 24 Ore,* 27 febbraio 2020.

valore precettivo delle loro condizioni d'uso. Si deve peraltro ricordare che, come gran parte della giurisprudenza in questa materia, le decisioni in commento sono state rese in sede cautelare, circostanza che non pare aver agevolato una elaborazione del tutto compiuta e matura sul ruolo dei prestatori di servizi.

Come è noto, le tre ordinanze del Tribunale di Roma[101] sono giunte a conclusioni opposte: ritenendo, in un caso - quello che interessava CasaPound - che l'oscuramento della pagina fosse illegittimo e, nell'altro, che riguardava Forza Nuova, che l'intervento di Facebook fosse non solo legittimo ma finanche doveroso. L'eterogeneità degli esiti partoriti da queste decisioni pare indicativa di una generale incertezza in merito allo statuto giuridico delle piattaforme e alla ricostruzione del loro ruolo nella sfera pubblica digitale. Al di là delle differenze sull'interpretazione delle fonti richiamate e di quelle derivanti dalle irripetibili peculiarità di ciascun caso, la divergenza di vedute sembra riconducibile, almeno in parte, al diverso grado di compenetrazione delle norme costituzionali e dei vincoli che esse pongono rispetto al regolamento contrattuale in essere tra soggetti privati. Il divario è così visibile che sembra possibile disporre questi provvedimenti secondo un *climax*. Dapprima, infatti, nell'ordinanza del dicembre 2019, il Tribunale di Roma ha espressamente sostenuto che il servizio di Facebook, vantando oltre 2,8 miliardi di utenti ed essendo accessibile tramite diversi canali, riveste un «ruolo centrale e di primaria importanza» che attribuisce al suo gestore una «speciale posizione». Da questa speciale posizione la sezione impresa ha tratto la conclusione per cui il rapporto tra Facebook e gli utenti «non è assimilabile al rapporto tra due soggetti privati qualsiasi» perché comporta che il social network «nella contrattazione con gli utenti, debba strettamente attenersi al rispetto dei principi costituzionali e ordinamentali finché non si dimostri (con accertamento da compiere attraverso una fase a cognizione piena) la loro violazione da parte dell'utente». Il rispetto dei principi costituzionali e ordinamentali, infatti, costituisce secondo il Tribunale «a[d] un tempo condizione e limite nel rapporto con gli utenti». Il giudice qualifica così, in via di fatto, Facebook come un servizio pubblico, pur senza ammetterlo espressamente, con tutto quanto ne deriva sul piano dei principi applicabili[102]. La motivazione di questa scelta si nutre peraltro anche di risultanze empiriche, legate alla peculiarità dell'associazione politica ricorrente: ad avviso del Tribunale, l'esclusione dalla comunità di Facebook si risolve in una estromissione dal dibattito politico[103], che frustrerebbe l'attuazione del

[101] Giova osservare che le ordinanze in parola sono state emanate da sezioni diverse, rispettivamente dalla sezione impresa e dalla sezione tutela dei diritti e immigrazione. Non è dato, naturalmente, comprendere se la differente "specialità" dei giudici assegnatari delle regiudicande abbia potuto in qualche modo giocare un ruolo ma si tratta di un dato che merita forse di essere registrato. Per una lettura critica dell'atteggiamento giurisprudenziale nel campo della responsabilità de prestatori di servizi mi permetto un rinvio, volendo, a M. Bassini, *Mambo Italiano: the perilous Italian way to ISP liability,* in B. Petkova-T. Ojanen (eds.), *Fundamental Rights Protection Online. The Future Regulation of Intermediaries,* Cheltenham-Northampton, 2020,84 ss.

[102] Mette bene in evidenza il punto, e soprattutto l'incongruenza di tale conclusione, con le conseguenze in termini di snaturamento del ruolo di questi soggetti che ne deriverebbero, P. Villaschi, *Facebook come la RAI?,* cit., spec. 441.

[103] Peraltro, proprio la qualificazione "in via di fatto" con richiami a circostanze empiriche operata dal giudice pone il dubbio sull'effettiva sovrapponibilità tra la categoria dei social network in quanto tale e l'ambito dei prestatori di servizi che rivestono una speciale posizione. Tutti i social network sono gravati da questa speciale responsabilità, o soltanto alcuni, per esempio quelli che contano un numero

principio del pluralismo partitico che si ricava dall'art. 49 Cost. Si sarebbe così realizzata un'estensione orizzontale, lungo il rapporto privato tra utente e social network, delle norme costituzionali che si fanno limite all'autonomia privata.

Le importanti affermazioni contenute nell'ordinanza monocratica non sembrano però essere state messe a profitto, tanto che in sede di reclamo, pur confermando l'illegittimità dell'oscuramento, il collegio ha rivisitato l'inquadramento giuridico prospettato dall'ordinanza sottoposta a gravame, disinnescandone così il potenziale. Il Tribunale, con l'ordinanza di aprile 2020, ha sgombrato il terreno da ogni equivoco, sottolineando come il rapporto tra utenti e social network soggiaccia alle ordinarie regole civilistiche; il che non esclude l'applicazione, secondo i principi costituzionali, di limiti come l'ordine pubblico e il buon costume, che si impongono a qualsiasi manifestazione di autonomia privata[104]. Questo passaggio ha consentito al Tribunale di svolgerne un altro in via successiva e consequenziale: la relazione tra social network e utente è equiparabile a un qualsiasi rapporto tra un soggetto che esercita la libertà di iniziativa economica tutelata dall'art. 41 Cost. e una controparte-utente che può rivendicare la tutela delle sue manifestazioni di pensiero *ex* art. 21 (o della sua adesione a un'associazione politica *ex* art. 18). Così, conclude il Tribunale, «la disciplina contrattuale non può lecitamente assumere come causa di risoluzione del rapporto manifestazioni del pensiero protette dall'art. 21 né consentire l'esclusione di associazioni tutelate dall'art. 18»[105].

Ne consegue che un soggetto privato non potrà, per via semplicemente contrattuale, trovarsi a esercitare «poteri sostanzialmente incidenti sulla libertà di manifestazione del pensiero e di associazione»[106]. Il che significa che un social network non può pretendere la sottrazione delle regole della comunità definite dai termini di servizio da qualsiasi controllo; può, come nel caso di Facebook, prevedere cause di esclusione dalla comunità, ma occorre che queste regole siano interpretate conformemente alle leggi dello Stato, cui spetta definire limiti cogenti ed esterni. Così argomentando, e passando in rassegna tutti i riferimenti normativi vigenti, il collegio ha potuto concludere che l'ordinamento italiano non permettesse di qualificare CasaPound come un'associazione illecita, così confermando l'illegittimità dell'oscuramento[107]. L'ordinanza collegiale

particolarmente elevato di utenti? Queste considerazioni non paiono così lontane sia dagli intendimenti perseguiti da alcuni legislatori nazionali (come quello tedesco, che con la già ricordata legge nota come NetzDG, ha previsto particolari obblighi di *enforcement* per i social network con più di due milioni di utenti in Germania, rafforzando significativamente la tutela dei diritti in rete ma anche minacciando importanti sanzioni a carico dei prestatori di servizi inadempienti), sia da quelli che paiono caratterizzare il legislatore dell'Unione europea che, con la proposta di regolamento nota come Digital Services Act, già richiamata, sembra collocarsi nella direzione di una modularità di regole che istituisca obblighi più stringenti in capo alle piattaforme online "di dimensioni molto grandi" (cfr. l'art. 25 della proposta), ossia quelle che «prestano i loro servizi a un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni», da calcolarsi secondo una metodologia specifica. In questa direzione sembra orientarsi anche O. Grandinetti, *Facebook vs. CasaPound e Forza Nuova,* cit., spec. 190.

104 In tema si può leggere M. Esposito, *Profili costituzionali dell'autonomia privata,* Padova, 2003.

105 Così al p. 10.

106 Così al p. 25.

107 Non mi diffondo in questa sede sul diverso grado di apertura che le norme interne e le norme sovranazionali offrirebbero rispetto all'inquadramento delle manifestazioni di pensiero qui in discorso, rinviando alle osservazioni svolte da Corrado Caruso e Marina Castellaneta con Pasquale de Sena nei contributi già cit. su *sidiblog.it.*

soddisfa così due obiettivi altrettanto importanti: da un lato, mantiene ferma la qualificazione prettamente contrattuale del rapporto tra social network e utenti; dall'altro, riconosce un limite all'autonomia privata derivante dal rispetto dei principi costituzionali, liberando al contempo i prestatori di servizi da un compito non riducibile a una mera funzione *in-house*.

Il Tribunale di Roma aveva nel frattempo avuto occasione di pronunciarsi, tra la prima e la seconda ordinanza, anche in un'altra controversia, quella che opponeva Facebook a Forza Nuova per effetto della decisione (adottata contestualmente a quella relativa a CasaPound) di oscurarne la pagina pubblica. Il giudice si è spinto ancora oltre, affermando che Facebook non avesse soltanto titolo ad adottare la misura in parola, ma vi fosse addirittura tenuto in forza della natura illecita di questi contenuti e dell'obbligo di provvedere alla relativa rimozione che la disciplina vigente (d.lgs. 70/2003, di attuazione della direttiva 2000/31/CE sul commercio elettronico) prescrive quando il prestatore di servizi abbia conoscenza effettiva di un illecito. In altri termini, ad avviso del Tribunale, Facebook si sarebbe dovuto considerare responsabile per la mancata rimozione della pagina qualora non si fosse adoperato, stante la natura illecita dei contenuti ivi pubblicati. L'ordinanza è tutta incentrata sulla valutazione della liceità della pagina riconducibile a Forza Nuova, mentre il ragionamento del giudice non si sofferma particolarmente sullo status di Facebook: lo si definisce un soggetto privato che svolge un'attività di indubbio rilievo sociale[108], il cui rapporto con gli utenti è regolato non soltanto dalle condizioni contrattuali ma anche dalla legge. La ricostruzione fattuale operata dal Tribunale, qualificando le attività compiute sulla pagina come illecite in base al quadro normativo richiamato[109], consente al Tribunale di dissociarsi dalla vicenda CasaPound e di ritenere corretto l'operato di Facebook, sia rispetto alle condizioni contrattuali sia rispetto all'ordinamento giuridico[110].

[108] Così a p. 14, dove si parla di una "speciale posizione" di Facebook senza tuttavia – così almeno pare – che ciò sottenda alcun rilievo normativo.

[109] Un esito analogo si è avuto con l'ord. 22 gennaio 2021 del Trib. Roma, sez. diritti della persona e immigrazione, in cui il collegio ha respinto le doglianze di due attivisti politici affiliati a CasaPound contro la rimozione dei rispettivi account Facebook occasionata dalla pubblicazione di contenuti incitanti all'odio. A giudizio del collegio, infatti, i post oggetto di condivisione da parte degli attivisti costituivano indubbiamente atti di incitamento all'odio, la cui natura illecita avrebbe potuto senz'altro essere riconosciuta a prescindere da un accertamento sulla legalità dell'associazione politica CasaPound. Proprio questa circostanza ha permesso al Tribunale di concludere che correttamente Facebook avesse provveduto alla rimozione in forza non soltanto delle disposizioni contrattuali ma anche di quelle di legge (che prevedono la responsabilità in caso di mancata rimozione di un contenuto manifestamente illecito di cui si abbia avuta conoscenza effettiva).

[110] Nello stesso senso si era espresso, nel gennaio 2020, anche il Tribunale di Siena (Trib. Siena, ord. 19 gennaio 2020), a seguito dell'oscuramento del profilo Facebook di un soggetto riconducibile a CasaPound e della pagina da lui per via della pubblicazione di esternazioni di carattere discriminatorio. Il giudice ha riconosciuto il diritto di origine contrattuale di Facebook di procedere alla disattivazione della pagina e del profilo del ricorrente, a causa della pubblicazione di contenuti risultati in violazione delle condizioni di policy. Secondo il Tribunale, la predetta disattivazione non integra quindi una violazione contrattuale, né tantomeno Facebook può «seriamente essere paragonata a[d] un soggetto pubblico nel fornire un servizio, pur di indubbia rilevanza sociale e socialmente diffuso, comunque prettamente privatistico» (p. 4). L'ordinanza soggiunge, inoltre, che «la scelta di privare l'utente della piattaforma social rientra nel diritto di recesso, peraltro compiutamente regolamentato. Né ciò può realmente rappresentare una lesione ai diritti fondamentali e[d] inviolabili della persona garantiti a livello costituzionale, ovvero di autodeterminarsi (art. 2 Cost), di poter svolgere la propria attività politica in un

Questa breve rassegna di decisioni giurisprudenziali conferma la tendenziale riluttanza delle corti italiane a sviluppare una riflessione di sistema sullo statuto costituzionale di Internet e dei social network e la preferenza per un approccio pragmatico legato anche all'apprezzamento casistico delle singole vicende. Non che questo tipo di riflessione possa dirsi agevole da percorrere, alla luce di un quadro normativo in materia ancora fermo – in Italia – al 2003 (che ha inevitabilmente causato fibrillazioni giurisprudenziali[111]). Forse, però, proprio la manifesta obsolescenza della disciplina presta il fianco a riflessioni di sistema che possono intercettare la distanza che si è venuta a creare tra lo *status quo* tecnologico esistente al momento del *drafting* legislativo e quello attuale, causa delle molte fibrillazioni che la giurisprudenza soprattutto statunitense ha captato e almeno in parte raccolto.

7. Conclusioni

I paragrafi che precedono costituiscono un tentativo di misurare la sensibilità sviluppatasi ai due lati dell'Atlantico rispetto a una nuova, possibile concettualizzazione del ruolo dei social network in rapporto all'esercizio della libertà di espressione degli individui. Si è cercato di cogliere, allo stesso tempo, il grado di fibrillazione causato da quello che si ritiene lo *status quo*, profondamente diverso da quello dei decenni scorsi, e "gli anticorpi" che ciascun ordinamento esprime in forma di resistenze rispetto ai possibili tentativi di ibridazione di una figura, quella dei social network, riconducibile al paradigma di soggetto privato.

Si è tentato, in particolare, di normativizzare o richiamare comunque all'esigenza di una concettualizzazione normativa di quella metafora ormai spesso utilizzata nel linguaggio comune ma anche di molti giuristi: quella che vede nei prestatori di servizi della società dell'informazione dei poteri privati. Occorre in altri termini tradurre nel dominio giuridico una metafora sicuramente accurata rispetto alla descrizione della rilevanza economica e anche sociale di questi attori, che ne coglie il coinvolgimento in un numero crescente di funzioni e di interazioni con gli individui secondo l'atteggiamento che è proprio dei pubblici poteri. Proprio questo mutato scenario, che ha fatto di Internet e dei social network strumenti in larga parte indefettibili per l'esercizio di una varietà di diritti e libertà, sollecita una risposta a queste tensioni.

Quale esito può partorire questo tentativo?

Un'ipotesi spesso dibattuta è quella di riconoscere nella missione propria delle piatta-

contesto di uguaglianza e pari opportunità con gli altri esponenti di tutte le altre fazioni (art. 3 Cost.), di ambire (anche in forma professionale e remunerata) a cariche politico-istituzionali (art. 4, 49, e 51 Cost.), di manifestare liberamente il proprio pensiero (art. 21 Cost.). Invero, trattasi di diritti, questi, certamente liberamente esercitabili in contesti diversi, pubblici e, comunque, idonei alla più ampia espressione della propria personalità nell'ambito di una leale competizione politica con la possibilità di condividere con gli appartenenti a quella certa corrente la propria ideologia» (p. 5). A commento di questa pronuncia si v. anche P. Villaschi, *Facebook come la RAI?,* cit., 443 ss. Nello stesso senso, v. anche Trib. Trieste, ord. 27 novembre 2020, con nota di S. Thobani, *L'esclusione da Facebook tra lesione della libertà di espressione e diniego di accesso al mercato,* in *Persona e mercato,* 2, 2021, 426 ss.

[111] Di cui è vivida testimonianza la già ricordata pronuncia Cass. civ., sez. I civ., n. 7708/2019.

forme i connotati di un servizio pubblico[112]. Questa opzione potrebbe forse giustificare una regolamentazione più stringente, e forse una riduzione di quel "differenziale" tra le condizioni di servizio e le norme dell'ordinamento giuridico, ma desta comunque criticità importanti.

In primo luogo, va osservato che se, da un punto di vista empirico i social network sono divenuti dei canali probabilmente essenziali per l'esercizio del diritto di parola, tale caratterizzazione non implica che si tratti di strumenti di accesso indispensabili e indefettibili senza i quali l'individuo sarebbe del tutto privato della possibilità di godere dei propri diritti costituzionalmente tutelati (sempre ammettendo che sia predicabile un "diritto all'utilizzo dei social network"). Si tratta forse di una giustificazione debole, che serve però a temperare un'esaltazione del mezzo come paradigma (quasi assoluto) della libertà, talvolta foriera di una loro impropria assimilazione[113].

Deve poi essere messo in evidenza come l'attrazione in questa categoria segnerebbe verosimilmente un allontanamento dalla caratterizzazione come intermediari propria dei prestatori di servizi e degli stessi servizi della società dell'informazione, da sempre estranei all'esercizio di una attività editoriale in senso stretto. Una emancipazione di cui nemmeno la proposta di regolamento nota come Digital Services Act sembra farsi portatrice, invero. Si tratta, infatti, di soggetti che, come ha ribadito la giurisprudenza, nel mettere a disposizione di terzi uno spazio virtuale per la condivisione di contenuti esercitano la loro libertà di impresa; non sono invece attori che intervengono in quanto titolari del diritto alla libertà di espressione, alla stregua di fornitori di contenuti.

In aggiunta, non si può trascurare che proprio questo assetto normativo ha permesso ai prestatori di servizi di ergersi a "volano" della libertà di espressione in rete, godendo di un regime giuridico di favore, soprattutto negli Stati Uniti, che ha permesso a ciascun individuo di poter contare su queste nuove agorà virtuali. Non vi sono evidenze che, se le norme giuridiche fossero state di diverso segno (nel senso di una maggiore e più stringente regolamentazione), si avrebbe avuto uno sviluppo della libertà di espressione più favorevole agli individui.

Da ultimo, occorre altresì fare i conti con le conseguenze che potrebbero discendere da una connotazione in senso pubblicistico dei servizi dei social network. Come si è evidenziato, il potere di moderazione delle piattaforme online si fonda sulla definizione di condizioni di servizio che potrebbero prevedere margini di intervento sui contenuti anche più ampi di quelli di quelli previsti da norme dell'ordinamento giuridico. Ma una qualificazione in senso pubblicistico non rischierebbe forse di eliminare questi margini, affrancando il potere di moderazione dei social network esclusivamente ai vincoli previsti dal diritto vigente? Si tratta di un tema non banale se si riflette all'attualità che presentano tuttora tematiche come il contrasto alla disinformazione, che interessano contenuti non necessariamente illeciti e rispetto ai quali i prestatori di servizi sono impegnati spesso in via di autoregolamentazione. Che ne sarebbe, in questo caso, se i

[112] Per una diffusa trattazione della missione del servizio pubblico in era digitale, si v. G.E. Vigevani, *I media di servizio pubblico nell'età della rete*, Torino, 2018.

[113] Naturalmente sul rapporto tra libertà e mezzi trasmissivi valgono le lungimiranti considerazioni esposte dalla più chiara dottrina in tempi non sospetti: A. Pace-M. Manetti, *Rapporti civili. La libertà di manifestazione del proprio pensiero. Art. 21 Costituzione*, in G. Branca (a cura di), continuato da A. Pizzorusso, *Commentario della Costituzione,* Bologna-Roma, 2006.

social network diventassero dei *public forum*?

Le motivazioni che precedono consentono di ritenere condivisibili gli approdi giurisprudenziali che mantengono ferma la connotazione privatistica del rapporto tra utenti e social network. Gli stessi argomenti, peraltro, paiono ben attagliarsi anche allo scenario comparato, e in particolare statunitense. Dove, tuttavia, le vicende più recenti, e quella che ha da ultimo riguardato Donald Trump in particolare, sembrano suggerire la presenza di un problema che parrebbe non destinato a risolversi neppure facendo dei social media più importanti un *public forum* permanente: il rapporto conflittuale con il potere pubblico e la possibilità di mettere in atto una censura privata che inevitabilmente può risentire dei *bias* e dei preorientamenti ideologici della piattaforma di turno[114]. Ma questo è un problema rispetto al quale il vero rimedio potrebbe non essere legato alla riqualificazione giuridica dei prestatori ma nella fissazione di regole che garantiscano maggiore trasparenza e *accountability*[115]. Regole, forse, che l'Unione europea potrebbe per prima avanzare nel lungo andare che segnerà il percorso del Digital Services Act[116]. Da questo punto di vista, forse, proprio la recente decisione del Facebook Oversight Board sulla sospensione permanente dell'account di Donald Trump, con i suoi richiami all'esigenza di regole procedurali chiare e al principio di proporzionalità, sembrano suggerire la via per una "autolimitazione" del potere privato delle piattaforme digitali che non passi necessariamente tramite inopportune assimilazioni.

[114] A tacere, in questa sede, delle problematiche che possono riguardare la protezione dei dati personali, su cui v. G. Cerrina Feroni, *Libertà di espressione, Garante privacy: "Troppo potere alle big tech, ecco come intervenire"*, in *agendadigitale.eu,* 11 maggio 2021.

[115] Rispetto alla specifica problematica del rapporto tra piattaforme online e figure politiche (e dunque tra "potere privato" e potere pubblico), nello stesso senso appare la prima proposta formulata da A. Palmieri, *Social è responsabilità!,* cit., 64, che richiama l'adozione dei Principi di Santa Clara definiti nel 2018, auspicandone piena considerazione anche all'interno del Digital Services Act.

[116] Spunti condivisibili nella stessa direzione sembrano emergere in V. Azzollini, *Chi ha paura della libertà di internet?,* in *IBL Focus,* 313, 13 dicembre 2019.

Il ruolo delle reti sociali nel contrasto ai reati commessi all'interno del web. Tendenze evolutive e prospettive di sviluppo*

Sofia Braschi

Abstract

Il saggio analizza il ruolo delle reti sociali nel contrasto ai reati commessi all'interno del web. Dopo una breve introduzione relativa al rapporto fra autorità pubblica e *provider*, l'Autrice si sofferma sul fondamento politico-criminale dell'attuale domanda di responsabilizzazione dei fornitori di servizi di *social networking*. L'attenzione si sposta quindi sulle posizioni recentemente assunte dalla dottrina e dalla giurisprudenza italiane, per concentrarsi infine sulle *notice and action procedure* come possibile strumento per assicurare una maggiore effettività della tutela penale.

The paper addresses the role of social networks in tackling cybercrime. After a short introduction on the relationship between the law enforcement authorities and the Internet Service Providers, the Author focuses on the criminal-political basis of the current request for accountability of Social Networks. The attention then moves to the positions recently held by Italian doctrine and case law; finally, it focuses on notice and action procedures as a possible means to ensure a more effective criminal protection.

Sommario

1. Premessa. – 2. Il concetto di "rete sociale" e la relativa disciplina. – 3. Il fondamento politico-criminale dell'attuale tendenza alla responsabilizzazione dei Social Network. – 4. Le soluzioni proposte dalla giurisprudenza e dalla dottrina. – 5. Le prospettive di sviluppo della materia: le "*notice and action procedure*". – 6. Considerazioni finali.

Keywords

responsabilità penale dell'Internet Service Provider - reati informatici - Social Network - *notice and action procedure* - *Digital Services Act*.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

1. Premessa

Nel settore della criminalità informatica[1], la collaborazione fra pubblico e privato costituisce una necessità, che tuttavia solleva molteplici problemi.

Se, infatti, i servizi di connettività sono forniti da operatori privati (gli *Internet Service Provider*, di seguito *ISP*), i quali dispongono di dati essenziali per l'individuazione dei responsabili degli illeciti commessi nella rete, va peraltro considerato che i principali *ISP* sono grandi società che operano su un mercato globale: per tale ragione, per poter acquisire informazioni la pubblica autorità deve generalmente sottostare ai vincoli della cooperazione giudiziaria internazionale, con apprezzabili ricadute in termini di effettività della tutela penale[2]. D'altra parte, però, l'imposizione di doveri di collaborazione che implichino un più diretto coinvolgimento degli *ISP* e una loro conseguente co-responsabilizzazione è in grado di impattare non solamente sulla libertà di iniziativa economica di questi operatori, bensì anche sulla libertà di comunicazione e informazione degli internauti; ne discende che l'intervento repressivo incontra limiti ulteriori, fondati sulla necessità di assicurare la funzione sociale di internet[3]. Infine, non si può trascurare che oggigiorno le grandi piattaforme sociali sono in grado di esercitare un'influenza significativa sulla vita politica delle nazioni[4]: il conferimento ad esse di

[1] * Il presente lavoro costituisce il testo aggiornato e integrato dell'intervento tenuto al *X Corso di formazione interdottorale di diritto e procedura penale "Giuliano Vassalli" per dottorandi e dottori di ricerca – VIII Convegno della sezione "giovani penalisti" del gruppo italiano dell'Association Internationale de Droit Pénal (AIDP),* svoltosi a Siracusa (22-24 ottobre 2020), ed è destinato al volume *I nuovi volti del sistema penale fra cooperazione pubblico-privato e meccanismi di integrazione fra* hard law *e* soft law.

Con questa espressione s'intende qui individuare non solamente i reati informatici in senso stretto, ma anche i c.d. reati cibernetici, cioè gli illeciti comuni commessi per il tramite della rete: su questa distinzione e sull'opportunità del suo superamento S. Seminara, Internet *(diritto penale)*, in *Enc. dir.*, 2014, Ann. VII, 567 s., e la letteratura ivi citata.

[2] Sul punto ampiamente C. Conti – M. Torre, *Spionaggio digitale nell'ambito dei* social network, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2019, 553 ss. Come noto, sull'effettività della tutela penale rispetto ai reati commessi tramite internet incide anche la volatilità del dato digitale; per approfondimenti sulla disciplina della *data retention* nel quadro eurounitario R. Flor, Cyber-criminality: *le fonti internazionali ed europee*, in A. Cadoppi – S. Canestrari – A. Manna – M. Papa (diretto da), Cybercrime, Torino, 2019, 131 ss.

[3] A conferma di ciò si consideri la *Décision n° 2020-801 DC du 18 juin 2020* del *Conseil Contitutionnel* francese, che ha dichiarato l'illegittimità costituzionale degli artt. 1, 4, 5, 7, 8, 9 e 18 della *LOI n° 2020-766 du 24 juin 2020*, che introduceva fra l'altro una serie di obblighi in capo ai gestori delle piattaforme sociali, volti ad assicurare la pronta rimozione dei contenuti illeciti caricati dagli utenti; nel dichiarare la contrarietà a Costituzione della legge, la Corte ha evidenziato l'attitudine delle suddette disposizioni a porre un limite non necessario e comunque sproporzionato alla libertà di espressione degli utenti (c.d. *chilling effect*: sul punto torneremo *infra*, § 6). Per un inquadramento generale della dimensione costituzionale della rete, in relazione al nostro sistema, vd. invece F. Donati, Internet *(diritto costituzionale)*, in *Enc. dir.*, 2014, Annali VII, 531 ss.

[4] Il riferimento va anzitutto alle pratiche di manipolazione del consenso realizzate tramite *Facebook*, che come noto sembrano avere influenzato la vittoria di Donald Trump alle elezioni presidenziali americane del 2016 e l'esito del *referendum* sulla c.d. Brexit (su questi episodi e sulla loro importanza per l'emersione del fenomeno delle *fake news* T. Guerini, Fake news *e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Torino, 2019, 30 ss.); nemmeno si può ignorare la recente tendenza delle piattaforme digitali a prendere esse stesse posizione all'interno del dibattito pubblico (da ult. vd. la decisione di alcuni *social* di bloccare l'*account* di Donald Trump in seguito all'assalto al Congresso americano: *E Zuckerberg oscura i profili del presidente americano: «Mina la legalità, rischio troppo grande»*, in *Corriere della sera*, 8 gennaio 2020). Sul piano giuridico, questa realtà è alla base dell'attuale

poteri di controllo si deve quindi confrontare con il principio della sovranità statale.
Come si vede, nel settore in esame il tema della collaborazione fra pubblico e privato è denso di risvolti problematici, che in questa sede non è possibile esaminare. Il mio intervento si concentrerà dunque sul ruolo di una particolare categoria di *ISP*, cioè i fornitori di servizi di *social networking*, rispetto alla repressione dei reati informatici che si realizzano mediante la pubblicazione di immagini, pensieri o informazioni: partirò dall'attuale tendenza a responsabilizzare i gestori delle piattaforme sociali, per poi analizzare le possibili implicazioni in campo penale della previsione di più stringenti obblighi di collaborazione in capo ai suddetti *provider*[5].

2. Il concetto di "rete sociale" e la relativa disciplina

Prima di entrare nel vivo del problema, è utile definire il concetto di rete sociale e ripercorrere i tratti essenziali della relativa disciplina. Con riferimento al primo profilo, si può affermare che i Social Network (di seguito *SN*) sono siti che mettono a disposizione uno spazio virtuale, all'interno del quale l'utente ha la possibilità di comunicare e divulgare contenuti, nonché creare un'identità personale e una rete di contatti con la quale condividere le proprie connessioni[6]; rispetto a questa schematizzazione generale, le maggiori piattaforme sociali si connotano altresì per l'offerta di un servizio gratuito e lo sfruttamento commerciale delle informazioni generate dai singoli fruitori.
Alla luce delle annotazioni che precedono non sorprende che, per questi operatori, venga comunemente esclusa l'applicabilità dell'art. 57 c.p., che come noto disciplina lo statuto di responsabilità dei *media* più tradizionali (quotidiani su carta stampata e, da ultimo, anche *on-line*)[7]: a tacer d'altro, nelle reti sociali la comunicazione ha carattere interattivo, di talché viene meno la tradizionale distinzione fra produttore e destinatario dell'informazione. L'attività dei *SN* è stata ricondotta invece al d. lgs. 9 aprile 2003, n.

dibattito relativo allo statuto costituzionale delle piattaforme sociali: per il riconoscimento ad esse di una funzione pubblicistica vd. l'isolata posizione di Trib. Roma, sez. impresa, ord. 11-12 dicembre 2019, RG n. 59264/2019, con cui è stato accolto il ricorso di Casa Pound Italia contro la decisione di *Facebook* di oscurare pagine e *account* riferibili all'associazione e ai suoi rappresentanti, accusati di avere pubblicato contenuti inneggianti all'odio. Per alcune considerazioni critiche intorno a tale ultima decisione P. Falletta, *Controlli e responsabilità dei* social network *sui discorsi d'odio* online, in *questa Rivista*, 1, 2020, 147 ss. e 155 ss.; più in generale, per una panoramica delle opinioni espresse sullo statuto costituzionale di questi *provider*, M. Monti, *Privatizzazione della censura e* Internet platforms*: la libertà di espressione e i nuovi censori dell'agorà digitale*, in *Riv. it. inf. dir.*, 1, 2019, 41 ss.

[5] Si precisa che l'attuale tendenza alla responsabilizzazione degli *ISP* non involge solamente i fornitori di servizi di *social networking*, bensì si proietta anche su altre piattaforme digitali, come i motori di ricerca; nell'impossibilità di una trattazione completa del tema, mi limiterò a esaminare la posizione delle reti sociali, che è stata recentemente al centro di alcune innovative decisioni in campo penale (*infra*, § 4).

[6] La definizione riportata nel testo si trova ad esempio in S. Martinelli, *L'autorità privata del* provider, in P. Sirena – A. Zoppini (a cura di), *I poteri privati e il diritto della regolazione*, Roma, 2018, 556 s. Si precisa che a una sì ampia nozione di *SN* possono essere ricondotti anche siti come *blog* e piattaforme di *video-sharing*; sul punto cfr. C. Conti – M. Torre, *Spionaggio digitale*, cit., 543 s., testo e nt. 19.

[7] Per l'estensione dell'art. 57 c.p. ai quotidiani *on-line* Cass., sez. V, 11 dicembre 2017, n. 13398, in *Guida dir.*, 17, 2018, 83; conf. da ult. Id., sez. V, 23 ottobre 2018, n. 1275, in *Guida dir.*, 15, 2019, 85; in dottrina, per alcune considerazioni critiche intorno a tale soluzione, I. Pisa, *La responsabilità del direttore di periodico* on-line *tra vincoli normativi e discutibili novità giurisprudenziali*, in *Dir. pen. proc.*, 3, 2019, 407 ss.

70, di attuazione della direttiva 2000/31/CE (c.d. Direttiva sul commercio elettronico); tale disciplina s'impernia sul principio di neutralità del prestatore di servizi nella rete e, in maniera coerente con questo presupposto, da un lato esclude un «obbligo generale di sorveglianza [del *provider*] sulle informazioni che trasmette o memorizza», dall'altro stabilisce all'art. 16 che il gestore del sito non risponde dell'eventuale memorizzazione di informazioni illecite a meno che, venuto a conoscenza «su comunicazione delle autorità competenti» del carattere illecito di tali informazioni, egli non agisca immediatamente per la loro rimozione. Dinanzi al quadro delineato, si è ritenuto che i gestori delle piattaforme sociali siano punibili solamente nei casi di partecipazione attiva ai reati commessi dagli utenti ovvero nell'ipotesi di mancata rimozione dei contenuti illeciti oggetto di segnalazione istituzionale[8].

Nei tempi più recenti, però, va diffondendosi la convinzione che la suddetta disciplina sia inadatta a regolare l'attività dei grandi *social media*, la quale invero va ben oltre la mera memorizzazione delle informazioni generate dagli internauti: sulla scorta di questa considerazione, un indirizzo giurisprudenziale vieppiù consistente riconosce in capo ai *provider* più penetranti doveri di intervento e conseguentemente allarga i presupposti per la configurazione della responsabilità civile e penale.

Data l'esiguità del tempo a disposizione, non è possibile analizzare le posizioni assunte dalle diverse corti, anche sovranazionali[9]; soffermiamoci invece sul fondamento politico-criminale dei suddetti orientamenti pretori, per poi riflettere sullo strumento tecnico più adeguato a realizzare un maggior coinvolgimento delle piattaforme sociali nel contrasto ai reati commessi per il mezzo della rete.

3. Il fondamento politico-criminale dell'attuale tendenza alla responsabilizzazione dei Social Network

Alla base dell'attuale domanda di responsabilizzazione dei *SN* vi è in primo luogo la considerazione di carattere generale secondo cui l'enorme espansione del mercato digitale ha determinato il venir meno delle esigenze economiche che, all'inizio degli anni duemila, avevano giustificato la creazione di aree di impunità a favore dei prestatori di servizi nella rete; per tale ragione, sembra invero ragionevole chiedere ai *provider* una più consistente partecipazione alla gestione dei rischi connessi all'utilizzo della rete e ai

[8] Così, ad esempio, Cass., sez. V, 19 febbraio 2018, n. 16751, in *Cass. pen.*, 11, 2018, 3743 ss. Per approfondimenti sul tema D. De Natale, *La responsabilità dei fornitori di informazioni in* internet *per i casi di diffamazione* on line, in *Riv. trim. dir. pen. ec.*, 3, 2009, 572 ss.; I. Salvadori, *I presupposti della responsabilità penale del* blogger *per gli scritti offensivi pubblicati su un* blog *da lui gestito*, in *Giur. mer.*, 4, 2007, 1074 ss.

[9] Per una ricognizione degli orientamenti giurisprudenziali relativi alla responsabilità degli intermediari digitali per gli illeciti commessi dagli utenti M. R. Allegri, Ubi social, ibi ius. *Fondamenti costituzionali dei* social network *e profili giuridici della responsabilità dei* provider, Milano, 2018, 61 ss. e 134 ss., in relazione rispettivamente alla tutela del diritto d'autore e alla fattispecie di diffamazione; con specifico riferimento alla giurisprudenza sovranazionale vd. invece L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in Cybercrime, cit., 81 ss. In questa sede ci limitiamo a richiamare l'attenzione sul concetto di "*host provider* attivo", enucleato dalla Corte di giustizia dell'Unione europea e penetrato anche nel nostro sistema: la nozione viene utilizzata per individuare i *provider* che agiscono sui dati memorizzati al fine di ottimizzarne la fruizione e che per questa ragione non potrebbero godere delle esenzioni di responsabilità previste dalla direttiva 2000/31/CE.

derivanti costi in termini di prevenzione. Peraltro, la capacità di internet di raggiungere una cerchia sempre più estesa di persone rende quanto mai grave l'offesa derivante dagli illeciti commessi nel web; si spiega così la necessità di assicurare una pronta rimozione dei materiali illeciti caricati dagli utenti.

A queste osservazioni si aggiunge che i *SN* costituiscono un terreno particolarmente fertile per la proliferazione di alcuni fenomeni criminali. Infatti, la possibilità per l'utente di nascondere la propria identità personale, unita alla facoltà di costruire una propria rete di connessioni, comporta il venir meno dei freni inibitori tipici della comunicazione reale; di qui la diffusione dei tradizionali reati di opinione e dei discorsi d'odio, i quali destano un peculiare allarme sociale anche per via della capacità di fuoriuscire dalla dimensione virtuale, sfociando nella commissione di azioni violente[10]. Inoltre, occorre considerare che il profitto dei grandi *SN* si basa sullo sfruttamento commerciale delle informazioni condivise dagli utenti; fra l'altro, tale caratterizzazione comporta che la rete sia organizzata in modo da attribuire una particolare visibilità ai materiali che suscitano un interesse maggiore[11]. Poiché, però, la popolarità di un contenuto prescinde dalla liceità della sua pubblicazione, ben può accadere che una simile funzionalizzazione della piattaforma allo scopo di profitto del *provider* entri in conflitto con le esigenze di protezione degli interessi degli internauti, conferendo particolare visibilità, ad esempio, a materiali offensivi o discriminatori[12]. Infine, con specifico riferimento agli *hate speech* non si può trascurare che la "politica d'impresa" seguita dalle maggiori piattaforme digitali sembra contribuire alla radicalizzazione dei fruitori della rete: invero, l'uso di programmi di intelligenza artificiale per offrire un'informazione targettizzata concorre a determinare la creazione di *filter bubble* che spingono l'utente a rafforzare le proprie opinioni e ad esacerbare il registro della comunicazione[13].

In breve: l'attività dei grandi *SN* esibisce rischi peculiari, che, dal punto di vista poli-

[10] Sul fenomeno dell'*hate speech*, in rapporto anche alla *hate violence*, per tutti, L. Goisis, *Crimini d'odio. Discriminazioni e giustizia penale*, Napoli, 2019, 202 ss.; con specifico riferimento alle reti sociali A. Spena, *La parola(-)odio*, in *Criminalia*, 2016, 580 ss., secondo il quale la diffusione all'interno dei *SN* dei discorsi d'odio va messa in correlazione con alcuni «meccanismi tipici dell'agire di massa», che tenderebbero a verificarsi anche in queste piattaforme digitali.

[11] Per approfondimenti, in prospettiva critica, sul modello economico seguito da alcune grandi piattaforme digitali (*SN* come *Facebook*, ma anche motori di ricerca come *Google*), S. Zuboff, *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, London, 2019, trad. it. a cura di P. Bassotti, *Il capitalismo della sorveglianza*, Roma, 2019, spec. 73 ss.

[12] A conferma delle considerazioni riportate nel testo è sufficiente rammentare la vicenda di Tiziana Cantone, giovane donna ritratta in alcuni video pornografici amatoriali successivamente diffusi senza il suo consenso su *Facebook* e diventati virali: la ragazza si tolse la vita, dopo avere intrapreso una dura battaglia legale volta ad ottenere la rimozione delle pagine che la riguardavano. Per alcune considerazioni sull'accaduto e sulla posizione della piattaforma sociale G. Pitruzzella, *La libertà di informazione nell'era di* Internet, in G. Pitruzzella – O. Pollicino – S. Quintarelli (a cura di), *Parole e potere. Libertà di espressione,* hate-speech *e* fake-news, Milano, 2017, ora in *questa Rivista,* 1, 2018, 37 ss.

[13] Per approfondimenti sul punto M. Lamanuzzi, *La disinformazione ai tempi dei* social media*: una nuova sfida per il diritto penale?*, in *Arch. pen.*, 1, 2020, 14 ss.; peraltro, la creazione di *filter bubble* sembra dover essere ricollegata esclusivamente alla c.d. *pre-selected personalization* (così ampiamente M. Monti, *Regolazione, internet e tecnica: le implicazioni di motori di ricerca e* social networks *sulla libertà di informazione*, in *federalismi.it*, 24, 2017, 20 ss.). Per una panoramica sui criteri seguiti da *Facebook* nell'organizzazione dei contenuti presenti nella rete vd. invece P. Costa, *Debolezze algoritmiche, umane fragilità. Tecnologie di apprendimento automatico e* bias *cognitivi nei dispositivi di selezione dei contenuti* on-line*,* in G.Avanzini – G. Matucci – L. Musselli (a cura di), *Informazione e media nell'età digitale*, Milano, 2019, 363 ss.

tico-criminale, giustificano l'attribuzione a questi *provider* di più stringenti compiti di controllo e d'intervento diretti ad assicurare la legalità delle comunicazioni. Una volta giunti a questa conclusione, però, occorre stabilire cosa precipuamente il *SN* sia tenuto a fare e quali siano le implicazioni in campo penale di una sua eventuale mancata attivazione: consideriamo brevemente le risposte recentemente offerte dalla giurisprudenza e dalla dottrina, per poi delineare i possibili sviluppi della materia.

4. Le soluzioni proposte dalla giurisprudenza e dalla dottrina

Il punto di partenza di qualsivoglia riflessione intorno al ruolo dei *SN* risiede nell'impraticabilità di doveri generalizzati di controllo e filtraggio preventivi: a tacer d'altro, una simile soluzione comporterebbe un'inammissibile limitazione della libertà di comunicazione e informazione degli utenti. Escluso dunque che l'*ISP* possa essere punito per non avere impedito all'internauta di pubblicare un materiale antigiuridico, l'indagine si sposta sulla possibilità di chiamare i gestori delle piattaforme sociali a rispondere del suo mantenimento nella rete. A questo proposito occorre ricordare che, *de iure condito*, la direttiva 2000/31/CE subordina la responsabilità del fornitore di servizi *internet* alla conoscenza effettiva dell'antigiuridicità del contenuto, mentre il d. lgs. n. 70 del 2003 stabilisce che l'*host provider* debba attivarsi in seguito alla richiesta dell'autorità giudiziaria.

Tale ultima previsione non consente però di assicurare una tempestiva rimozione del materiale antigiuridico presente nella rete; pertanto, una parte della giurisprudenza e della dottrina ha preso ad affermare che il *SN* risponde della sua mancata attivazione già in seguito alla segnalazione di un privato. Per giungere a questo risultato, un primo orientamento sostiene la configurabilità di una responsabilità per omesso impedimento della protrazione dell'altrui reato[14], mentre un secondo afferma la qualificazione del *provider* alla stregua di un produttore di contenuti, autonomamente punibile per l'illecita diffusione del materiale precedentemente pubblicato dall'utente[15]. Il presupposto di entrambe le ricostruzioni è che il *SN* offre un servizio non "neutrale" e per questa ragione non può godere dei *safe harbour* previsti dalla su richiamata Direttiva[16].

Quanto alla prima soluzione, va considerato però che la maggior parte dei reati di manifestazione del pensiero ha carattere istantaneo[17]; per tale ragione, il mantenimento

[14] Così Cass., sez. V, 14 luglio 2016, n. 54946, con nota critica di R. Carbone, *Responsabilità del* blogger*: parziale* revirement *della Cassazione?*, in *Cass. pen.*, 7-8, 2017, 2782 ss.; aperture verso la soluzione proposta dalla Cassazione si rinvengono, invece, in R. Bartoli, *Brevi considerazioni sulla responsabilità penale dell'*internet service provider, in *Dir. pen. proc.*, 5, 2013, 606.

[15] In questi termini Cass., sez. V, 8 novembre 2018, n. 12546; in dottrina P. Lasalvia, *La diffamazione via* web *nell'epoca dei* social network, in Cybercrime, cit., 356 s. Su questa sentenza e su quella citata nella nota che precede B. Panattoni, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel* cyberspace, in *Sist. pen.*, 5, 2020, 310 ss.; in merito sia consentito rinviare anche a S. Braschi, Social media *e responsabilità penale dell'*Internet Service Provider, in *questa Rivista*, 3, 2020, 163 ss.

[16] Chiaro il riferimento alla figura dell' "*host provider* attivo", a proposito della quale vd. *retro*, nt. 9.

[17] Sul punto S. Seminara, *La responsabilità penale degli operatori* su internet, in *Dir. inf.*, 4-5, 1998, 765; diversamente L. Picotti, *Diritto penale e tecnologie informatiche*, cit., 89 ss. Si segnala che all'interno della

nella rete del contenuto antigiuridico dà luogo a una condotta susseguente, che giocoforza fuoriesce dallo schema del concorso di persone. Inoltre, poiché nell'attuale sistema normativo non è possibile affermare che, in linea generale, i *SN* sono titolari di una posizione di garanzia[18], la punibilità per omesso impedimento dell'altrui violazione può trovare spazio solamente in una prospettiva di politica criminale. Osservazioni non dissimili valgono per l'orientamento che afferma la configurabilità di un'autonoma responsabilità del *provider*: in effetti, in assenza di un obbligo di rimozione, non è agevole comprendere come mai l'automatico, ininterrotto funzionamento dei meccanismi di diffusione dei dati nella rete dovrebbe acquisire un'autonoma tipicità penale; se poi si considera che le piattaforme sociali affidano l'organizzazione delle informazioni a sistemi di intelligenza artificiale, sembra impossibile affermare che il *provider* ha il dolo richiesto per la punibilità delle singole violazioni[19]. Infine, nel silenzio del legislatore, le due ricostruzioni affidano il giudizio sulla neutralità della piattaforma sociale all'interprete e una simile impostazione cozza con le esigenze di certezza del diritto e prevedibilità della sanzione.

Il vero è che, al fine di ottenere una maggiore responsabilizzazione dei gestori delle piattaforme sociali, risulta imprescindibile un intervento del legislatore; assunta questa prospettiva, però, restano da chiarire il fondamento e l'ampiezza della punibilità del *provider*. In proposito, si è già osservato che il fornitore del servizio di *social networking* non ha un legame con l'utente-produttore del contenuto, che giustifichi una responsabilità di tipo editoriale; aggiungiamo che, considerata l'enorme quantità di dati presenti nella rete, nemmeno sembra sensato addebitare al gestore del sito la *volontaria* diffusione di un materiale antigiuridico. La mia opinione è che, più ragionevolmente, al *SN* possa essere rimproverata la mancata assunzione di misure volte a contenere il rischio della circolazione dei contenuti illeciti pubblicati dagli utenti; il significato di questa affermazione risulterà più chiaro dopo una breve digressione sul funzionamento delle

giurisprudenza civile ricorre l'affermazione del carattere permanente dei reati commessi nella rete: così, *ex multis*, Cass. civ., sez. I, 21 febbraio 2019, n. 7708, in *Riv. dir. ind.*, 4-5, 2019, II, 201.

[18] Invero, tralasciando la possibilità di ricavare, nell'ambito delle normative di settore, degli specifici doveri di protezione, la dottrina e la giurisprudenza maggioritarie ritengono che il d. lgs. n. 70 del 2003 costituisca la fonte di obblighi di attivazione, che solo nel caso di una richiesta d'intervento della competente autorità amministrativa o giudiziaria possono dare luogo a un'autonoma responsabilità penale: così spec. Cass. pen., sez. III, 17 dicembre 2013, n. 5107, in *Riv. pen.*, 5, 2014, 495; in dottrina, *ex multis*, A. Ingrassia, *Responsabilità penale degli* internet service provider*: attualità e prospettive*, in *Dir. pen. proc.*, 12, 2017, 1626 s.; S. Seminara, Internet, cit., 597 s. Sostiene, invece, l'esistenza di una posizione di garanzia in capo al gestore di una piattaforma di *video-sharing* F. Sgubbi, *Parere* pro veritate, in *Dir. inf.*, 4-5, 2009, 745 ss.; cfr., con riferimento al settore della pedopornografia, L. Picotti, *Art. 600*-ter, *III comma c.p.*, in A. Cadoppi (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Padova, 2006, 210 ss., e, rispetto a quello del diritto d'autore, R. Flor, Social network *e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Riv. trim. dir. pen. ec.*, 3, 2012, 681 s.

[19] Per alcune considerazioni critiche intorno a questa soluzione B. Panattoni, *I riflessi penali*, cit., 316 ss.; evidenzia la difficoltà di rinvenire una «concreta rimproverabilità», anche una volta risolto il problema della tipicità oggettiva dell'illecito addebitato al *provider* C. Melzi d'Eril, Fake news *e responsabilità: paradigmi classici e tendenze incriminatrici*, in *questa Rivista*, 1, 2017, 66. In generale, sulle implicazioni a livello costituzionale dell'assimilazione delle piattaforme sociali ai *content provider*, O. Pollicino, *Tutela del pluralismo nell'era digitale: ruolo e responsabilità degli* Internet Service Provider, in *Consulta Online*, 3 febbraio 2014, 18 ss.

"procedure di segnalazione e rimozione" (*notice and action procedure*).

5. Le prospettive di sviluppo della materia: le *"notice and action procedure"*

Con l'espressione "*notice and action procedure*" o "*notice and take down procedure*" s'intende un meccanismo di controllo successivo, caratterizzato per l'eliminazione da parte del gestore della piattaforma sociale dei contenuti illeciti segnalati dagli utenti; sorte sul terreno del diritto d'autore e progressivamente estese alla repressione dei discorsi d'odio, siffatte "procedure di segnalazione e rimozione" stanno acquisendo un'importanza sempre maggiore all'interno del continente europeo[20].

In primo luogo, infatti, non si può trascurare che, in una prospettiva di parziale superamento della direttiva 2000/31/CE, lo scorso 15 dicembre 2020 la Commissione Europea ha presentato una proposta di Regolamento (*Digital Services Act*, di seguito *DSA*), che mira a subordinare l'esonero dalla responsabilità per la memorizzazione dei contenuti illeciti generati dagli utenti all'adozione, da parte degli *hosting provider*, di procedure di segnalazione e rimozione. Si prevede che i fornitori di servizi di memorizzazione debbano mettere in atto meccanismi trasparenti e facilmente accessibili, che consentano a qualsiasi persona di segnalare la presenza di specifici contenuti illegali (art. 14)[21]. Quindi, si chiarisce che, nel caso di segnalazione sufficientemente precisa e motivata, il gestore della piattaforma digitale ha una "conoscenza effettiva" della violazione commessa dall'utente; donde la sua responsabilità nel caso di mancata rimozione del contenuto oggetto di memorizzazione[22]. Tale innovazione non sorprende, ove solo si consideri che in un'analoga direzione si era già orientata la direttiva (UE) 2019/790 del 17 aprile 2019, in tema di *copyright*: dopo avere stabilito che le piattaforme di *file-sharing*

[20] Sulle origini delle procedure di segnalazione e rimozione, anche in ottica comparata, B. Panattoni, *Il sistema di controllo successivo: obbligo di rimozione dell'ISP e meccanismi di* notice and take down, in *Dir. pen. cont.*, 5, 2018, 256 ss. Per completezza, va ricordato che nel 2016 la Commissione europea, in collaborazione con alcune piattaforme digitali, ha promosso la redazione del *Code of conduct countering illegal hate speech online*, il quale fra l'altro stabilisce che «le aziende informatiche predispongono procedure chiare ed efficaci per esaminare le segnalazioni riguardanti forme illegali di incitamento all'odio nei servizi da loro offerti, in modo da poter rimuovere tali contenuti o disabilitarne l'accesso»; l'importanza delle suddette procedure è stata ribadita anche dalla Raccomandazione n. 2018/334, del 1° marzo 2018.

[21] Per maggiori dettagli, vd. il testo della *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE*.

[22] Va evidenziato che le *online platform* di medie e grandi dimensioni devono altresì adottare un sistema interno di reclamo e comunicare ai competenti organi di polizia le informazioni di cui siano venuti a conoscenza, dalle quali sia possibile ricavare il sospetto che è stato commesso o è in corso un grave reato, il quale comporti un pericolo per la vita e l'incolumità fisica della persona; la definizione di *online platform* si rinviene all'art. 2, lett. h («un prestatore di servizi di *hosting* che, su richiesta di un destinatario del servizio, memorizza e diffonde al pubblico informazioni, tranne qualora tale attività sia una funzione minore e puramente accessoria di un altro servizio»), mentre l'art. 16 chiarisce che sono esentati dagli obblighi previsti dalla sezione le *online platform* che rientrino nella nozione di *micro or small enterprise* ai sensi della Raccomandazione 2003/361/EC. Per completezza, segnaliamo infine che il *DSA* prevede ulteriori doveri per le *very large platform*, fra i quali rientrano l'adozione di misure di valutazione e mitigazione dei rischi di diffusione di contenuti antigiuridici e obblighi di trasparenza e rendicontazione (art. 25 ss.).

non beneficiano delle esenzioni stabilite dalla Direttiva sul commercio elettronico, l'art. 17 da un lato ha affermato la responsabilità del *provider* per la messa a disposizione del materiale protetto da diritto d'autore, dall'altro ha stabilito che il gestore del sito non risponde nel caso in cui dimostri «di aver agito tempestivamente, dopo aver ricevuto una segnalazione sufficientemente motivata dai titolari dei diritti, per disabilitare l'accesso o rimuovere [dal sito] *web* le opere o altri materiali oggetto di segnalazione e aver compiuto i massimi sforzi per impedirne il caricamento in futuro»[23].

Analoghe soluzioni sono state già sperimentate nell'ambito delle legislazioni nazionali. Anzitutto, va rammentato che nel 2017 la Germania si è dotata di una "legge per il miglioramento della tutela dei diritti sui social network" (*Netzwerkdurchsetzungsgesetz*, di seguito NetzDG), la quale prevede che i *SN* con più di due milioni di utenti registrati all'interno dello stato tedesco siano tenuti ad adottare procedure trasparenti ed efficaci per la rimozione del materiale antigiuridico[24]. Senza entrare nel dettaglio della normativa, è bene sottolineare che la NetzDG impone termini stringenti per la rimozione dei contenuti oggetto di segnalazione (ventiquattro ore nelle ipotesi di illiceità manifesta, sette giorni negli altri casi), stabilendo peraltro che, per la soluzione dei casi più controversi, il *SN* abbia la possibilità di interpellare un organo di autoregolamentazione indipendente appositamente creato; commina inoltre onerose sanzioni pecuniarie per l'ipotesi della sua mancata attuazione (fino a cinque milioni di euro nei casi più gravi, § 4). Nella medesima direzione sembra volersi orientare anche l'ordinamento austriaco[25], mentre in Francia il *Conseil Constitutionnel* ha censurato la *LOI n° 2020-766*, *du 24 juin 2020*, che imponeva alle piattaforme digitali l'adozione di misure di *notice and action*, minacciando gravi sanzioni in caso di inadempimento: partendo dal presupposto che la previsione di doveri di controllo e di rimozione da attuare entro termini stringenti incentivi l'assunzione da parte degli *ISP* di atteggiamenti censori, la Corte ha ritenuto

[23] È opportuno precisare che la Direttiva si applica al «prestatore di servizi della società dell'informazione il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro» (art. 2, n. 6). Se, in linea generale, «i prestatori di servizi di condivisione di contenuti *online* sono responsabili per atti non autorizzati di comunicazione al pubblico, compresa la messa a disposizione», la loro responsabilità è però esclusa – oltreché nei casi indicati nel testo – se dimostrano di «aver compiuto i massimi sforzi per ottenere un'autorizzazione» ovvero di «aver compiuto, secondo elevati standard di diligenza professionale di settore, i massimi sforzi per assicurare che non siano disponibili opere e altri materiali specifici per i quali [abbiano] ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti» (art. 17).

[24] BT-Drucksache 18/12356; il testo in italiano della legge può essere consultato in *Dir. inf.*, 4-5, 2017, 723 ss. (trad. a cura di G. Codiglione). Sui contenuti del provvedimento e sulle ragioni alla base della sua adozione vd. S. Müller-Franken, *Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Verfassungsrechtliche Fragen*, in *Archiv für Presserecht*, 2018, 1 ss. e, nella dottrina italiana, T. Guerini, Fake news *e diritto penale*, cit., 79 ss. Si evidenzia che la NetzDG, se da un lato adotta una nozione ampia di *SN*, dall'altro dà rilevanza alla finalità di profitto dell'attività svolta da questi operatori; siffatta soluzione, che per la verità sembra un ragionevole tentativo di limitare l'operatività degli obblighi ai soggetti dotati dei mezzi economici necessari alla loro implementazione, è invece criticata da M. Bassini – G. E. Vigevani, *Primi appunti su* fake news *e dintorni*, in *questa Rivista*, 1, 2017, 19, secondo i quali l'«approccio tedesco (basato sul *follow the money*) appare problematico in quanto presuppone che la capacità di ottenere profitti da parte di una piattaforma significhi un suo maggiore coinvolgimento (o quantomeno l'esigibilità di una condotta attiva) nella rimozione dei contenuti».

[25] Si allude alla *Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-gesetz-KoPi-G*.

la suddetta legge lesiva della libertà di comunicazione e informazione degli utenti[26].
Quanto, infine, al nostro sistema, alle procedure di segnalazione e rimozione dei contenuti fa riferimento la l. 29 maggio 2017, n. 71, in tema di *cyberbullismo*: l'art. 2 prevede che il minore ultraquattordicenne, nonché il genitore o esercente la responsabilità del minore che abbia subito atti di *cyberbullismo* possono chiedere l'oscuramento di qualsiasi dato personale della vittima al titolare della piattaforma sociale. La legge non contempla alcuna sanzione per l'ipotesi in cui il *provider* ometta di dare un riscontro tempestivo; tuttavia, stabilisce che, in questa eventualità, l'utente abbia la possibilità di adire il Garante della *privacy* al fine di ottenere la pronta rimozione del contenuto illecito oggetto della segnalazione. Infine, verso l'introduzione di procedure obbligatorie di segnalazione e rimozione si orientava anche il d.d.l. n. 3001, del 14 dicembre 2017, c.d. d.d.l. Zanda-Filippin, il quale presentava contenuti affini alla su menzionata NetzDG; tale proposta, però, non ha mai avviato l'*iter* parlamentare[27].
Sintetizzando, si può affermare che sul versante legislativo si registra una comune tendenza ad attribuire alle piattaforme sociali doveri di controllo successivo, eventualmente sanzionandole per la loro mancata implementazione: in tal modo, si ritiene possibile limitare i danni derivanti dalla pubblicazione di materiali antigiuridici, senza peraltro gravare gli *ISP* di obblighi eccessivamente onerosi né attuare una sorveglianza generalizzata delle comunicazioni.

6. Considerazioni finali

A questo punto, è possibile svolgere alcune considerazioni conclusive intorno ai possibili sviluppi della materia. Abbiamo visto che, in linea generale, si fa strada l'idea secondo cui, per minimizzare il rischio della circolazione di materiali antigiuridici nella rete, è opportuno incentivare l'adozione da parte delle piattaforme sociali di meccanismi di controllo successivo, attivabili su richiesta dell'utente e finalizzati alla rimozione dei contenuti illeciti. Questa evoluzione, se da un lato riflette condivisibili esigenze di tutela, dall'altro consente di ovviare alla inadeguatezza dei modelli di responsabilità già sperimentati con riferimento ai *media* più tradizionali: a tacer d'altro, la loro estensione ai *SN* è ostacolata dalle caratteristiche della comunicazione digitale e dall'ampiezza dei dati presenti nella rete. Dal confronto fra le disposizioni che abbiamo prima menziona-

[26] Va però segnalato che nel 2018 la Francia si è dotata di due leggi (*Loi organique n° 2018-1201* e *n° 2018-1202*, *du 22 décembre 2018*), che prevedono alcuni obblighi di trasparenza in capo ai *provider* e stabiliscono la possibilità, durante il periodo elettorale, di ricorrere agli organi giudiziari per ottenere entro 48 ore la rimozione di notizie fase diffuse nella rete; tali previsioni sono state giudicate compatibili con la Costituzione dal *Conseil Constitutionnel* con la *Décision n° 2018-773, du 20 décembre 2018*. Per approfondimenti sui contenuti della legge e sulla decisione T. Guerini, Fake news *e diritto penale*, cit., 75 ss.; C. Magnani, *Libertà d'informazione* on-line *e* fake-news*: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in forumcostituzionale.it, 18 aprile 2019, 16 ss.

[27] Sul contenuto della proposta e per alcune considerazioni critiche T. Guerini, Fake news *e diritto penale*, cit., 173 ss.; F. De Simone, *"*Fake news*", "*post truth*", "hate speech": nuovi fenomeni sociali alla prova del diritto penale*, in *Arch. pen.*, 2 aprile 2018, 17 ss.; dal punto di vista del diritto costituzionale, M. Monti, *La proposta del d.d.l. Zanda-Filippin sul contrasto alle* fake news *sui* social network*: profili problematici*, in dirittocomparati.it, 7 dicembre 2017, spec. 3 ss.

to emerge però che la valorizzazione delle misure di *notice and action* solleva due fondamentali interrogativi: il primo involge l'ampiezza dei poteri che possono essere delegati alle piattaforme digitali, il secondo riguarda invece il riflesso delle suddette procedure sulla responsabilità del fornitore di servizi nella rete. Esaminiamoli brevemente.

Con riferimento alla prima questione, si è visto che l'attribuzione al *SN* del compito di stabilire la liceità di una pubblicazione solleva perplessità che attengono al rispetto della libertà di espressione e informazione degli internauti. In effetti, il *provider* non è un soggetto imparziale, sicché il conferimento ad esso di funzioni di controllo non sembra offrire sufficienti rassicurazioni contro il pericolo di decisioni arbitrarie[28]; peraltro, il *SN* a differenza di un editore ha uno scarso interesse alla singola pubblicazione e per questo motivo è portato a eliminare i contenuti oggetto di segnalazione, così ulteriormente comprimendo la libera circolazione delle opinioni nella rete (c.d. *chilling effect*)[29]. Infine, non si possono trascurare i costi derivanti dalla necessità di soddisfare gli obblighi di controllo imposti dal legislatore, i quali rischiano di pregiudicare i siti di piccole dimensioni e conseguentemente intaccare il pluralismo dell'informazione.

Sebbene dotate di fondamento, queste osservazioni non sembrano però decisive. Per non pregiudicare la funzione sociale delle piattaforme digitali, una parte della dottrina ha invero proposto di affiancare i *provider* nelle singole decisioni, mediante l'istituzione di appositi organi statali[30]: questa soluzione consentirebbe di assicurare il controllo sull'operato del *SN* e al contempo arginare l'adozione di atteggiamenti censori, volti a ridurre il rischio di incappare nella responsabilità civile e penale. Nella medesima direzione si muove anche il *DSA*, il quale, se da un lato impone alle medio-grandi piat-

[28] Sul punto M. Monti, *Privatizzazione della censura*, cit., 37 ss.; il problema era stato già sollevato, con riferimento però al motore di ricerca *Google*, da O. Pollicino, *Google rischia di "vestire" un ruolo paracostituzionale*, in *Il Sole 24 ore*, 14 maggio 2014. È chiaro, peraltro, che il rischio di decisioni arbitrarie si manifesta soprattutto allorché si rende necessario bilanciare esigenze di tutela e libertà costituzionali, come nei tradizionali reati di opinione, ovvero in presenza di illeciti politicamente più sensibili (cfr. però, con riferimento ai reati di parola collegati al terrorismo internazionale di matrice islamica F. Fasani, *Le "parole preparatorie". I reati antiterrorismo di parola nell'era dei* new media, in *Dir. pen. cont. – Riv. trim.*, 1, 2019, 117 ss.).

[29] Si tratta del fenomeno del c.d. *overblocking*: in merito vd. le considerazioni di E. Rosati – G. Sartor, Social networks *e responsabilità del* provider, in *EUI working papers*, LAW 5, 2012, 8: «Mentre l'editore del giornale ha un forte interesse alla pubblicazione degli articoli, ciascuno dei quali è importante elemento del giornale e concorre a determinarne il valore commerciale, il titolare di una piattaforma aperta per il *Web* ha scarso interesse alla presenza di un particolare contributo […] e pertanto normalmente anziché difendere quel contributo di fronte alle rimostranze dei terzi, preferirà procedere alla sua rimozione». Condividono queste osservazioni, *ex multis*, M. Bassini – G. E. Vigevani, *Primi appunti*, cit., 20; C. Melzi d'Eril, Fake news *e responsabilità*, cit., 66. Con specifico riferimento all'impostazione accolta dalla NetzDG, cfr. G. Nolte, *Hate-Speech, Fake-News, das «Netzwerkdurchsetzungsgesetz» und Vielfaltsicherung durch Suchmaschinen*, in *Zeitschrift für Medienwissenschaft*, 2017, 556 ss. e A. Lang, *Netzwerkdurchsetzungsgesetz und Meinungsfreiheit. Zur Regulierung privater Internet-Intermediäre bei der Bekämpfung von Hassrede*, in *Archiv des Öffentlichen Recht*, 2, 2018, 232 ss.

[30] Così M. Monti, *Le* Internet platforms*, il discorso pubblico e la democrazia*, in *Quad. cost.*, 4, 2019, 826 s., il quale sostiene la necessità di affidare alla pubblica autorità il giudizio "in secondo grado" sulla liceità della pubblicazione; la necessità del coinvolgimento di organi statali è stata affermata per la prima volta da G. Pitruzzella, *La libertà di informazione*, cit., 26. Nella letteratura penalistica cfr. T. Guerini, Fake news *e diritto penale*, cit., 206 ss., il quale individua nella NetzDG un modello di disciplina esportabile anche nel nostro paese, ritenendo peraltro opportuno affidare a un'autorità amministrativa indipendente – nello specifico l'AGCOM – il ruolo di «intermediario tra chi propone il reclamo e il gestore del *social network*, chiamato a valutarne la fondatezza».

taforme di implementare sistemi interni di reclamo, dall'altro statuisce che i soggetti raggiunti da un provvedimento del *provider*, che abbia stabilito la rimozione di un contenuto o la disabilitazione del relativo *account* personale, abbiano la possibilità di rivolgersi ad appositi e riconosciuti organi stragiudiziali; in ogni caso, resta impregiudicato il diritto dell'utente alla tutela giurisdizionale[31].

Più articolato – quantomeno nella prospettiva del cultore del diritto penale – è il discorso relativo all'incidenza delle procedure di *notice and action* sulla responsabilità del *provider*: a questo proposito occorre assicurare che il *SN* eserciti un controllo effettivo, senza peraltro sfociare in forme di responsabilità di posizione, che avrebbero, fra l'altro, la conseguenza di mortificare l'iniziativa economica degli operatori e la libertà di informazione degli utenti. Ciò precisato, abbiamo visto che la direttiva (UE) 2019/790 sembra individuare nella predisposizione di meccanismi di segnalazione e rimozione un'esimente per la responsabilità derivante dalla diffusione dei contenuti antigiuridici pubblicati dall'utente, mentre il sistema tedesco ha optato per la creazione di un autonomo illecito amministrativo, incentrato sulla mancata implementazione delle suddette procedure.

A livello strutturale, la prima soluzione ricalca la più tradizionale responsabilità di tipo editoriale, dalla quale si distingue però per il carattere successivo del controllo e per la maggiore specificazione del dovere di diligenza imposto alla piattaforma sociale: in buona sostanza, si tratta infatti di addebitare al *provider* la *colposa* diffusione del contenuto antigiuridico prodotto dall'utente[32]. La ricostruzione presta il fianco però a due obiezioni: anzitutto, si potrebbe osservare che ha poco senso applicare al *SN* la pena prevista per il fatto principale, atteso che la sua "colpa" consiste in un difetto di organizzazione; in secondo luogo, in assenza di una specifica previsione, il compito di verificare l'adeguatezza del sistema di segnalazione e rimozione spetta al giudice competente per il reato informatico e una simile impostazione potrebbe incidere negativamente sulla prevedibilità della sanzione[33]. Sotto questo profilo, parrebbe dunque preferibile la soluzione accolta dalla NetzDG, che affida a un apposito ufficio il giudizio relativo alla congruità dei meccanismi di "*notice and action*"[34]; parametrando la sanzione alle dimensioni del *SN*, questa legge sembra inoltre assicurare una maggiore effettività

[31] In proposito vd. gli artt. 17 e 18. Il *DSA* prevede inoltre l'istituzione, all'interno di ciascuno stato membro, di un *Digital service coordinator* chiamato a vigilare sull'esatta attuazione del Regolamento; fra l'altro, questo soggetto deve certificare l'imparzialità e adeguatezza degli organismi di risoluzione delle controversie citati nel testo.

[32] Sul modello di responsabilità disciplinato dall'art. 57 c.p., che secondo la dottrina più recente configura un autonomo reato proprio colposo dell'editore, vd. per tutti, F. Mantovani, *Manuale di diritto penale. Parte generale*, Milano, 2020, 429, e la letteratura ivi citata; è peraltro opportuno sottolineare ancora che il rapporto fra *SN* e produttore del contenuto è molto meno stretto di quello che lega editore e giornalista.

[33] È cioè evidente che l'illecito commesso dalla piattaforma sociale presenta un più marcato carattere economico; con riferimento alla seconda osservazione, parafrasando considerazioni sviluppate nel settore della responsabilità amministrativa degli enti, si potrebbe affermare che "alla certezza dei costi (di progettazione e implementazione del sistema di segnalazione e rimozione) si contrappone l'incertezza della valutazione di adeguatezza" (sul punto vd. ampiamente C. Piergallini, *Il modello organizzativo alla verifica della prassi*, in *Le Soc. Gli speciali*, 2011, 49 ss.).

[34] Per alcune considerazioni critiche sulla terzietà dei soggetti coinvolti nella valutazione dell'adeguatezza del sistema di *notice and action* C. Magnani, *Libertà d'informazione* on-line, cit., 15 s.

all'obbligo di implementare il sistema di segnalazione e rimozione. D'altra parte, però, occorre evidenziare che la disciplina tedesca si caratterizza per un notevole rigore punitivo, il quale trova scarsa giustificazione alla luce della posizione secondaria dell'*ISP* rispetto all'autore della violazione principale; se poi si considera che nel settore della comunicazione la previsione di sanzioni fortemente afflittive solleva delicati problemi in termini di legittimità costituzionale[35], prende forza l'idea della necessità di temperare le sanzioni applicabili alle piattaforme sociali.

Concludendo, segnaliamo che, al fine di assicurare l'attuazione del Regolamento, il *DSA* prevede che gli stati membri debbano adottare sanzioni «efficaci, proporzionate e dissuasive», senza peraltro superare limiti percentuali legati all'entità del fatturato del singolo intermediario digitale (art. 42): ove ve ne fosse bisogno, la previsione conferma che i *provider* sono destinati a ricoprire un ruolo sempre più importante nel contrasto ai reati commessi nella rete e suggerisce l'importanza di aggiornare la riflessione intorno allo statuto penale di questi operatori.

[35] In proposito, è sufficiente rammentare le numerose prese di posizione della Corte Europea dei Diritti dell'Uomo contro il ricorso alla pena detentiva per le violazioni commesse dai *media* più tradizionali e la conseguente questione di legittimità costituzionale avanzata nel nostro sistema per il delitto di diffamazione a mezzo stampa: sul punto, per tutti, M. C. Ubiali, *Diffamazione a mezzo stampa e pena detentiva: la Corte costituzionale dà un anno di tempo al Parlamento per trovare un punto di equilibrio tra libertà di espressione e tutela della reputazione individuale, in linea con i principi costituzionali e convenzionali*, in *Riv. it. dir. proc. pen.*, 3, 2020, 1476 ss.

Diversity of exposure in social media markets: regulating or unbundling content curation*

Maria Luisa Stasi

Abstract

Access and exposure to a diversity of voices is a fundamental pillar of democracy. On social media markets, exposure diversity is limited by various factors, one being how platforms curate the content each user sees. The algorithmic systems for content curation used by those platforms artificially can reduce exposure diversity to the benefit of profit-making parameters. This paper describes the challenge, suggests two possible regulatory solutions to address it, and proposes an analytical framework to assess and compare them. The first is to regulate content curation in a way that guarantees diversity. The second is to unbundle hosting from content curation activities, and to oblige large platforms to allow third parties to offer content curation to users. The two remedies come from different normative paths and require different enforcement mechanisms, among others. The preliminary conclusion is that the unbundling might be a better option.

Table of contents

1. Introduction. - 2. Media diversity. - 3. Exposure diversity. - 4. Exposure diversity on social media: the market failures. - 5. Two proposals. - 6. An analytical framework to assess them. - 7. Conclusions

Keywords

content curation - exposure diversity - social media – unbundling – regulation and competition

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

I am extremely grateful to Prof Giorgio Monti and Prof Alexandre de Streel for their suggestions and comments. Errors and inaccuracies remain mine.

1. Introduction

Access and exposure to a diversity of voices are a fundamental pillar of a democracy, and a necessary premise for an open and informed public discourse that allows citizens to form their opinions and to engage in civic space. The media diversity landscape has changed substantially in the past two decades. Digitalisation and the rise of social media platforms have created numerous new channels for information and content to be produced, shared and accessed. Nevertheless, the increase of content available online might not automatically translate in an increase in the diversity of content each individual is exposed to online. This paper focuses on social media markets, and on individuals' diversity of exposure therein.

Social media platforms have revolutionised the way people communicate, access and share information. In little over a decade, they have reached billions of people around the globe, enabling exciting achievements but also raising serious concerns relating to the protection of human rights. The impact they have had on society is multi-faceted, and has opened the door to many research questions, relevant for social, political and economic studies alike. Much has been said already, both in support of and against the impact of these platforms on the economy and society. Recently, the major social media companies have been under attack for a number of reasons, facing proceedings before data protection and competition authorities as well as national and regional courts, and have been targeted by various legislative, regulatory and policy actions.

Notwithstanding this hype, the various challenges that social media platforms raise for competitors, users and society still require sustained scrutiny, and resolution. Among other questions, the way Facebook, Twitter, YouTube and similar platforms curate content remains at the centre of harsh debate. "Content curation", *per se*, is quite a vague concept[1], which is accused of playing a major role in phenomena like the spread of disinformation, the creation of echo chambers, the spread of hate speech online, and the manipulation of elections, among other things.

Less prominent in the discussion of how content is curated appears to be the issue of reduced diversity of exposure for individual users, that is the reduction in the diversity of content they are exposed to, which is a tiny fraction of the diversity of content which exists online. While there are many reasons why individuals suffer from under-exposure on social media, the artificial reduction of exposure diversity caused by the profit-driven business models and automated systems used by private actors is to be further explored, not least to allow decision makers and regulators to properly approach it. This artificial reduction is what this paper focuses on. Part I briefly in-

[1] In this paper, I call "content curation" the measures taken by social media platforms that affect the availability, visibility and accessibility of content, such as ranking, promotion, demotion. These measures are performed by fully or partially automated systems based on algorithms. Content curation differs from content moderation, which usually indicates the activities undertaken by social media platforms to detect, identify and address illegal content or content incompatible with their terms and conditions, such as demotion and removal. For a definition of these concepts see: European Commission, Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM(2020) 825 final, Article 2; E. M. Mazzoli - D. Tambini, *Prioritisation Uncovered. The Discoverability of Public Interest Content Online*, Council of Europe study, DGI(2020)19, 2020.

troduces the concept of media diversity, with specific reference to exposure diversity. Part II looks at the under exposure on social media markets, and provides some arguments about the role played by content curation in this market failure. Part III suggests two possible regulatory solutions, comparing them against a list of benchmarks. Part IV briefly sum ups and provides some conclusive thoughts that might be useful for to regulators and scholars.

Part I

2. Media diversity

Media diversity is used to refer to the broadest possible diversity of information, ideas and viewpoints that are communicated. Together with media plurality, which refers to the plurality of media actors, types of media, and ownership, media diversity is a component of the concept of media pluralism, an essential element of open and free debate in society, and thus a pillar of a democracy.

Media diversity is a normative value, and the way it is framed and operationalised depends on the specific legislative instrument of reference[2]. It is not a goal in itself but rather a means to an end: it is instrumental to the achievement a number of democratic goals, such as «promoting a critical debate and wider democratic participation of persons belonging to all communities and generations»[3]. As recently reminded by the Council of Europe, States have the obligation to protect media diversity by putting in place an appropriate legislative and policy framework to promote «the availability, findability and accessibility of the broadest possible diversity of media content as well as the representation of the whole diversity of society in the media»[4].

However, notwithstanding its central value for media law and policy, media diversity is ill-defined, there is even conceptual disagreement on the meaning of the notion[5]. Research has shown that, often, the terms media pluralism and media diversity are used interchangeably[6]. However, some scholars insist on the fact that the two terms refer to different components and use diversity as a measure for content and pluralism as a measure for the sources[7].

---

[2] N. Helberger - K. Karppinen - L. D'Acunto, *Exposure diversity as a design principle for recommender systems*, in *Information, Communication & Society*, 21(2), 2018, 191 ss.

[3] Council of Europe, Recommendation CM/Rec(2018)1[1] of the Committee of Ministers to member States on media pluralism and transparency of media ownership, 2018.

[4] *Ibid.*

[5] M. Pearson - J.E. Brand - D. Archbold - H. Rane, *Sources of News and Current Affairs,* Gold Coast, 2001; Ofcom, *Measurement Framework for Media Plurality: Ofcom's Advice to the Secretary of State for Culture, Media and Sport*, 2015.

[6] F. Loecherbach - J. Moeller - D. Trilling - W. Atteveldt, *The Unified Framework of Media Diversity: A Systematic Literature Review*, in *Digital Journalism*, 8(5), 2020, 605 ss.; C. P. Hoffman - C. Lutz - M. Meckel - G. Ranzini, *Diversity by Choice: Applying a Social Cognitive Perspective to the Role of Public Service Media in the Digital Age,* in *International Journal of Communication*, 9(1), 2015, 1360 ss.; A. Ciaglia, *Pluralism of the System, Pluralism in the System: Assessing the Nature of Media Diversity in Two European Countries*, in *International Communication Gazette*, 75(4), 2013, 410 ss.

[7] A. Masini - P. Van Aelst, *Actor Diversity and Viewpoint Diversity: Two of a Kind?,* in *Communications*, 42(2),

A certain degree of uncertainty around the concept of media diversity expands to how to measure it[8]. Possibly the most complete indications and measures of media diversity in the EU are provided by the Media Pluralism Monitor Project, which makes clear that diversity is a complex outcome which cannot be measured by looking at one of few indicators only[9]. In addition, it is noted that the benchmark(s) for a satisfactory level of media diversity might vary depending on the specific goal to be achieved[10].

3. Exposure diversity

While discussing media diversity, various tended to concentrate on the supply side of the market, that is on the sources. However, in recent years this conceptualisation seems to have evolved, and scholars have added the diversity of exposure dimension, and argued that diversity of supply does not guarantee it. For example, with regard to traditional broadcasting, scholars have pointed at the mismatch between the diversity as sent and the diversity as received[11].

Diversity of exposure is defined as indicating the diversity received and effectively consumed by individuals[12]. This concept looks not at the overall offering available on the market, but at the offering that is factually available to each individual and, some have argued, includes an additional element, that is the choice among the absolute amount of content available[13].

To the extent that the amount of content supplied largely exceeds the amount of content that each individual can consume[14], exposure diversity becomes an ever more

2017, 107 ss.; C. Baden - N. Springer, *Conceptualizing Viewpoint Diversity in News Discourse*, in *Journalism*, 18(2), 2017, 176 ss.

[8] Some scholars have identified a number of sub-dimensions of diversity in order to make this measurement easier to operationalise. The main sub-dimensions are: diversity of entities, topic diversity, viewpoint diversity and structural diversity. For an overview, see: F. Loecherbach - J. Moeller - D. Trilling - W. Atteveldt, *The Unified Framework of Media Diversity: A Systematic Literature Review,* cit.

[9] Centre for Media Pluralism and Media Freedom, *Media Pluralism Monitor 2020,* 2020.

[10] D. Raejimaekers - P. Maeseele, *Media Pluralism and Democracy – What's in a Name*, in *Media, Culture and Society*, 37(7), 2015, 1042 ss.

[11] Scholars have also argued that diversity as received was not sufficiently considered by media law and policy, and called for the integration of research from various disciplines, such as communications sciences, in media policy. See, among others, N. Helberger, *Exposure Diversity as a Policy Goal*, in *Journal of Media Law*, 1(4), 2012, 65 ss. More in general, scholars from different disciplines have noted that diversity of supply, on its own, cannot secure diversity of reception, or diversity of choice for people; see, respectively, D. McQuail, *Media Performance: Mass Communication and the Public Interest*, 1993, 158 ss.; R. Van der Wurft, *Supplying and Viewing Diversity: The Role of Competition and Viewer Choice in Dutch Broadcasting,* in *European Journal of Communication,* 19, 2004, 215 ss.

[12] J. G. Webster, *Diversity of Exposure,* in P. Napoli (ed.), *Media Media Diversity and Localism: Meaning and Metrics,* London, 2007, 309 ss.; P. Napoli, *Exposure Diversity Reconsidered*, in *Journal of Information Policy,* 1, 2011, 246 ss.; K. Karppinen, *Rethinking media pluralism*, New York, 2013; N. Helberger - K. Karppinen - L. D'Acunto, *Exposure diversity as a design principle for recommender systems*, cit.

[13] R. Van der Wurft, *Supplying and Viewing Diversity: The Role of Competition and Viewer Choice in Dutch Broadcasting,* cit.

[14] Since the advent of the Internet, the mismatch between diversity of content available and exposure diversity became ever more serious. Digitalisation, and the related technological developments have led

important element for the achievement of the public goals traditionally attached to diversity of content. However, to measure exposure diversity can be a difficult task: regulators appear to have struggled, in their reports, to spell out how to measure the difference between diversity of content available and diversity of exposure to content. As a consequence, exposure diversity remains substantially under-assessed. An element that certainly does not help is the scarce availability of data, which derives from a substantial asymmetry of information between content distributors and consumers or content creators in the relevant markets.

It is possible to identify a number of endogenous and exogenous factors, which might impact on diversity of exposure. The endogenous refer to the choice that individuals make about what content they want to consume, and, more in general, about how they interact with the content available[15]. The exogenous include various elements that reduce, select, or otherwise modify the availability of content for each individual, such as the existence of intermediaries like social media platforms, their number and the variety of business models they use.

Part II

4. Exposure diversity on social media: the market failures

It is argued that exposure diversity is of utmost importance on social media markets because social media are an important channel for access to and distribution of news and information. Studies have reported an increase in the number of people that access news through Facebook, Twitter and the other major social media platforms. By way of example, Ofcom found that in 2019 about 50% of adults in the UK ac-

to a substantial change in the scenario: from a purely quantitative perspective, currently we have more diversity of information online than ever before. Digitalisation has made the creation and distribution of content substantially easier, cheaper and faster. Therefore, at least in principle, society has at its disposal an increasingly diverse body of content. It is important to note, however, that while content and information do not appear to be subject to scarcity any more, attention is. Each person's capacity to dedicate attention to the information available online is limited; therefore, what counts form an individual perspective is not necessarily the diversity of content available, but the diversity of content each person can easily access or is exposed to. For a discussion of this topic see, among others: T. Wu, *Blind Spot: The Attention Economy and the Law*, in *Antitrust Law Journal*, 3, 2017, 82 ss.; T. B. Ksiazek - S.J. Kim - E.C. Malthouse, *Television News Repertoires, Exposure Diversity and Voting Behavior in the 2016 U.S. Election*, in *Journalism & Mass Communication Quarterly*, 2019, 1 ss.; J. Naughton, *Platform Power and Responsibility in the Attention Economy*, in M. Moore - D. Tambini (eds.), *Digital Dominance: The Power of Google, Amazon, Facebook and Apple*, New York, 2018, 388 ss.

[15] Some have argued that on online markets the growing power of consumers to "filter" what they see due to technological advances leads to a process of personalisation that reduces their exposure to the more or less limited list of topics and perspectives of their own choosing. See, for example, C. R. Sunstein, *Republic.com,* Princeton, 2001. On the same topic, see also: B. Bodó – N. Helberger – S. Eskens – J. Möller, *Interested in Diversity*, in *Digital Journalism*, 7(2), 2019, 206 ss.; F. Borgesius Zuiderveen – D. Trilling – J. Möller – B. Bodó – C.H. de Vreese – N. Helberger, *Should We Worry about Filter Bubbles? An Interdisciplinary Inquiry into Self-Selected and Pre-Selected Personalized Communication,* in *Internet Policy Review,* 5(1), 2016.

cessed news via social media, and the percentage is higher in people aged 16-24[16]. The Australian Competition and Consumer Commission (ACCC) reported that in 2019 the number of users that accessed news websites through referrals from Google and Facebook was broader than the number of users that access those websites directly[17]. Although recent reports signal that the social media use for news consumption has started to fall in a number of key markets after years of steady increase, chiefly because of wider users' lack of trust on this channel, it is possible to conclude that social media remains an important when not yet the major channel for news consumption, especially among younger people[18].

The fundamental role played by these platforms as a vehicle for news and information appeared in all its strength during the Covid-19 pandemic. A number of governments in different areas of the world recurred to these platforms as the main channel for their information campaign about the spread of the virus and the measures to be taken to contrast it and keep population safe. The Reuters Institute 2020 Report on news consumption explains that, in average, 35% of the population used Facebook to find, share and discuss information about the virus, and 30% used YouTube. From their side, Facebook, Twitter and YouTube have been confronted with the complex challenge of tackling disinformation spreading on their platforms[19]. It is reported that the amount of disinformation and misinformation circulating on those platforms saw a steady increase, reaching an extremely wide base of users, sometimes putting their life and that of those nearby at risk[20]. The pandemic has then shed light on an significant dynamic: due to the current role that a handful of social media platforms have on access to and circulation of information, the content curation algorithm they use can have an enormous impact at individual level, on the diversity of exposure of each users and, at the collective level, on the flow of information in society.

In a similar vein, regulators and scholars noted that social media platforms play the role of gateways to news media on the Internet for a large number of citizens, and have increasing influence in shaping users' online news choices[21].

A closer look at social media markets can reveal that the hiatus between diversity of content available on the market and the diversity of content each individual user is exposed to might be larger than in other media markets. A number of reasons can explain this hiatus, some of which seem to verify systemically and therefore can be qualified as market failures.

---

[16] Ofcom, *News Consumption in the UK: Main Findings*, 2019. Similar data result from the Italian regulatory authority AGCOM report of 2018, see: AGCOM, *Rapporto sul consumo di informazione*, 2018.

[17] ACCC, *Digital Platforms Inquiry. Final Report,* 2019.

[18] Reuters Institute for the Study of Journalism, *Digital News Report*, Oxford University Institute, 2019.

[19] Reuters Institute for the Study of Journalism, *Digital News Report*, Oxford University Institute, 2020.

[20] These platforms have changed their policies to include certain disinformation on Covid-19 within the scope of the "harmful" content they remove. Cf, for example: Twitter, COVID-19 misleading information policy, 2020; Facebook, An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19, 2020.

[21] M. Moore - D. Tambini, *Digital Dominance: The Power of Google, Amazon, Facebook and Apple*, cit., 4; ACCC, *Digital Platforms Inquiry. Final Report,* cit.; E. M. Mazzoli - D. Tambini, *Prioritisation Uncovered,* cit.

Social media platforms use content curation algorithms[22] to filter and sort the amount of content available and make personalised selection for users, and they do so based on the information they collect about users by tracking their online activities and behaviours, and by gathering as many data as possible about them[23].

It is argued that content curation algorithms are not neutral towards diversity. Platforms monetise users' attention and have no incentives to expose users to all content potentially available, but only to the tiny portion of it that will keep them more engaged[24]. The platforms therefore design their content curation activities accordingly[25]. In other words, the personalisation of content is not performed looking at criteria such as diversity of content or diversity of sources, but rather having as the end goal the maximisation of users' engagement and thus the maximisation of profit. Therefore, it can be expected that the algorithmic curation optimised for engagement shrinks exposure diversity[26].

By way of example, during the recent ACCC's inquiry on digital platforms, Facebook indicated that its News Feed algorithms are focused on promoting "meaningful social interactions" between users, and it explained that the consequence is that users will see less public content, such as posts from media, and more posts from friends. As

[22] There is a vast literature on algorithmic recommendation systems used for content curation. Traditionally, scholars distinguish between two basic methods to produce recommendations for a user: collaborative filtering (U. Shardanand - P. Maes, *Social information filtering: Algorithms for automating "Word of mouth",* in *Proceedings of the SIGCHI conference on Human factors in computing systems*, Denver, Colorado, United States, ACM Press/Addison-Wesley Publishing Co., 1995, 210 ss.) and content-based filtering (P. W. Foltz - S. T. Dumais, *Personalized information delivery: an analysis of information filtering methods* in *ACM Commun.* 35(12), 1992, 51 ss.). Collaborative filtering is based on users' consumption and behaviour patterns, while content-based filtering produces recommendations based on shared features of the content. The kind of data and metadata needed for each of them is different: the former needs consumption data, the latter needs metadata descriptions of each item. Both systems come with shortcomings, which have led companies to use hybrid systems (F. Cacheda - V. Carneiro - D. Fernández - V. Formoso, *Comparison of collaborative filtering algorithms: Limitations of current techniques and proposals for scalable, high-performance recommender systems,* in *ACM Transactions on the Web*, 5(1), Article 2, 2011; F. Ricci - L. Rokach - B. Shapira (eds.), *Recommender Systems Handbook,* New York - London, 2015). For a discussion of the topic see also: G. Sartor - A. Loreggia, *The impact of algorithms for online content filtering or moderation*, Study requested by the European Parliament's Committee on Citizens' Rights and Constitutional Affairs, September 2020; N. Helberger, *On the Democratic Role of News Recommenders*, in *Digital Journalism*, 2019.

[23] Various scholars and practitioners have defined social media networks providers as "ad-funded" aggregators, who provide "free" services to consumers and monetise through ads or data collection. See, for example, M.L. Stasi, *Social Media Platforms and Content Exposure: How to Restore Users' Control,* in *Competition and Regulation of Network Industries*, 20(1), 2019, 86 ss.; C. Caffarra - F. Etro - O. Latham - F. Scott Morton, *Designing regulation for digital platforms: Why economists need to work on business models,* in *voxeu.org*, 4 June 2020.

[24] Studies demonstrate that the most engaging content is typically what Mark Zuckerberg called "borderline" (M. Zuckerberg, *A Blueprint for Content Governance and Enforcement,* 2018) that is the content which is more sensationalist and provocative, including those stories that appeal to our baser instincts and trigger outrage and fear. See, among many: Z. Tufekci, *The Real Bias Built in at Facebook*, in *New York Times,*19 May 2016; S. Vosoughi - D. Roy - S. Aral, *The Spread of True and False News Online,* in *Science,* 359(6380), 2018, 1146 ss.; The Cairncross Review, *A Sustainable Future for Journalism,* 2019.

[25] Z. Tufecki *The Real Bias Built in at Facebook,* cit.

[26] T. Wu, *Blind Spot: The Attention Economy and the Law,* cit., 4; S. Wolfram, *Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms*, Testimony before U.S. Senate Subcommittee on Communications, Technology, Innovation, and the Internet, 25 June 2019.

for Twitter, the company stated that a user will see tweets from users they follow and "recommended tweets", that is tweets that Twitter believes the user will enjoy based on their platform activity[27]. In both cases, the platforms' automated systems for content curation can decrease exposure diversity of users, because they prioritise certain categories of content only, and demote or exclude others based on criteria other than diversity, and which can conflict with it.

Various scholars have recognised, at theoretical level, the impact that platforms' algorithmic recommendation systems might have on exposure diversity[28]. They have also noted that these systems approach diversity differently from media policy: it is not a normative value aimed to societal enlightening, but rather a question of providing a stimulating variety for the user to stay more on the platform and to consumer more[29]. Thus, it is typically the diversity within a set of recommendations selected for each user, not the diversity of the entire pool of content available. While these systems are presented as tailoring to the interests and preferences of users, the data-driven inferences, which are the main part of the business model, can have as trade-off the silencing of individual and collective voices alike. In fact, because recommendation systems seem to be, in principle, set to predominantly deliver information that aligns

[27] ACCC, *Digital Platforms Inquiry*, Final Report, cit.

[28] It has to be noted, however, that empirical research on how platforms' algorithmic recommendations systems impact exposure diversity is yet limited due to the limited availability of data, which platforms refuse to share with academics, regulators or civil society alike. Nevertheless, a number of studies have argued that diversity of exposure online has increased in the past years, not the contrary. For example, in a comparative study based on surveys data from four countries, Fletcher and Nielsen have reached the conclusion that even if one looks at social media only, people are incidentally receiving news which are more diverse in sources (R. Fletcher - R. K. Nielsen, *Are People Incidentally exposed to News on Social Media? A Comparative Analysis*, in *New Media Soc.,* 20, 2018, 2450 ss. Like many survey studies, it can be argued that the study naturally suffers from limited accuracy and reliability (M. Scharkow, *The Accuracy of Self-Reported Internet Use – A Validation Study Using Client Log Data,* in *Commun. Methods Meas,* 10, 2016, 13 ss.). Self-reporting measures have been recently criticised for being biased toward active news choices and routine use (H. Taneja - A. X. Wu - S. Edjerly, *Rethinking the Generational Gap in Online News: An Infrastructural Perspective,* in *New Media Soc.,* 20, 2018, 1792 ss.) as well as for being particularly inaccurate when people access news via intermediaries (cA. Kalogeropolous - R. Fletcher - R. K. Nielsen, *News Brand Attribution in Distributed Environments: Do People Know Where They Get Their News?,* in *News Media Soc.*, 21, 2019, 583 ss.). To avoid these biases and inaccuracies, Scharkow et al. have looked at large tracking datasets of individual-level browsing behaviour in Germany, collected independently in 2012 and 2018, and applied a random-effects within-between model (REWB) to identify the effects on social media and other intermediaries to news exposure. They argue that incidental news exposure, that is the news exposure users get without looking for it but simply as part of their connection to the platform, is higher for those users that access social media sites more often on a given day. However, their research seems to focus on the quantity of news exposure, rather than on the diversity of it (M. Scharkow - F. Mangold - C. Stierc - J. Breuerc, *How Social Network Sites and Other Online Intermediaries Increase Exposure to News,* in *PNAS* 117 (6), 2020, 2761 ss.). In any case, this paper argues that to assess if there is a marker failure in terms of exposure diversity on social media, the counterfactual is not the market situation of ten or five years ago, as referred to by many scholars, but a present hypothetical market where content is curated in a neutral way, or where a sufficient number of alternatives for content curation are concretely available to users and there is transparency and sufficient information about how the curation is performed. If the market failure consists in the artificial and intentional limits that social media platforms put on exposure diversity today, the counterfactual should be the exposure diversity in a market where that market failure is solved, or internalised by those who cause it.

[29] For a discussion on how to combine these two types of diversity and create an algorithmic diversity diet, see J. K. Sørensen - J. H. Schmidt, *An algorithmic diversity diet? Questioning assumptions behind a diversity recommendation system for PSM*, Working paper, Hans-Bredow-Institute for Media Research, 2016.

with people's current interests and preferences, they might lead to homogeneity and lower users' chances to encounter different content, opinions and viewpoints. It has been argued that this might lead users into "filter bubbles" or "echo chambers"[30], which are segregated and homogeneous spheres of information and debate that in the long-term erode the idea of the public sphere and its function of providing people with diverse perspectives and opinions on matters of collective relevance, which is considered to be crucial to the functioning democracy[31]. It is noted, however, that the empirical research about the likely effects of content curation on exposure diversity remains limited due to the scarce availability of data[32].

Another way social media platforms' content curation impacts exposure diversity can be observed by looking at the relationship between these platforms and media outlets. A significant proportion of the latter's referral traffic comes from social media; therefore, media outlets consider those platforms an unavoidable trading partners to reach certain audiences[33]. Here again, platforms can be seen as gatekeepers, and media outlets might be forced to consider, and adjust to, the way these platforms personalise content, or their content will not get through and it will not be seen by users. As a consequence, social media platforms' algorithms have substantially changed media outlets and journalists' incentives towards the production of certain type of content. If media businesses want to monetise their content and maximise referral traffic to their websites, they should opt for the production of content that satisfies the demands of the platforms' content curation systems, rather than producing content that is in line with their editorial choices, diverse and in the public interest[34]. Once again, diversity appears to give way to other criteria.

The above suggests that the content curation algorithms used by social media platforms create externalities in terms of exposure diversity, which the platforms do not seem to acknowledge and to internalise. Such externalities constitute a market failure that is problematic at individual level, because it limits users' freedom of information, and at societal level, because as mentioned, exposure diversity is a normative value instrumental to a democratic system.

The preliminary conclusion is therefore that content curation systems used by social media platforms can interfere with the content users are exposed to, lowering its diversity. In this scenario, social media markets can frustrate the idea of the Internet as a manifestation of users' freedom of choice, control and sovereignty[35]: indeed, this

[30] C. R. Sunstein, *Republic.com,* cit.; E. Pariser, *The Filter Bubble: What the Internet Is Hiding From You*, London, 2011.

[31] J. G. Webster, *Diversity of Exposure,* cit.; J. K. Sørensen - J. H. Schmidt, *An algorithmic diversity diet?* cit.; J. Harambam - N. Helberger - J. van Hoboken, *Democratizing Algorithmic News Recommenders: How to Materialize Voice in a Technologically Saturated Media Ecosystem,* in *Philosophical Transaction of the Royal Society A*, 376(2133), 2018.

[32] N. Helberger - J. Moeller - S. Vrijenhoek, *Diversity by Design,* paper prepared for the Department of Canadian Heritage and the Canadian Commission for UNESCO, 2020.

[33] Reuters Institute, *Digital News Report,* 2019, cit.

[34] ACCC, *Digital Platforms Inquiry*, cit.

[35] A. L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, New York, 2000.

idea does not hold if personalised recommendations and exposure aim to nudge users and direct their attention to selected content only[36].

Exposure diversity on social media might be also impacted by other additional factors. One is a diffuse content availability asymmetry: the pool of content where content curation algorithms draw might not be a neutral representation of public opinion, but rather tend to be biased towards the interest of the most active contributors. In addition, there appears to be relatively weak incentives to share content displaying scientific or societal consensus. Finally, users' behaviours might also, to a certain extent, play a role: likes, shares, retweets, clicks and similar actions can create popularity or trigger the virality of some content[37]. This can be the result of genuine behaviours, but also of inauthentic behaviours: sometimes sophisticated users can put in place mechanisms to alter the automated curation systems set by platforms in order to introduce intentional distortions[38].

Another factor that might have an impact on exposure diversity is the substantial lack of transparency in the market. Individuals have limited or no knowledge about how the content they are exposed to is curated by algorithms and according to which criteria; therefore, they are not sufficiently aware of the hiatus between the diversity of content available online and the diversity of content they are exposed to. In other words, users are not aware that choices that limit their diversity of exposure have been made for them; on the contrary, they might consider the newsfeed as neutral, reflecting the existing diversity and abundance of viewpoints. This lack of awareness impacts on their autonomy, and on their capacity to make choices to remedy the reduced exposure. Scholars have noted that the lack of autonomy and independence of users' decision-making is a key element of market failures deriving from gatekeeping positions[39].

The European Commission, in its recent proposal for a Digital Services Act (DSA), seems determined to tackle this problem in two main ways: by imposing transparency obligations on all players, and by requiring very large online platforms to provide users with the possibility «to select and modify at any time their preferred option for each of the recommender systems that determines the relative order of information presented to them»[40].

What has been described so far refers mainly to the content users are passively exposed to. Users remain free, at least in theory, to actively look for more diverse and plural

[36] E. Pariser, *The Filter Bubble,* cit.; C.R. Sunstein, *The Ethics of Nudging,* in *Yale Journal of Regulation*, 32, 2015, 413 ss.

[37] K. Thorson - C. Wells, *Curated Flows: A Framework for Mapping Media Exposure in the Digital Age*, in *Communication Theory,* 26(3), 2015, 309 ss.

[38] The phenomenon of inauthentic behaviours is not marginal. The big platforms dedicate increasing attention to it. For example, Facebook has started to publish regular reports on the topic, see: Facebook, *February 2021 Coordinated Inauthentic Behaviour Report*, 3 March 2021. The European Commission too is dedicating attention to the phenomenon within its strategy against disinformation; see, recently: European Commission, *Guidance on Strengthening the Code of Practice on Disinformation*, COM(2021) 262 final, 26 May 2021.

[39] R. Podszun, *Digital Ecosystems, Decision-Makings, Competition and Consumers – On the Value of Autonomy for Competition,* in *ssrn.com*, 2019; E. Fish - M. Gal, *Echo Chambers and Competition Law: Should Algorithmic Choices Be Respected?,* in *Competition Policy International*, 2020.

[40] European Commission, Digital Services Act, cit., Article 29(2).

content, either by changing the default settings on the platform or outside the platform. In practice, though, they rarely do so. Behavioural studies have documented that users do not always choose the best course of action, and are generally reluctant to act outside of the status-quo[41]. Furthermore, platforms are able to exploit these users' bias through specific designs that promote addictive behaviours[42] such as default settings, dark patterns and similar forms of nudging, which users very rarely react to[43]. In other words, users will rarely, if ever, change the default settings on their profile on Facebook or Twitter, despite the fact that doing so could free them from the platforms' massive interference with the content they see, and could allow them to access more diverse information. This is so for two main reasons. On the one hand, because of the mentioned extreme asymmetry of information and lack of transparency in the social media markets. On the other hand, to change default settings has a meaningful cost for users, at least in terms of time, which discourages it.

The challenges described above are exacerbated by the high concentration in social media markets[44], which are dominated by a few companies only; therefore, what is distributed by or shared on these few companies is visible to a vast public, while what is not distributed by or shared on these few companies might not be visible to the majority of individuals. Moreover, social media markets present high barriers to entry and they do not appear easily contestable[45]. Therefore, dominant players are able to adopt business models and practices which are not driven by demand and to lower the quality of the service offered to users without suffering any competitive pressure. Users do not appear to have at disposal viable alternatives and platforms have various ways to keep switching costs artificially high[46]. As a result, large social media companies can play a bottleneck role in the distribution of content, and affect users' diversity of exposure. In addition, because of their size and market power, social media platforms might represent a sort of unavoidable trading partners for media outlets, which, as argued, are impacted by the platforms' content curation systems with little negotiating

[41] ForbrukerRadet, *Deceived By Design. How Tech Companies Use Dark Patterns to Discourage Us From Exercising Our Right to Privacy*, 2018; Behavioural Insight Team, *The Behavioural Science of Online Harm and Manipulation, and What To Do About It*, 2019.

[42] Ofcom, *Online Market Failure and Harms. An Economic Perspective on the Challenges and Opportunities in Regulating Online Services*, 2019.

[43] Scholars and regulators have highlighted the challenges related to defaults, dark patterns and nudging. For an overview of the topic, see among others, O. Bar-Gill - O. Ben-Shahar, *Rethinking Nudge: An Information-Costs Theory of Default Rules*, in *University of Chicago Law Review*, 88, 2021, 531 ss.; Competition and Markets Authority, *Online Platforms and Digital Advertising*, Market Study Final Report, 1 July 2020; ACCC, *Digital Platforms Inquiry*, cit.

[44] P. L. Parcu, *New Digital Threats to Media Pluralism in the Information Age,* in *RSCAS/CMPF Working Paper,* RSCA 2019/9, 2019.

[45] The European Commission has explicitly recognised this problem and its recent regulatory proposal for a Digital Markets Act is supposed to solve it (see: European Commission, Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 Final, 2020/0374 COD).

[46] A number of distinguished studies describe the existence of these challenges in digital markets; see, for example: Ofcom, *Market Failure and Harm*, cit.; J. Cremer - Y. A. de Montjoye - H. Schweitzer, *Competition Policy for the Digital Era,* 2019; Sitlger Committee on Digital Platforms, Final Report, 2019; Competition and Markets Authority, *Online Platforms and Digital Advertising*, cit.

power. Therefore, size and market power seem to play a role in the under-exposure of users to diversity.

To conclude, this section has discussed the under-exposure to diversity on social media markets and its causes. The way social media markets work means that exposure diversity is low as a result of a number of factors, which this section has tried to list. The main appears to be the algorithmic systems of content curation used by social media platforms. Other factors that contribute to this reduction are the high market concentration and the bottleneck role that could be played by large players in the distribution of content, the asymmetry of information between platforms and users, and the absence of viable alternatives for the latter.

The key role that platforms' automated content curation systems play for exposure diversity has been acknowledged by decision makers and regulators. The Council of Europe has recommended to member States to «improve the transparency of the processes of online distribution of media content, including automated processes: - assess the impact of such processes on users' effective exposure to a broad diversity of media content; - seek to improve these distribution processes in order to enhance users' effective exposure to the broadest possible diversity of media content»[47]. In a similar vein, regulators have called for appropriate and consistent regulation of platforms' functions of selecting and curating content, evaluating content based on specific criteria, and ranking and arranging content for display to users[48]. The European Commission, in its recent proposal for a Digital Services Act (DSA), has suggested that very large online platforms perform a risk assessment with regard to their content curation systems, and that they amend the latter in a way that does not have negative effects for the exercise of freedom of expression and information by users, which exposure diversity is part of[49].

The next section of this paper looks at the decision makers and enforcers' perspective and discusses two possible ways to solve the reduction of exposure diversity with regulation.

Part III

5. Two proposals

There are arguably various ways regulators could intervene to fix the problem at stake. *Ex ante* remedies appear to be the best fit because of the various characteristics of social media markets. First, they are fast moving markets, where developments in technology and business models occur rapidly, definitely more rapidly than in traditional *ex post* enforcement. Second, social media markets' dynamics are as such that economies of scale and scope, once achieved, raise barriers to entry and make it difficult to

[47] Council of Europe, Recommendation CM/Rec(2018)1, cit.

[48] ACCC, *Digital Platforms Inquiry,* cit.

[49] European Commission, Digital Services Act, cit., Article 26. For a definition of "very large online platform" see Article 25.

reverse the situation and to make markets competitive and contestable again. Indeed, the difficulties in tackling consolidated positions of (abusive) dominance fuel extreme calls to "break up" the giants[50]. *Ex ante* regulation could be useful in case of markets that have already tipped, because it can lower barriers to entry and make markets contestable again.

In addition, *ex ante* remedies present a number of advantages: they can be tailored to specific situations, they can be behavioural or structural in nature, and are potentially an open-ended list. Finally, the procedure to impose *ex ante* remedies could be less formal than an *ex post* infringement procedure, and, depending on circumstances, it could imply a certain degree of negotiation, or at least confrontation, between the enforcer and the target.

In the case at hand, where we are confronted with a harm strictly linked to a market failure that is at least reinforced by the substantial market concentration and high barriers to entry, regulators could decide to use asymmetric regulation to fix the problem. Asymmetric regulation would involve imposing specific obligations on players which possess a significant degree of market power. Scholars and regulators have put forward various proposals about how to identify these players[51]. Indeed, numerous regulatory proposals currently discussed in different areas of the world focus on platforms with market power, therefore there is consensus on the need for asymmetric regulation.

This paper identifies and discusses two main *ex ante* regulatory solutions: (i) the imposition of a certain level of regulated diversity; (ii) the imposition of unbundling between hosting and content curation activities, in order to open the market to competitors and reinstall competitive dynamics. The first solution regulates content curation in a way that guarantees diversity. As previously explained, the under exposure in social media markets is not linked to a decrease in the availability of content, but rather to, first among others, the way the content is distributed: social media platforms distribute content to their users via content curation activities, which have the potential to decrease diversity. Seen from the user's perspective, the decrease does not concern the content they actively access, but rather the content they are passively exposed to on a daily basis. As the market failure concerns distribution, a possible solution is to impose some form of "must view" obligation on the platforms to expose individual users to some degree of content diversity.

The second solution is to separate hosting activities from content curation activities and to oblige large platforms to allow third parties to offer content curation to the platforms' users. For example, a user that creates or has a profile on Facebook should be asked by the platform whether she wants the content curation service to be provided by Facebook itself, or by other players to be freely selected. The option to stay with

[50] See among many: A. W. Herndon, *Elizabeth Warren Proposes Breaking Up Tech Giants Like Amazon and Facebook*, in *The New York Times,* New York, 8 March 2019; Editorial, *Tech giants face new threats from the government and regulators*, in *The Economist,* San Francisco and Dallas, 14 March 2019.

[51] See, among others: E. Noam, *Online Video: Content Models, Emerging Market Structure, and Regulatory Policy Solutions,* in *TPRC47: The 47th Research Conference on Communication, Information and Internet Policy,* 2019; Digital Competition Expert Panel, Unlocking Digital Competition, 2019; Autorité de la Concurrence, *Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques,* 19 February 2020; Competition and Markets Authority, *Online Platforms and Digital Advertising*, cit.

the large platform should be presented as opt-in, rather than opt-out. Such a measure would help defend against users' unwillingness to change from the status-quo and would avoid that platforms undermine the effects of the unbundling by making the switching hard for users and by nudging them towards a locked-in situation.

Both proposals are for asymmetric regulation, based on various reasons. First, the market failure they are supposed to fix is an externality of large platforms' business models and content curation algorithms. Because of their power, these platforms account for the vast majority of the market; therefore, to address the market failure it could be sufficient to address these players. Second, additional regulatory burdens will likely weigh more on small platforms, which might not have adequate resources and tools for compliance, than on big platforms, and further strengthen the latter competitive advantage, which, as mentioned, is a factor that reinforces the market failure. Third, asymmetric regulation would be a less invasive regulatory intervention than a sector-wide regulation. These benefits would likely overtake potential trade-off of asymmetric regulation in terms of difficulties for monitoring and enforcement.

The follow-up question is to identify which platforms are large enough to warrant regulation. Regulators should set thresholds that reflect the gatekeeping capacity of platforms, and their disproportionate power towards users, rather than look at their turnover or financial capacity. Among others, regulators could consider parameters such as the number of users, the time spent on the platform or the number of interactions on the platform, to assess the size; the low ability and incentive to multi-homing for users or the economic dependency of business users to assess the gatekeeping role; and the existence of barriers to entry on existing and future services to assess if the gatekeeping position is likely to endure[52].

A further step is to decide on what type of platforms the remedies should be applied. Social media platforms can be broadly divided into two categories: "generalists" and "specialised" ones. The European Commission, in its decision about the Microsoft/LinkedIn merger, explained that general social network services are used to build social relations among people who share similar personal and career interests, activities, backgrounds or real-life connections. A sub-set of social network services are focused on professional contacts and are therefore typically referred to as "professional social network" services, and should be considered a different market; the Commission considered LinkedIn an example of the latter[53]. Although this distinction has been made based on merger rules about market definition and market power, it might be possible to borrow these definitions and make use of them in a different regulatory context. For our purposes, the suggestion to apply diversity obligations on generalists social

[52] P. Alexiadis - A. de Streel, *Designing an EU Intervention Standard for Digital Gatekeepers*, in *EUI Working Paper Series,* RSCAS 2020/14, 2020. In its recent proposal for a Digital Services Act, the European Commission has opted for the imposition of asymmetric obligations on "very large platforms", defined based on the average monthly users in the EU. A more complex assessment is foreseen in the second proposal recently issued by the Commission, the Digital Markets Act (DMA). The latter defines "gatekeepers" based on the combination of three quantitative parameters: annual turnover, average market capitalisation, and average monthly users for at least three financial years. However, the DMA also provides the possibility, for the Commission to define a gatekeeper based on a case-by-case qualitative assessment, if needed (see European Commission, Digital Markets Act, cit., Article 3).

[53] European Commission, *Microsoft v LinkedIn*, Case M.8124 [2016].

media, such as Facebook, Twitter and TikTok appears more proportionate to the objective of media diversity, because generalist platforms are the ones that can potentially transmit more diverse types of content and information.
In the following section, an analytical framework is suggested to compare the merits of both proposals based on a number of benchmarks.

6. An analytical framework to assess them

In this section, the regulated diversity and the unbundled access to content curation are assessed against a number of benchmarks, which could be useful to measure their effectiveness, strengths and weakness both from a substantive and from an enforcement point of view. The seven suggested benchmarks have been chosen to help regulators answering two key questions: what are the aims that they want to achieve; and how to do so, dealing with the related challenges.

6.1. Normative approach

The regulated diversity falls within the traditional State's approach to media diversity as a public objective that deserves protection[54]. While shaping this remedy, regulators should carefully define diversity of content and viewpoints and establish how much diversity is enough diversity: in other words, which and how many viewpoints need to reach the individual user for the latter to be exposed to a sufficient degree of diversity[55].
The remedy at stake reflects a paternalistic approach to exposure diversity and it could be grounded on a participatory theory of democracy[56]. Under this conception, individuals' freedom and autonomy are not values *per se*, but as they are instrumental to furthering the common good. Citizens, therefore, cannot afford to be uninterested in politics because they have an active role to play in society[57]. Imposing citizens a certain degree of exposure diversity is substantially in line with this vision, as it helps citizens

[54] This approach is based on the recognition that States have the sovereign right to formulate, adopt and implement policies and measures for the protection of diversity of cultural expression (see W. King - A. Shramme, *Cultural Governance in a Global Context: An International Perspective on Art Organisations,* London, 2019; A. Vlassis, *Diversity of Content in the Digital Age – Towards Guiding Principles*, paper prepared for the Department of Canadian Heritage and the Canadian Commission for UNESCO, 2020). Along those lines, the EU Audiovisual Media Service Directive, at Recital 25, affirms that Member States may «[…] impose obligations to ensure the appropriate prominence of content of general interest under defined general interest objectives such as media pluralism, freedom of speech and cultural diversity» (see Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L 303, 69–92).

[55] The Cairncross Review, *A Sustainable Future for Journalism,* cit.

[56] D. Held, *Models of Democracy,* Redwood City, 2006.

[57] J. Strömbäck, *In search of a standard: Four models of democracy and their normative implications for journalism,* in *Journalism Studies*, 6(3), 2005, 331 ss.

to play their role.
Nevertheless, some scholars remain sceptical about the opportunity to regulate exposure diversity and impose on people the consumption of certain media, even if "valuable" ones, because it conflicts with individuals' freedom of expression and personal autonomy[58]. Indeed, the European Convention on Human Rights protects the right of individuals to «hold opinions and to receive and impart information and ideas without interference by public authority»[59]. Therefore, any public-authority driven prescription about how much diversity of content people ought to see or consume risks crossing the line between legitimate media policy objectives and normative censorship, or the structuring of thought and societal choices by consciously manipulating or inducing biases in computational decisions. Moreover, if not well designed and enforced, the regulated exposure diversity can raise issues of transparency, ethics, security, loyalty and above all neutrality of the Internet. For this regulatory tool to be legitimate, the intent or purpose of the authorities venturing into it need to be clear and transparent, and the intervention needs to be proportionate and necessary.
On the other hand, the unbundled access to content curation lands in the economic regulation approach. Rather than imposing a minimum degree of diversity of exposure in the market, this remedy relies on competition to increase variety of content curation systems and therefore diversity of outcomes, and leaves users free to select what they prefer. The unbundling, triggering decentralisation and opening the doors to more players, could help dilute the power of current gatekeepers and build the counter powers we need to prevent a few social media platforms from becoming quasi-governments of online speech, while also ensuring that they each remain one of many content curation providers that allow people to engage in public debate[60]. Therefore, this regulatory approach is less invasive and more in line with a liberal democratic theory, where personal development and autonomy of citizens remains central and is respected by the State, who does not intervene but with a minimal nudging[61].

6.2. Impact on users' empowerment

As recalled various times by the European Commission Executive Vice-President Vestager, users' empowerment is a fundamental pillar of the European way, where is technology that serves people and not the other way around[62]. This benchmark is

[58] P. Valcke, *Digitale Diversitcit. Convergentie van Media – Telecomm en Mededingingsrecht,* Brussels, 2004; P. Napoli, *Media Diversity and Localism. Meaning and Metrics,* London, 2006.

[59] European Convention on Human Rights [1953], Article 10.

[60] D. Kaye, *A New Constitution for Content Moderation,* in *OneZero.medium.com,* 26 June 2019; N. Helberger, *The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power,* in *Digital Journalism*, 2020; F. Fukuyama - B. Richman - A. Goel, *How to Save Democracy from Technology. Ending Big Tech's Information Monopoly*, in *Foreign Affairs*, January/February 2021.

[61] M. M Ferree - W. A. Gamson - J. Gerhards – D. Rucht, *Four Models of the Public Sphere in Modern Democracies,* in *Theory and Society,* 31, 2002, 289 ss.; J. Strömback, *In search of a standard,* cit.

[62] See among others: M. Vestager, *When Technology Serves People*, 1 June 2018; Ead., *Internets of the World Conference*, 5 December 2019.

strictly interlinked with the normative approach benchmark. Indeed, the users' empowerment potential of each remedy is inversely related with the level of paternalism toward users that each remedy implies.

The imposition of regulated diversity has a limited impact in terms of users' empowerment: it does not widen users' choices, but considers them passive targets of a certain policy outcome. However, depending on how the remedy is designed and on whether it is accompanied by further transparency obligations, it can raise users' awareness on how content curation algorithms work and on why they see the content they see on their feeds, pages etc. It remains true, though, that knowledge without the possibility to change or chose alternatives remains a blunt weapon. Regulators could partly obviate this problem by including rules on defaults that provide users with a certain degree of autonomy in setting their own preferences about the content they want to be exposed to. As mentioned, this path has been followed by the European Commission in its Digital Services Act proposal.

The scenario looks different in the case of unbundled access to content curation. The greater availability of choices could increase the bargaining power of users in relation to platforms, and could enable users to discipline, to a certain extent, the quality and diversity of the content offered to them by switching to another supplier of content curation if they are not satisfied by the one they are currently using. The availability of choices could also allow the fragmentation of users into groups with different preferences. In other words, in the medium and long term unbundling could strongly empower users.

To conclude, when assessing the two proposals regulators should consider that the unbundling appears to have a stronger impact on users' empowerment, which remains a policy and regulatory priority in the framework of the EU Digital Single Market.

6.3. Sustainability and impact on competition and innovation

Another fundamental step in deciding which remedy to adopt is to look at the impact it has on the market at present, as well as in the years to come. Regulators should look at the goal they want to achieve in the short as well as in the medium and long term. In particular, the remedy's sustainability in the long run and its impact on competitive dynamics and innovation on the market are significant elements to consider when making the choice.

Imposing platforms to include the parameter of diversity in the design of their content curation systems (diversity by design) could create commercial constraints for the platforms, because they will not be free to optimise their algorithms for profit purposes only. The impact of this economic disincentive should be carefully evaluated, in order to avoid quality degradation or decrease of innovation in the medium and long term. In addition, regulated diversity might do little to overtake the structural market problems identified in the previous part of this paper: it does not lower barriers to entry nor it imposes any new competitive constraint on platforms, which could make them

more incline to change their content curation systems.
On the contrary, the form of unbundling suggested here appears to be capable of addressing not only the reduction of exposure diversity on social media, but also the market failure that originates this reduction. Unbundling could open the content curation market to competitors, thus making it contestable again. In the medium and long term, the competitive pressure could stimulate all companies to innovate and offer better quality services, to the benefit of consumers. If competition is reinstalled in the market, diversity of exposure could be ensured in a sustainable way both in the short term as well as in the long-term. A healthy competitive market could deliver better quality services *per se*, without the need for further regulation.
Nonetheless, unbundling could present some shortfalls too. As previously mentioned, the way content is currently shaped on social media platforms is led by the advertising-driven business model adopted by these platforms. If the alternative operators use the same business model, the problem of the reduction in the diversity of exposure might not be solved in the medium and long term. Therefore, the key question becomes how economically sustainable other business models may be, whether there are sufficient incentives to stimulate their adoption, or whether the States or regulators might have to provide these incentives.
Overall, based on the above, regulated diversity might limit platforms' monetisation mechanisms, reduce their incentive to innovation and might not help to solve the lack of sufficient competition in the market. On the other hand, the unbundled access solution could expose large platforms to more competition making markets contestable again, and could thus be expected to create incentives for innovation.

6.4. Complementary measures

This benchmark considers whether each remedy is sufficient to achieve the set goal and/or if a number of complementary measures might be needed for this purpose, as well as to avoid possible medium and long term trade-offs.
If regulated diversity is chosen, a complementary measure should be to increase transparency between social media platforms and their users, in order to diminish information asymmetry and to allow users to make more informed and conscious choices. This can be done through the imposition of detailed transparency obligations on platforms. Various regulators have already moved in this direction, such as, for example, the German broadcasting authority and, more recently, the European Commission[63].

[63] The recent initiative of the German broadcasting authority (the Medienstaatsvertrag or MstV) addresses media platforms and streaming services, but also "media intermediaries", which are defined as «any tele-media that aggregates, selects, and presents third-party journalistic/editorial offers, without presenting them as a complete offer». While definitions still need to be clarified, the draft MStV includes a list of digital offers ranging from search engines to social networks and news aggregators. Under the transparency provisions, media intermediaries will be required to provide information about how their algorithms operate, including the criteria that determine: (i) how content is accessed and found, and (ii) how content is aggregated, selected, presented and weighed. Indeed, transparency rules address information asymmetries for users by increasing their awareness on how what they see is selected and curated. The shortfalls for our purposes remain that MstV rules do not provide users with the possibility

In case of unbundled access to content curation one of the possible short-falls concerns the sustainability of alternative business models for content curators, which depends, to a large extent, on users' willingness to pay, which in turn depends on how much users value diversity of exposure. States could stimulate this willingness to pay through media policies that increase digital literacy. Among others, States could promote actions to increase users' awareness of the key role played by media diversity in determining their capacity to make informed decisions and engage in public life; or they could enforce policies that reduce the information asymmetries in social media markets, for example, by mandating or encouraging more transparency around platforms' business models and the use of algorithms in content curation[64]. These transparency measures could also reduce the competitive advantage large platforms have with regards to smaller competitors.

Another way to promote alternative business models, as well as to promote algorithms that implement diversity metrics, could be by providing support via public funding for a temporary period. In this scenario, while the costs society would have to bear may be justified by the importance of the public objective to be achieved, in the long term this solution may not be sustainable.

Finally, alternative business models could be indirectly supported by an increase in users' empowerment; regulators could encourage practices that go in this direction, and more specifically towards users' playability, that is their capacity to interact with the algorithm and to choose their preferred settings[65]; in other words, people should be given a voice, that is the possibility to exert a certain degree of control over the algorithms that curate the content they see[66]. A way to do so is to mandate platforms not to use default settings, and rather let users make their choices and to easily change them at any time. The European Commission's proposal for a Digital Services Act seems to go in this direction when it establishes that very large online platforms «shall provide easily accessible functionality on their online interface allowing the recipient of the service to select and modify at any time their preferred option for each of the recommender systems that determines the relative order of information presented to them»[67].

to choose the criteria according to which the ranking or sorting it performed. Awareness about status quo without the possibility to choose alternatives is a blunt weapon. The European Commission's proposal for a DSA also chooses the way of transparency, with a first layer of obligations imposed on all players and additional ones imposed on very large platforms. See European Commission, Digital Services Act, cit.

[64] Here again, default settings have a role to play. Regulators could call platforms and alternative players to guarantee, by default, a specific degree of transparency about the services they provide, and in particular about how their algorithm works. Germany is experimenting a similar approach: the German Network Enforcement Act (NetzDG) imposes transparency rules that some platforms have implemented in their default settings. However, the NetzDG does not expressly target defaults, and this is why some players, like for example Facebook, have been able to maintain their defaults, adding an alternative possibility for users which complies with the NeztDG, but which remain far less utilized by users.

[65] D. Tchehouali, *Analysis of Potential Measures to Support Access and Discoverability of Local and National Content*, paper prepared for the Department of Canadian Heritage and the Canadian Commission for UNESCO, 2020.

[66] J. Harambam - N. Helberger - J. van Hoboken, *Democratizing Algorithmic News Recommenders,* cit.

[67] European Commission, Digital Services Act, cit., Article 29(2).

Apart from State intervention, the shortfalls of unbundling could be addressed by multi-stakeholders forms of self-regulation. In other words, if and to the extent that competitive process would not be able to deliver sufficient quality in the medium and long term, and in order to avoid a race to the bottom with regards to alternative business models to be adopted by third-parties, multi-stakeholders' initiatives as the social media councils mentioned above could be supported to define additional diversity standards to be applied by all players in the market.

In conclusion, both regulatory solutions might need complementary measures to be implemented. For regulated diversity these measures are limited to more transparency in the market. However, as the unbundling could have a stronger impact on market dynamics, it seem to require more complementary measures to deal with the new market setting, and to nudge towards alternative business models and support their sustainability.

6.5. Design/Implementation

This benchmark looks at how each measure might be designed and implemented in practice, and which weakness and strengths it implies.

Regulated diversity has to be implemented by algorithmic recommendation systems. This solution therefore implies the imposition of a sort of diversity by design. Diversity of exposure is a value, and translating a public value into a design requirement is not a simple process. Scholars have identified three main steps in this process: the conceptualisation of the value; the translation of it into one or more norms or metrics; the translation of those norms or metrics into more specific design requirements[68]. Technical developers might encounter difficulties in translating a normative value into concrete criteria that the system they develop has to possess and to implement. Therefore, to effectively achieve the objective, the technical and the editorial departments of social media platforms should work together[69].

Moreover, attention is needed to operationalise exposure diversity while avoiding arbitrary intervention by the State. To this aim, regulators could promote and rely on multi-stakeholder solutions. This approach has been suggested by the Council of Europe, who recently called on States to encourage social media, media, search and recommendation engines and other intermediaries which use algorithms, along with media actors, regulatory authorities, civil society, academia and other relevant stakeholders to engage in open, independent, transparent and participatory initiatives aimed at improving distribution processes in order to enhance users' effective exposure to the broadest possible diversity of media content, among other aims[70]. The multi-stakeholder approach is supported by various actors. For example, some civil society groups have suggested the creation of "Social Media Councils", a multi-stakeholder accountability mechanism

[68] I. Van der Poel, *Translating values into design requirements,* in D. Mitchfelder, N. McCarty, D. E. Goldberg (eds), *Philosophy and Engineering: Reflections on Practice, Principles and Process*, Springer, 2013.

[69] N. Helberger - J. Moeller - S. Vrijenhoek, *Diversity by Design,* cit.

[70] Council of Europe, Recommendation CM/Rec(2018)1, cit.

for content moderation on social media. The Councils aim to provide an open, transparent, accountable and participatory forum to address content moderation issues on social media platforms on the basis of international standards on human rights and could help to establish best practices with regard to exposure diversity[71].

Furthermore, diversity by design should look not only at the algorithm, but also at the broader societal context where the latter is implemented[72]. In fact, diversity of exposure will always depend on the diversity of content available in a certain context and therefore it is a moving target, not a fixed measure. For example, the variety of content in a region of a EU state that chiefly speaks a language different from the national one might not be comparable with the variety of content available at national level. When the diversity of content increases in a certain context, the increase should be reflected in the diversity of exposure too.

Regulators could approach the operationalisation of diversity in the platforms' algorithmic recommendation systems in various ways. The first, less intrusive, is to impose to the platform an obligation with regard to the outcome, and let it free to decide how to implement it. The second is to intervene in the operationalisation process and to dictate (some of) the criteria through which the algorithm should perform content curation. The second option raises the question of which safeguards should be put in place to avoid arbitrary intervention, which could result in censorship or propaganda. Some have noted that similar problems could emerge, for example, in the approach taken in the EU Code of Practice on Disinformation[73], which asks platforms to prioritize "trustworthy" content[74].

A number of governments and public actors seem oriented towards the first option, and towards asking platforms to make their algorithms accommodating public interest considerations; however, it remains unclear which considerations they refer to, how platforms are supposed to operationalise this call and how regulators can monitor and evaluate platforms' efforts. To find an efficient answer to these questions, co-regulation might be a better fit than regulation. A co-regulatory response, in fact, could gain from the information companies have but regulators lack about how the algorithms work, and how to shape their design to achieve the needed results. A co-regulatory response might also make enforcement easier.

On the other hand, the unbundled access to content moderation would need to be deployed and enforced at two layers: (i) contractual terms and commercial behaviour and (ii) technical standards and protocols. The unbundling could be reflected in the contractual relationship between the large platform and the content curation providers, which could contain, at least, the obligations: not to bundle the two services; not to impose restrictions on the users' ability to use alternative players for the provision of content curation activities; to provide access to alternative players on fair, reasonable

71 ARTICLE 19, Social Media Councils: Consultation Paper, 2019.

72 B. Friedman - D. G. Hendry - A. Borning, *A Survey of Value Sensitive Design Methods*, in *Human–Computer Interaction,* 11(2), 2017, 63 ss.

73 EU Code of Practice on Disinformation, 2018.

74 N. Helberger - P. Leersen - M. Van Drunen, *Germany proposes Europe's first diversity rules for social media platforms,* in *LSE blog*, 29 May 2019.

and non-discriminatory terms.

From a technical perspective, the unbundling could imply to design core services to be interoperable (for example, to design the APIs to be interoperable) at cost-based price which is objectively justifiable. In fact, in order to be able to provide content curation on social media platforms, third parties would need to have access to the platform's APIs, or to be able to integrate their own API on the social media platform. At present all the major social media platforms have their own APIs and provide app developers access to them according to different conditions, so it is reasonable to believe that the first option would be the easiest solution[75]. What is needed is thus a meaningful degree of interoperability. Scholars, experts and civil society have advanced proposals that span from partial and unidirectional interoperability to full protocol interoperability[76]. To set the adequate degree of interoperability to be imposed on major platforms could remain a regulator's task, or it could be left to the industry, with the provision of some form of independent oversight and minimum parameters to be respected[77].

Furthermore, the unbundling could imply to design core services in a way that allows to manage privacy, security and similar technical concerns, in compliance with the relevant legislative frameworks as well as with industry and technical standards; not to withhold, withdraw, depreciate or otherwise change APIs in a way that has a material adverse effect on users without sufficient consultation or objective justification; to ensure that standards developed are interoperable[78]. This deployment of the unbundling seems to fit well in the framework of the recent European Commission's proposal for a Digital Markets Act. Indeed, the Digital Markets Act calls for gatekeepers to allow the installation and effective use of third-party applications that interoperate with the operating system of the gatekeeper[79].

As for the best way to shape and enforce unbundling, because of stark information asymmetries in the market, co-regulation might once again be a better fit. A possible

[75] However, some scholars remain skeptical with regards to the technical feasibility of this solution. See, for example, D. Keller, *Platforms Content Regulation – Some Models and Their Problems*, in *The Centre for Internet and Society blog*, 6 May 2019.

[76] Suggestions about interoperability measures and how to shape them with regards to specific use cases can be found, among others, in : J. Cremer - Y. A. de Montjoye - H. Schweitzer, *Competition Policy for the Digital Era*, cit.; I. Brown, *The technical components of interoperability as a tool for competition regulation,* OSF preprint, 2020; V. Bertola, *A Technical and Policy Analysis of Interoperable Internet Messaging,* 2020; Internet Society, *White Paper: Considerations for Mandating Open Interfaces*, December 2020; B. Cyphers - C. Doctorow, *Privacy Without Monopoly: Data Protection and Interoperability*, Electronic Frontier Foundation Paper, 2021; P. Marsden - R. Podszun, *Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement*, Konrad-Adenauer-Stiftung, Berlin, German. e. V. 2020.

[77] P. Alexiadis - A. de Streel - *Designing an EU Intervention Standard for Digital Gatekeepers,* cit.

[78] Competition and Markets Authority, *Online Platforms and Digital Advertising,* cit. It should be noted that the relevant behaviours of dominant social media platforms I deal with in this paper could be shaped as exploitative abuse towards users complemented by an exclusionary effect on competitors. Although in principle unbundling as *ex post* competition remedy could have the same or a similar impact to a regulatory unbundling, in this case, however, I am convinced that it would not. This is because the case a stake is about a persistent market failure, which is extensive, and where timely intervention is indispensable. For this reason, following what stated in Recital 16 of the European Commission Recommendation 2014/710, I suggest unbundling as an *ex ante* and not an *ex post* remedy and I call for regulatory intervention, rather than the enforcement of competition rules.

[79] European Commission, Digital Markets Act, cit., Article 6(1)(c).

solution could be to include unbundling and its related obligations in codes of conduct, which could be drafted mainly by companies in dialogue with regulators and then approved and made mandatory by the latter. In recent times, decision makers have expressed preference for this kind of instrument. The European Commission has recurred to it to try to solve a number of challenges hitting hard on social media platforms, such as disinformation of hate speech[80]. The Furman Report has suggested the development of a Code of Competitive Conduct, which would apply to digital platforms designated with a "strategic market status"[81]. The ACCC as well asks designated digital platforms to provide a code of conduct that govern their commercial relationships with news and media businesses[82]. Code of conducts have to set the minimum requirements, but companies could go higher. However, regulators should be able to enforce those codes in case companies do not voluntarily comply; they should also have the capacity and expertise to monitor and assess the enforcement of the codes.
To sum up, the design of both remedies implies solving complex technical issues. The regulated diversity needs the operationalisation, into an algorithm, of the normative value of diversity. The unbundled access requires platforms to open their APIs or to put in place similar solutions for competitors to plug-in and run their algorithms on the platform, and all this has to happen adequately protecting users' data and by maintaining high standards of security. In both cases, the remedy asks regulators for technical expertise that they might don't have internally, and it could be better implemented if regulators engage in a transparent and fruitful dialogue with companies' technical departments, in addition to the policy and regulatory ones.

6.6. Consistency with existing rules that apply to social media platforms

Social media platforms are subject to a number of different rules: some apply horizontally to all services they provide (such as competition law), while others apply only to the provision of specific services (such as data protection rules or rules on the prevention of hate speech or on the removal of illegal content). As the two proposed remedies land in a shared regulatory space, this benchmark helps regulators to assesses how consistent each of them is with the existing rules social media platforms are subject to. Regulators have to consider that to impose on social media platforms a certain degree of diversity while performing content curation might imply an obligation for companies to monitor all content that circulates on their platforms. This could result in a form of general monitoring of users' speech by private actors, which would constitute a blatant violation of freedom of expression. Moreover, such control could open the door to censorship, or to an ever greater influence on the public debate. The current EU regulatory framework provides hosting platforms with a liability exemption insofar as they do not interact in any way with the content they host. This liability exemption,

[80] *Ibid.*; European Commission, *Code of Conduct on Countering Illegal Hate Speech Online*, 2016.

[81] Digital Competition Expert Panel, *Unlocking Digital Competition,* cit.

[82] ACCC, *Digital Platforms Inquiry*, cit.

provided by the E-commerce Directive[83], is retained in the new Commission's proposal for a Digital Services Act[84]. In a scenario where companies are charged with must view obligations, it can be argued that they will necessarily interact with the content, or at least with part of it, thus losing the safe harbour, or liability exemption. Regulators should then consider the additional consequences of this remedy, and assess if the trade-offs are compatible with the results it aims to achieve.

On the other hand, the unbundled access to content curation might not necessarily imply a change in the current intermediary liability regime for social media platforms. Indeed, separating content curation from hosting, and mandating the possibility for third parties to provide content curation services on large social media platforms, does not imply matching any quotas in the diversity of sources and viewpoints, and therefore does not require the imposition of a general monitoring obligation. Aside from eliminating the risk of violating the international standards of freedom of expression, it also has the advantage of being compatible with the European Commission's proposal for a Digital Services Act.

Nonetheless, while access to the APIs is essential for this remedy to function in practice, a number of related issues must also be carefully addressed. An adequate system should be put in place in order to guarantee that both incumbent and third-party players collect, process, store and use users' data according to the General Data Protection Regulation (GDPR)[85] rules and principles. Civil society groups have argued that processing should be strictly limited to that needed to support interoperability[86].

Some have suggested that to avoid revealing private user information to an abundance of providers, the content curation provider's system should run on the platform's infrastructure. This way, the platform that provides the hosting would be responsible for the overall user experience[87]. The likely weakness of this suggestion is that if the platform remains also responsible for delivering ads against the selected content, it would subtract the main avenue of monetization to content curation providers, that is to its potential competitors.

Concerns similar to those highlighted for data protection could be raised with regard to security. Here as well, the introduction of an intermediary for the content curation

[83] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") [2000] OJ L 178, 1–16.

[84] European Commission, Digital Services Act, cit., Article 5.

[85] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) [2016] OJ L 119.

[86] B. Cyphers - C. Doctorow, *A Legislative Path to an Interoperable Internet*, Electronic Frontiers Foundation Deeplink, 28 July 2020. On a similar vein, the European Data Protection Board (EDPB), in the context of assessing interoperable solutions for Covid-19 apps, has emphasised that interoperability should not be used as an argument to extend the collection of personal data beyond what is necessary, and that the respective roles, relationships and responsibilities of the joint controllers in regards to the data subject will need to be defined and this information needs to be made available to the data subject (see EDPB, *Statement on the Data Protection Impact of the Interoperability of Contact Tracing Apps*, 16 June 2020.

[87] S. Wolfram, *Optimizing for Engagement: Understanding the Use of Persuasive Technology on Internet Platforms,* cit.

could create uncertainty about the allocation of responsibilities and liabilities, which should be dissipated either through adequate contractual agreements, or, if needed, via regulatory intervention.

Finally, the implementation of algorithms for content curation, irrespective of whether they are used by large social media platforms or by alternative operators, should be compliant with international standards on human rights. In particular, the design and deployment of algorithms should comply with the criteria suggested by various norms and recommendations that are progressively contributing to shape a regulatory framework for Artificial Intelligence[88]. At the bare minimum, players should properly assess, both at the design phase and through the entire process, the potential impact of the algorithm on users' fundamental rights, and should put in place efficient measures to avoid or minimise any negative impacts. In addition, players should put in place adequate remedies in case the negative impact occurs and make them easily accessible for users.

To conclude, when assessed under this benchmark, the key difference between the two regulatory solutions seems to be that regulated diversity might raise conflicts with the platforms' liability regime with regards to the content they host, which are not raised by the unbundled access. This could be a major shortfall for regulated diversity, which regulators should take into due account while designing the measure.

6.7. Institutional considerations

There is increasing pressure to regulate social media platforms, and calls are addressed to a number of regulators. This benchmark looks at whether and to what extent the two remedies would require a new regulator, and at how an existing regulator in charge of enforcing each of the remedy could coordinate with the others that share the regulatory space of these platforms.

Media diversity has traditionally been one of the policy objectives of media regulators; therefore, this remedy naturally lands in the scope of competence of those regulators and does not require the setting of a new one. Nevertheless, media regulators should coordinate with bodies in charge to protect people's freedom of expression rights, as the remedy impacts exposure diversity in a paternalistic way that has to be kept in check. In addition, at least a minimum degree of coordination might be required with data protection and consumer authorities, to ensure that the must carry obligations are implemented in a way that is compliant with data protection and consumer protection rules. No coordination with competition authorities seems to be required in this case.

The unbundling, on the other hand, is part of the traditional toolbox of both telecom

[88] High Level Expert Group on AI, Ethics Guidelines for a Trustworthy AI, 2019; Council of Europe Commissioner for Human Rights, Unboxing Artificial Intelligence: 10 Steps to Protect Human Rights, 2019; United Nations Special Rapporteur on Freedom of Expression, Report of the Special Rapporteur to the General Assembly on Artificial Intelligence Technologies and Implications for the Information Environment, A/73/348, 2018; United Nation Special Representative of the Secretary-General on human rights and transnational corporations and other business enterprises, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Annex to Report A/HRC/17/31, 2011.

regulators and competition authorities. The former have traditionally applied it *ex ante* to incumbents, while the latter can impose it *ex post* on dominant platforms that abuse their position of power. As the remedy proposed here is to be applied *ex ante*, telecoms regulators might be best placed. An additional advantage would be that in the EU the majority of telecoms regulators also deal with the media sector, and thus has the expertise needed to deal with media diversity issues.

The unbundling should be shaped and enforced in a way that guarantees consumers' rights, including data protection ones. To do so, the regulator should seek the advice of data and consumer protection authorities, who have the needed expertise. This could be done in the form of consultation, which allows the regulator to analyse the issue from the different relevant perspectives and to benefit from the specific expertise it doesn't have internally. In addition, an agreement on the remedy can avoid conflicts in the enforcement phase, as through the consultation the authorities reach an agreed position on the nature of the infringement of the remedy[89].

A form of coordination might be needed with competition authorities, too. First, because platforms with gatekeeping power might also reach the threshold of dominance, and thus their behaviour could become relevant under Article 102 TFEU. Second, because gatekeeping power can traduce in anti-competitive behaviours that competition authorities might decide to target *ex post*. Here again, the two regulators gain substantially from some form of cooperation that leads to an agreed remedy, and this translates also into greater legal certainty for the companies the remedy is imposed on. Indeed, there have been examples, in the past, of *ex ante* rules, which included unbundling, imposed on operators that have nevertheless been accused of infringing Article 102 TFEU while applying the remedy. An example is Deutsche Telekom: in 2003, the company was obliged to unbundle the local loop and apply wholesale prices approved by the German telecom authority[90]. However, the approved wholesale and retail prices were found to constitute price squeeze, contrary to Article 102 TFEU. Deutsche Telekom argued that it relied on the regulator's directions and so assumed that its pricing policy were lawful. The Commission, on its part, argued that the company had a sufficient margin of discretion in setting its pricing policy that the conduct was to be considered its own, rather than an imposition by the regulator. As the conduct was autonomous, then competition law applies, and the approach was confirmed by the Court of Justice[91]. A consultation among the regulator and the competition authority while shaping the remedy can improve the quality of decision making, provide more legal certainty, eliminate wasteful duplication and guarantee effective enforcement.

To conclude, from an institutional perspective, the regulated diversity is more contained in the regulatory space traditionally attributed to media regulators, and therefore might require less coordination among the latter and other regulators. On the contrary, the unbundled access, to be properly designed and enforced, might need a higher de-

[89] G. Monti, *Attention Intermediaries: Regulatory Options and their Institutional Implications,* TILEC Discussion Paper, DP 2020-018, 2020.

[90] European Commission, Case COMP/C-1/37.451, 37.578, 37.579 — *Deutsche Telekom AG* [2003], OJ L 263/9.

[91] CJEU, C-280/08 P, *Deutsche Telekom AG v European Commission* (2010).

gree of cooperation among the various regulators that deal with the various aspects of the remedy, from competition to data protection ones.
As overall remark for this part, it has to be considered that while each of the benchmarks identified and used in this section has its own scope in the assessment of the two proposals, various degrees of overlaps and interplays exist among them. For example, as mentioned above, the normative approach has an impact on users' empowerment. The consistency with existing rules that apply to social media platforms has an influence in the role the regulator plays in the regulatory space he shares with the enforcers of those rules. The need for complementary rules depends on how the measure is concretely designed. Regulators, therefore, should not look at the benchmarks separately, but consider their strict relations.

Part IV

7. Conclusions

The massive process of digitalisation over the past two decades has enormously increased the possibilities for individuals to create, share and access content online. While this ever wider amount of information is theoretically available for all, the ability of individuals to concretely reach and enjoy such plurality and diversity can be strongly limited, in social media markets, by a number of factors. This paper contributes to the debate by looking at under exposure to diversity on social media markets and by focusing on what could be one of its main causes, that is the way content is curated by the automated systems used by platforms. It also suggests two possible regulatory solutions and proposes an analytical framework that regulators could use to assess the solidity and efficiency of each of them under a number of benchmarks.
The first solution is to regulate diversity by imposing "must view" obligations on players with gatekeeping powers. The second is to unbundle hosting activities from content curation activities and to oblige large platforms to provide fair, reasonable and non-discriminatory access to those competitors that want to provide content curation on their platforms.
The benchmarks in the analytical framework have been selected to help regulators in their assessment, and to provide input for more research on elements that might still be unexplored or not sufficiently explored. The benchmarks look at the proposed solutions from different perspectives: their content, their impact on markets, consumers, and on the existing regulatory frameworks, and their enforcement and challenges related to institutional setting issues.
The preliminary conclusion is that unbundled access to content curation might be a better option than regulated diversity. With the unbundling, the State intervenes on market dynamics and relies on healthy competition among players to ensure diversity; in addition, it seems to provide an adequate response not only to the market failure in terms of exposure diversity, but also to other market failures in social media markets, such as the existence of high barriers to entry, the high concentration in the market,

and the lack of viable alternatives for users. This particularity might play an important role in the regulators' assessment. Indeed, in an increasing number of online marketplaces it is possible to observe various market failures at once. As often these marketplaces fall in the remit of different regulators, each of them should intervene for the aims and objectives within its remit; nevertheless, when selecting the right instrument for intervention, each regulator should also take into utmost account the impact each instrument could have on the objectives other regulators are called to ensure in the same marketplace, and choose the one that facilitates, or at least does not conflict with those objectives. The unbundled access appears to be a good example of this approach.

It remains to be noted that for this remedy to work properly and not to undermine users' human rights, a few additional challenges might need to be solved. This paper has tried to identify these challenges, while noting that they would benefit substantially from further research and debate in order to be properly addressed.

To that aim, a better knowledge of how algorithms for content curation work would certainly be beneficial for regulators to make more informed decisions. There is still need for additional research, the main obstacle to which appears to be the lack of access to the information that is needed to perform it. Regulators could play a role here too, for example by obliging platforms and content curators to be more transparent about the automated systems they use, and in general about their business models, and to oblige them to provide access to information and data for independent research. Both the DSA and the DMA proposals appear to go in this very same direction.

Furthermore, technical standards could help to make automated systems, and therefore content curation, more compliant with human rights and more sensitive to exposure diversity. To this aim, a continuous dialogue between the industry and other interested stakeholders would likely lead to better outcomes for users as well as for society as a whole.

Finally, it has to be taken into account that regulated diversity and unbundling of hosting and content curation are not necessarily mutually exclusive. There are various ways they could be combined, to different degrees. One scenario could be the regulator that imposes the unbundling and, at the same time, intervenes on the criteria or standards used by players for the provision of content shaping. In this case, the final result, that is the selection of content that users see, is not left totally to the automated system. Certain degree of experimentalism by regulators might be welcome in this scenario, where a large number of commercial and technical factors have to be considered and dealt with in order to achieve and guarantee public interest objectives. However, the regulatory instincts have to be kept in check; for this reason, regulators should remain anchored to the proportionality and necessity tests while shaping regulatory interventions.

Siamo tutti giornalisti? Appunti sulla libertà di informazione nell'era *social**

Alessandro Lauro

Abstract

Il saggio riflette sulla libertà di informazione alla luce dell'evoluzione tecnologica, concentrandosi sulla circostanza che oggi qualunque utente di Internet può diventare giornalista.
L'indagine è condotta secondo una prospettiva di diritto costituzionale interno e comparato, con speciale riguardo alle giurisprudenze dei giudici costituzionali nazionali (fra le quali l'ord. 130/2020 della Corte costituzionale italiana) e delle corti sovranazionali europee. In particolare, ci si focalizza su come l'evoluzione tecnologica abbia modificato i contorni di questa libertà, ampliando considerevolmente il numero di coloro che possono esercitarla in maniera diffusa, e su quali limiti si rendano necessari, oggi più di ieri, affinché il suo proficuo esercizio non collida con altri diritti fondamentali, determinandone un insanabile sacrificio.

The essay reflects on freedom of information in the light of technological evolution, focusing on the circumstance that today any Internet user can transmit information and thus become a "journalist".
The study is conducted from the perspective of domestic and comparative constitutional law, with special attention to the case-law of national constitutional judges (including the order no. 130/2020 of the Italian Constitutional Court) and supranational European courts. In particular, it focuses on how technological evolution has changed the contours of this freedom, considerably expanding the number of those who can exercise it in a widespread manner, and on what limits are necessary, today more than yesterday, so that its profitable exercise does not collide with other fundamental rights, causing an irremediable sacrifice.

Sommario

1. Introduzione. – 2. La libertà di informazione nello spettro delle libertà comunicative. – 3. Il problema del mezzo: Italia, 1973 - Gran Bretagna, 2016. – 4. Una libertà adespota? La sentenza *Sergejs Buivids* della CGUE (C-345/17) e il giornalismo diffuso. – 5. La necessità di cercare nuovi bilanciamenti: l'ordinanza n. 132 del 2020 della

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Corte costituzionale italiana. – 6. La libertà di informazione come libertà politica e la protezione del suo versante passivo. – 7. Conclusioni.

Keywords
informazione – giornalismo – Internet – social network – giurisprudenza costituzionale

Aut tacere, aut loquere meliora silentio
(O taci, o di' qualcosa di meglio del silenzio)
dall'*Autoritratto* di Salvator Rosa.

1. Introduzione

La rivoluzione tecnologica rappresentata dalla capillare diffusione delle infrastrutture digitali e della rete Internet ha consegnato a chiunque vi abbia accesso un'incredibile opportunità di divulgare il proprio pensiero senza limiti spaziali, fisici e temporali. In maniera immediata, un commento affidato alla rete può fare il giro del mondo, secondo modalità inimmaginabili sino a pochi decenni fa. La nascita e la diffusione dei *social network* hanno ulteriormente amplificato queste possibilità comunicative[1].
Se nel 1789 l'art. 11 della *Déclaration des droits de l'homme et du citoyen* celebrava la libera comunicazione dei pensieri e delle opinioni come uno dei diritti più preziosi dell'uomo, oggi questo valore inestimabile parrebbe essere accresciuto e definitivamente consacrato dalle nuove tecnologie.
Questo contributo si prefigge di riflettere attorno ad una particolare forma di libertà di comunicazione – ovvero la libertà di informazione – indagata in una prospettiva di diritto costituzionale interno e comparato, con speciale riguardo alle giurisprudenze dei giudici costituzionali nazionali e delle corti sovranazionali europee. In particolare, le osservazioni che seguiranno si focalizzeranno su come l'evoluzione tecnologica abbia modificato i contorni di questa libertà, ampliando considerevolmente il numero di coloro che possono esercitarla in maniera diffusa, e su quali limiti si rendano necessari, oggi più di ieri, affinché il suo proficuo esercizio non collida con altri diritti fondamentali, determinandone un insanabile sacrificio.

[1] Si ricorderà la provocatoria frase di Umberto Eco in occasione della *lectio magistralis* per il conferimento della laurea *honoris causa* in Comunicazione e cultura dei media presso l'Università di Torino, l'11 giugno 2015: «I social network hanno dato diritto di parola a legioni di imbecilli».

2. La libertà di informazione nello spettro delle libertà comunicative

È opportuno, innanzitutto, tracciare la cornice teorico-costituzionale in cui si inserisce la libertà di informazione, dal momento che negli ordinamenti costituzionali contemporanei è garantita ai singoli una vasta gamma di libertà comunicative.
La prima distinzione da sottolineare concerne le libertà di *comunicazione privata,* che vanno individuate separatamente rispetto alle libertà di *comunicazione pubblica*[2].
Nelle prime rientrano tutte quelle esternazioni che il singolo vuole limitate ad una sfera ristretta di destinatari, nell'ambito di rapporti riservati e privati. Questa tipologia di libertà di comunicazione privata trova una precipua e classica tutela nella libertà di domicilio (con la conseguente protezione dei discorsi e delle comunicazioni che intervengono nell'ambito sottratto al controllo pubblico) e, ancor più evidentemente, nella libertà di corrispondenza. Non a caso, il diritto alla riservatezza è stato proprio ricondotto – nella sua versione minima – alla combinazione fra questi due capisaldi degli ordinamenti liberali[3].
Le libertà di *comunicazione pubblica* si caratterizzano per il fatto di dare tutela a quei messaggi destinati ad una categoria indefinita di destinatari e, in particolare, alla comunità di riferimento del mittente, senza che questi possa selezionare i propri interlocutori[4].
Va detto sin da subito che, sebbene sia possibile in astratto individuare una specifica "frequenza" per ciascun sotto-tipo di libertà di comunicazione pubblica, nella pratica le "bande di oscillazione" di queste libertà – volendo continuare nella metafora – interferiscono fra loro e non è sempre agevole sceverare quale libertà sia esercitata in

[2] Sebbene, come rilevato dalla dottrina, l'evoluzione tecnica rende più sfuggente anche questa distinzione: v. P. Caretti, *Comunicazione e informazione*, in *Enciclopedia del diritto - Annali,* I, Milano, 2007, 219: «Il progressivo venir meno della distinzione tra mezzi di comunicazione e servizi, da un lato, che caratterizza tutto il settore della comunicazione elettronica (e la conseguente possibilità di utilizzare uno stesso mezzo per diffondere messaggi della più diversa natura: dati, notizie, messaggi vocali, immagini), il nascere di nuove forme comunicative che si pongono a cavallo tra le tradizionali forme di comunicazione interpersonale e quelle invece di comunicazione aperta, destinata ad un pubblico indifferenziato, e di nuovi sistemi di accesso interattivo alle reti, dall'altro, sono tutti fenomeni che reagiscono sullo stesso modo di classificare le diverse attività che in essi sono coinvolte e di ricostruirne appunto il regime giuridico, alla luce delle indicazioni costituzionali».

[3] Fondamentale, nell'ordinamento italiano, la pronuncia della Corte di Cassazione nel c.d. "caso Soraya" (Cass. civ., sez. I, 27 maggio 1975, n. 2129, in *Il Foro Italiano*, 99, 1976), che ha ricostruito il diritto alla riservatezza ricollegandolo ad una trama di principi costituzionali: «Un duplice spunto di convalida al diritto di riservatezza si trae anche dall'art. 3 Cost. sia perché, riconoscendosi la dignità sociale del cittadino, si rende necessaria una sfera di autonomia che garantisca tale dignità, sia in quanto rientrano nei limiti di fatto della libertà ed eguaglianza dei cittadini anche quelle menomazioni cagionate dalle indebite ingerenze altrui nella sfera di autonomia di ogni persona. E, sotto questo profilo, va ricordata anche la inviolabilità della libertà personale (art. 13), intesa questa in un senso più ampio della libertà meramente fisica. Già si è notata la rilevanza che sul problema della riservatezza ha l'art. 14 della Costituzione, che riguarda, oltre la inviolabilità del domicilio, anche i limiti alle ispezioni, alle perquisizioni, agli accertamenti per motivi pubblici. Nella stessa linea si pone il successivo art. 15, relativo all'inviolabilità della libertà e della segretezza della corrispondenza».

[4] C. Chiola, *L'informazione nella Costituzion*e, Padova, 1973, 16-17: «Così, mentre pensieri e notizie che vengono comunicati ad un numero indeterminato di persone rientrano nella tutela predisposta dall'art. 21 Cost., il trasferimento dei medesimi nella sfera conoscitiva di uno o più soggetti determinati va riferito all'art. 15».

concreto[5]. Ciò, però, non può scoraggiare l'interprete dal definire alcune differenze fra queste libertà embricate eppure distinte, poiché, da un lato, ciascuna di esse può godere di una diversa intensità rispetto alla sua tutela, intensità che varia in base all'esercizio del diritto in contesti specifici o da parte di soggetti privilegiati (si pensi alla libertà delle arti, della ricerca scientifica o alla libertà di insegnamento). Dall'altro lato, l'identificazione più precisa della libertà esercitata consente di tracciarne i limiti e contenerne gli abusi.

La libertà più ampia – o, se si vuole meno specifica – all'interno di questa categoria è la *libertà di espressione*, intesa come possibilità di esprimere con qualunque mezzo la propria personalità[6]. Più ristretta, ma ancora molto ampia, è la *libertà di manifestazione del pensiero* o *libertà di opinione,* che garantisce l'esternazione, fuori da contesti meramente privati, delle proprie idee e opinioni a terzi.

Venendo alla nostra *libertà di informazione*, essa consiste nella facoltà di trasmettere ad altri informazioni, dati e notizie che rechino un qualche interesse della collettività alla loro conoscenza, sicché si parla di questa anche sotto la formula del *diritto di cronaca*[7].

In quest'ottica, data la differenza dell'oggetto contenuto nella comunicazione, non pare che la libertà di informazione costituisca propriamente un sottoinsieme della libertà di opinione. È tuttavia chiaro che l'esercizio della prima comporta il contestuale esercizio della seconda: per un verso, infatti, è difficile che l'informante riesca a trasmettere in maniera completamente neutra l'informazione, senza che essa sia filtrata

[5] Vale, dunque, in termini più generali quanto affermato da L. Paladin, *Problemi e vicende della libertà di informazione nell'ordinamento giuridico italiano*, in Paladin (a cura di), *La libertà di informazione*, Torino, 1979, 8, rispetto alla sola libertà di informare: «Quando si tratta della libertà d'informazione, bisogna tener presente, in altri termini, che essa non corrisponde né ad un diritto unitario, né ad un fascio di diritti fra loro coerenti, ma si risolve piuttosto in una formula che congiuntamente allude ad esigenze assai eterogenee (e a volte confliggenti le une con le altre)». G. Pascuzzi, *Il diritto dell'era digitale*, Bologna, 2010, 17 osserva che a seguito del fenomeno della c.d. «convergenza tecnologica» (che assottiglia la differenza fra reti e strumenti di accesso a tali reti, quali telefono, televisione o computer) si verifica un «appannamento della distinzione fra art. 15 e 21 della Costituzione».

[6] C. Chiola, *L'informazione nella Costituzione*, cit., 15: «Così, sembra difficilmente accettabile la dilatazione dell'art. 21 Cost., fino al punto di intendere il "pensiero", oggetto della tutela in questo previsto, come libertà di "espressione". L'ampiezza concettuale sottintesa da quest'ultimo termine permetterebbe, infatti, di estenderne l'applicabilità ad una serie indefinita di comportamenti umani, tanto che la linea di demarcazione tra questa particolare libertà e la tutela della personalità individuale, generalmente prevista dall'art. 2 Cost., finirebbe per svanire». *Ibidem*, nota 43, l'A. fa l'esempio della nudità come forma di espressione non verbale riconosciuta da una Corte di Los Angeles.

[7] Ivi, 23, si suggerisce di condurre il diritto di cronaca ai diritti della personalità *ex* art. 2 Cost. in combinato disposto con l'art. 8 della Convenzione Europea dei diritti dell'uomo («la pretesa a narrare può essere egualmente garantita invocando l'art. 2 Cost. qualora si sostenga che dall'intangibilità del principio di libertà che ne deriva, ogni limite che a questa si volesse imporre deve pur sempre corrispondere a un interesse costituzionale»). A. Lamberti, *Libertà di informazione televisiva e diritti fondamentali*, Milano, 2009, 154 riconduce «la libertà di informazione come diritto fondamentale» anche «al caposaldo costituzionale dato dall'art. 3, secondo comma», in particolare alla promozione della partecipazione effettiva dei lavoratori all'organizzazione politica, economica e sociale del Paese e dunque «affinché la libertà di informazione possa esercitarsi in modo pieno ed "eguale" per tutti gli appartenenti ad una comunità», occorre che «il complessivo sistema informativo del settore considerato sia strutturalmente idoneo a garantire la completezza e l'obiettività dei flussi di notizie e dati che esso è destinato ad erogare. Così, la diffusione di informazioni in condizioni di eguaglianza esige l'esistenza del pluralismo delle fonti e, nei limiti in cui ciò non contrasti con altri valori di rilievo costituzionale, asseconda il pluralismo all'interno di ciascuna fonte».

dalle sue convinzioni o opinioni personali[8]. Per altro verso, e forse con maggiore pregnanza, la stessa selezione delle informazioni da trasmettere presuppone un giudizio di valore compiuto sull'informazione stessa, che si produce naturalmente sulla base delle opinioni della persona che informa. Dunque, se è vero che esiste una natura servente delle *informazioni* rispetto alle *opinioni,* poiché l'acquisizione delle une è necessaria perché si formino le altre[9], non è men vero che il possesso di opinioni orienti la ricerca e l'individuazione delle informazioni. Sul diritto di cronaca grava poi un dovere di veridicità, che non può essere rintracciato nell'esercizio della libertà di opinione[10].
Alla libertà di informazione in senso attivo corrisponde un diritto passivo ad ottenere informazioni[11], tant'è che negli ordinamenti anglosassoni il riferimento alla *freedom*

[8] V. Crisafulli, *La problematica della "libertà di informazione"*, in *Il Politico*, 2, 1964, 288: «Si contesta, in particolare, la stessa configurabilità della notizia oggettiva, quindi quel carattere di neutralità che dovrebbe contrassegnare l'informazione, così intesa ; anche la scelta delle notizie, pur se divulgate nel modo più scrupolosa-mente completo ed imparziale, non può non implicare, si osserva, una valutazione, necessariamente soggettiva ed in questo senso, dunque parziale» L'A. sottolinea quindi che «la libertà di informazione, come avente ad oggetto notizie, quindi come manifestazione differenziata della più generale libertà di espressione (o di informazione in senso largo), [merita] un posto a sé ed un rilievo particolare». Nello stesso senso P. Barile, *Libertà di manifestazione del pensiero*, in *Enciclopedia del diritto,* XXIV, Milano, 1974, § 13: «lo sceverare il fatto dal giudizio (ad esempio, dal modo come esso viene presentato) è, per comune e pacifica esperienza (che si rispecchia nella giurisprudenza di merito), praticamente impossibile, almeno nella maggioranza dei casi».

[9] C. Poncet, *La liberté d'information du journaliste: un droit fondamental? Étude de droit suisse et comparé*, in *Revue internationale de droit comparé*, 1980, 733 afferma: «*La liberté de l'information est à la liberté d'opinion et à la liberté d'expression ce que l'eau est au moulin*». Cfr. anche V. Crisafulli, *La problematica della "libertà di informazione",* cit., 287: «Solo dove i testi costituzionali distinguono libertà di opinione da libertà di informare […] potrebbe semmai sorgere dubbio in proposito; ma, a parte il rilievo che anche in questi casi la garanzia della libertà di informare non è certo minore della garanzia apprestata alla libertà di esprimere opinioni, si ritiene generalmente che il riconoscimento esplicito di questa seconda implica logicamente riconoscimento della prima, perché le opinioni si formano sui fatti e non potrebbe esservi circolazione delle idee se non vi fosse del pari circolazione delle notizie».

[10] Cfr. la STC 107/1988 del Tribunale costituzionale spagnolo: «*la libertad de expresión es más amplia que la libertad de información al no operar en el ejercicio de aquella el límite interno de veracidad que es aplicable a esta*».

[11] Nella dottrina italiana si è discusso se esista un vero e proprio "diritto soggettivo ad essere informati". A favore di questa configurazione N. Lipari, *Libertà di informare o diritto ad essere informati? (Spunti di riflessione)*, in *Il diritto delle radiodiffusioni e delle telecomunicazion*i, 1978, 2: «Nella sua formulazione letterale l'art. 21 Cost. considera esclusivamente il diritto di manifestare il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione. Nel momento in cui diamo a questo testo (io credo legittimamente) il significato di una garanzia della libertà di "informare", abbiamo già compiuto un salto qualitativo rispetto alla semplice libertà di manifestare il proprio pensiero, perché abbiamo già caratterizzato il dettato costituzionale non semplicemente in funzione dell'interesse di chi utilizza il mezzo di diffusione, ma altresì in funzione dell'utilità di un prevedibile destinatario della comunicazione». Contra A. Pace, *Libertà di informare e diritto ad essere informati. Due prospettive a confronto nell'interpretazione e nelle prime applicazioni dell'art. 7, co. 1, del T.U. della radiotelevisione*, in *Diritto pubblico*, 2, 2007, 459 ss.: «l'operatore informativo, pur negando al suo pubblico la spettanza di pretese giustiziabili nei suoi confronti per ciò che attiene al contenuto e alla forma del "messaggio", non è, per definizione, insensibile agli umori e, in una certa misura, ai gusti del suo pubblico. È infatti lo stesso interesse economico (e cioè la remuneratività del capitale di rischio) ad imporgli, qualora si muova in un'ottica squisitamente economica, di essere sensibile agli orientamenti del suo peculiare "mercato". Ciò potrebbe, in teoria, addirittura implicare un "miglioramento" della qualità del suo prodotto, se il mercato gli richiedesse una "maggiore" completezza, imparzialità e obiettività, il che purtroppo non accade... sempre. Più spesso il "miglioramento" del prodotto richiesto dall'opinione pubblica implica, paradossalmente, una "minore" completezza, imparzialità e obiettività dell'informazione. La quale, beninteso, resta parimenti tutelata dall'art. 21 Cost., sempre che il prodotto informativo non violi i consueti limiti del divieto del subiettivamente falso e del rispetto dell'altrui dignità personale».

of information attiene propriamente al diritto positivo ad accedere all'informazione, in particolare se essa è posseduta da autorità pubbliche[12]. La rivoluzione digitale ha addirittura condotto alcune giurisdizioni a riconoscere l'accesso ad Internet come diritto fondamentale direttamente ricollegato alla libertà di informarsi[13].

Dal punto di vista del diritto positivo, l'autonomia concettuale della libertà di informazione – accanto alla più tradizionale libertà di espressione – è oggi recepita da vari testi di valore costituzionale e, osservando la successione delle carte costituzionali, è andata via via affermandosi più nettamente. Le carte liberali, infatti, tutelavano non tanto la libertà di informazione in sé, ma anzitutto l'utilizzo di mezzi particolari (v. *infra*) per veicolare le proprie opinioni[14]. In origine, dunque, vi era una tutela della *libertà di stampa* (o, meglio*, libertà di stampare*[15]), mentre successivamente – e compiutamente nelle Costituzioni del secondo dopoguerra – è la stampa, come *sistema dei mezzi di informazione a carta stampata* (cioè i periodici), che viene protetta da indebite ingerenze da parte dei poteri pubblici[16]. Ancora, nei testi più recenti forme di garanzia costituzionale si esten-

[12] Ad esempio, il *Freedom of Information Act* emanato nel 1966 a livello federale negli Stati Uniti e il *Freedom of Information Act* (FOIA) adottato nel 2000 dal Parlamento del Regno Unito. In Italia, ciò è stato garantito dalla disciplina del "diritto di accesso", contenuta negli art. 22 e seguenti della legge 241/1990, poi ampliato con il c.d. accesso civico (nella versione "semplice" e "generalizzata"), introdotto dal d.lgs. 33/2013 modificato nel 2016 da d. lgs. n. 97 (anche in Italia ribattezzato FOIA).

[13] Cfr. la *décision* del *Conseil constitutionnel* francese n. 2009-580 DC del 10 giugno 2009, *Loi favorisant la diffusion et la protection de la création sur internet*. Nel c*onsiderant* n. 12, il Consiglio afferma: «*en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services*».

[14] Cfr. J. Rivero, *Il regime giuridico dell'informazione in Francia*, in Paladin, *La libertà di informazione*, cit., 67: «fare intendere delle idee, non far conoscere degli avvenimenti, ecco quel che sembra essenziale agli uomini della Rivoluzione. All'inizio, la libertà della stampa è dunque orientata non verso l'informazione, ma verso la diffusione delle ideologie». Come già ricordato l'art. 11 della Dichiarazione del 1789 stabilisce che «*tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi*». Il I emendamento della Costituzione degli Stati Uniti, approvato nel 1791, riconosce, accanto alla libertà di parola, la libertà di stampa: «*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances*».

[15] Anche rispetto alla Costituzione italiana, L. Paladin, *Problemi e vicende della libertà di informazione nell'ordinamento giuridico italiano*, cit., 6 afferma che «della stampa stessa viene esaltato il momento consistente nel diritto di stampare, a detrimento della "libertà della stampa", vale a dire di quella disciplina delle componenti materiali ed umane delle imprese giornalistiche».

[16] L'art. 5 della *Grundgesetz* sancisce il diritto ad informarsi da fonti accessibili a tutti, oltre a stabilire la libertà dell'informazione tramite la radio ed il cinema. Come ha spiegato il Tribunale costituzionale di Karlsruhe (BverfGe 85, 1, § 39): «*Während die in einem Presseerzeugnis enthaltene Meinungsäußerung bereits durch Art. 5 Abs. 1 Satz 1 GG geschützt ist, geht es bei der besonderen Garantie der Pressefreiheit um die einzelne Meinungsäußerungen übersteigende Bedeutung der Presse für die freie individuelle und öffentliche Meinungsbildung, die Art. 5 Abs. 1 GG gewährleisten will*» ("mentre l'espressione di un'opinione tramite un mezzo stampato è protetta dall'art. 5, par. 1, primo periodo, la speciale garanzia della libertà della stampa riguarda l'importanza della stampa per la libera formazione delle opinioni individuali e collettive, che va oltre l'esternazione dell'opinione individuale, che l'art. 5, comma 1, vuole garantire", traduzione nostra). Si v. al proposito F. Reimer, *Freiheit der Meinungsäußerung. Eine rechtsvergleichende Perspektive – Deutschland*, in *European Parliament Research Service*, ottobre 2019 (disponibile all'indirizzo: www.europarl.europa.eu/thinktank/de/home.html). Quanto all'art. 21 della Costituzione italiana è in particolare al suo comma quinto che recepisce l'idea di un sistema di informazione (la stampa periodica) di cui disciplina i finanziamenti (v. ancora L. Paladin, *Problemi e vicende della libertà di informazione nell'ordinamento giuridico italiano*, cit., 7). L'art. 10 della CEDU, dopo aver proclamato il diritto alla libertà di espressione, garantisce che in esso

dono più specificamente ai soggetti che per primi esercitano la libertà di informazione (i giornalisti)[17], arrivando ad estendere tale libertà alla dimensione globale del sistema delle telecomunicazioni e del mercato dell'informazione[18].
Questo processo di autonomizzazione della libertà di informazione rispetto alla più generale libertà di manifestazione del pensiero segue, ovviamente, l'evoluzione tecnica che nel corso dei secoli ha fornito nuovi mezzi di comunicazione all'umanità. Come si vedrà, il problema del mezzo – insieme alla discussione sulla titolarità del diritto di cronaca – è centrale nell'analisi della libertà in questione.

3. Il problema del mezzo: Italia, 1973 - Gran Bretagna, 2016

Quando ci si confronta con la libertà di comunicazione, diviene ineludibile il problema del mezzo tramite cui le esternazioni sono veicolate. Si tratta di una questione chiaramente identificata in dottrina[19] e centrale nella misura in cui, da un lato, l'ampliamento dei mezzi comunicativi e l'accesso a questi costituisce una garanzia di esercizio del diritto. Dall'altro lato, l'evoluzione dei mezzi impone di ripensare i limiti alla libertà in parola, poiché il diritto acquisisce una maggiore potenzialità offensiva nei confronti di interessi fondamentali di pari grado, dei singoli e della collettività[20]. Non abbisogna di

si includa «la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive».

[17] L'art. 20 della Costituzione spagnola del 1978, forte anche delle esperienze di altri ordinamenti, riconosce il diritto (comma 1, lett. d) «*a comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades*». L'art. 38 della Costituzione portoghese è ancora più esplicito nei confronti dei giornalisti. In particolare al comma secondo, consacra: «*a) A liberdade de expressão e criação dos jornalistas e colaboradores, bem como a intervenção dos primeiros na orientação editorial dos respetivos órgãos de comunicação social, salvo quando tiverem natureza doutrinária ou confessional; b) O direito dos jornalistas, nos termos da lei, ao acesso às fontes de informação e à proteção da independência e do sigilo profissionais, bem como o direito de elegerem conselhos de redação*».

[18] La Carta dei diritti fondamentali dell'Unione europea riprende, nel suo art. 11, il contenuto della corrispondente disposizione della CEDU. Ad essa aggiunge un secondo comma in cui garantisce il rispetto della «libertà dei media e il loro pluralismo». La scelta del termine *media* è volta a racchiudere l'ampio ventaglio dei mezzi di comunicazione forniti dall'evoluzione tecnologica, che mezzo secolo prima sfuggiva ai redattori della CEDU.

[19] M. Manetti, *La libertà di manifestazione del pensiero*, in R. Nania – P. Ridola (a cura di), *I diritti costituzionali*, II, Torino, 2001, 551: «In relazione a ciascun mezzo cambia infatti sia la quantità di coloro che possono esprimere il pensiero, sia l'ampiezza del pubblico a cui lo stesso pensiero è rivolto, e quindi l'efficacia del messaggio». Similmente M. Michetti, *Disciplina dei «mezzi» e libera manifestazione del pensiero*, in M. Ainis (a cura di), *Informazione Potere Libertà*, Torino, 2005, 309: «I particolari problemi interpretativi che nascono con riguardo all'utilizzazione del "mezzo" e alla sua scelta, invece, concernono tanto i presupposti dell'effettivo esercizio del diritto, quanto quelli dell'efficacia del mezzo stesso. Ogni "mezzo" si caratterizza, infatti, per la capacità di trasmissione dell'atto di libertà compiuto, ma ha in sé una propria vis comunicativa».

[20] A. Pace, *Comunicazioni di massa – Diritto*, in *Enciclopedia delle scienze sociali*, Roma, 1992, § 6: «Qualsiasi trattazione, ancorché rapida e sommaria, degli aspetti giuridici dei mass media non può concludersi senza un accenno alle tecniche generalmente utilizzate per salvaguardare quelli che, con formula generica ma efficace, sono chiamati i 'valori della persona umana'. L'incidenza sui quali - a ben vedere

grandi dimostrazioni l'affermazione per cui la società dell'informazione[21] si fonda sulla possibilità di (quasi) tutti di accedere alla rete Internet e di condividere la più grande varietà di contenuti, con un'evidente ampliamento delle possibilità di esercizio del diritto fondamentale alla libera comunicazione[22], ma con un altrettanto palese rischio per altri diritti che sono messi in pericolo da un uso disinibito degli strumenti informatici e per i regimi delle conseguenti responsabilità[23]. Primo fra tutti ad arrischiare l'immolazione sull'altare delle comunicazioni digitali è, notoriamente, il diritto alla riservatezza della vita privata e al controllo dei propri dati personali (secondo la doppia visione, statica e dinamica, della privacy[24]).

La libertà di informazione, esercitata con i nuovi strumenti digitali, è sicuramente una delle libertà confliggenti con questo diritto e con quelli ad esso più strettamente connessi (es. diritto all'onore e alla reputazione). A questo proposito due pronunce giurisprudenziali – rese in tempi e luoghi diversi – possono perfettamente dimostrare come questa tensione fra diritti (quasi naturale, volendo ben vedere) sia aumentata nel tempo, fino ad assumere connotati drammatici.

Il primo caso è tratto dalla giurisprudenza costituzionale italiana.

Nella sentenza n. 38/1973, la Corte si trovava a giudicare della legittimità costituzionale dell'art. 700 c.p.c. (sulle cosiddette misure cautelari atipiche) messo in relazione ad alcuni articoli della legge n. 633/1941 sul diritto d'autore, rispetto al parametro costituito dall'art. 21, c. 3, Cost. Più nel dettaglio, si discuteva della possibilità per il giudice di ordinare con provvedimento cautelare l'inibitoria all'utilizzo di "scatti rubati", entrati nella disponibilità di un'impresa giornalistica, ma non ancora dati alle stampe. L'utilizzo della norma processuale, infatti, avrebbe costituito una forma surrettizia di sequestro, esondante dai limiti del paradigma costituzionale.

La Corte – evitando di sviluppare in maniera del tutto rigorosa le affermazioni rese pochi anni prima nella sentenza n. 122 del 1970[25], grazie ad una distinzione finemente

- è, per così dire, 'fisiologica' nelle comunicazioni di massa, sia nel momento dell'acquisizione dei dati informativi (fonici, iconici, letterari) necessari per la predisposizione del messaggio, sia nel momento della sua diffusione tra gli utenti».

[21] Dove "informazione", come è noto, ha un significato tecnico diverso dall'oggetto della nostra libertà, rinvenibile nella definizione data dall'art. 1 della direttiva 98/34/CE. La direttiva successiva 2000/31/CE sul commercio elettronico, peraltro, ha ricondotto - «in numerosi casi» - la "libera circolazione dei servizi della società dell'informazione" alla libertà di espressione prevista dall'art. 10 CEDU (cfr. considerando 9 della direttiva).

[22] V. supra, nota 12.

[23] V., per tutti, G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *questa Rivista*, 1, 2018, 19 ss., e F. Donati, Fake news *e libertà di informazione*, in *questa Rivista*, 2, 2018, 440 ss.

[24] S. Rodotà, *Riservatezza*, in *Enciclopedia Italiana*, VI Appendice, Roma, 2000.

[25] Nella sentenza del 1970, infatti, il giudice costituzionale aveva da un lato riconosciuto che: «quando la stampa viene in considerazione come strumento di diffusione del pensiero - presupposto che discende dalla già rilevata connessione fra libertà di stampa e libertà di pensiero -, la norma contenuta nel terzo comma dell'art. 21 della Costituzione copre l'intera area del sequestro, qualunque sia il contrapposto interesse col quale la stampa entra in collisione. In altri termini, il fatto che la Costituzione ammetta il sequestro preventivo solo "nel caso di delitti per i quali la legge sulla stampa espressamente lo autorizzi" o "nel caso di violazione di norme che la legge stessa prescriva per l'indicazione dei responsabili" non può non escludere la legittimità di tale misura in ogni altro caso» (sentenza n. 122 del 1970, § 3 del *considerato in diritto*). Tuttavia «ciò non significa che al di fuori delle predette ipotesi la libertà di stampa non conosca confini. Per il già richiamato carattere di strumentalità, essa soggiace agli stessi limiti che

operata[26] – affermò che l'inibitoria pronunciata *ex* art. 700 c.p.c. fosse pienamente compatibile con la Costituzione e, anzi, un efficace strumento di tutela provvisoria per fondamentali diritti della personalità del soggetto illegittimamente ritratto e delle persone a lui più prossime[27].

Oltre quarant'anni dopo, un caso non dissimile veniva portato innanzi alla Corte Suprema del Regno Unito[28].

Ai *Lord Justices* veniva richiesta una *anonymised interim injunction* sulla base dello *Human Rights Act* del 1998[29] affinché venisse fermata la diffusione, tramite il sito internet di un quotidiano, di una notizia di cronaca rosa attinente alle infedeltà amorose di un celebre personaggio, notizia scandalistica che avrebbe recato grave danno alla sua famiglia, in particolare ai suoi figli minori.

La Corte, nella veste di massimo consesso giurisdizionale per l'Inghilterra e il Galles, accedeva alla domanda del ricorrente garantendo l'inibitoria richiesta e pare qui opportuno riportare alcuni passaggi dell'opinione di maggioranza data dal *justice* Lord

circoscrivono la libertà di manifestazione del pensiero. Ma si tratta di limiti che vanno ricercati in sede di interpretazione del primo comma dell'articolo 21: il terzo comma, che disciplina la diversa materia della misura cautelare del sequestro, deve essere interpretato nel senso che non tutte le violazioni di siffatti limiti possono legittimare il ricorso a tale misura. Per garantire la diffusione della stampa, che potrebbe essere compromessa o addirittura definitivamente pregiudicata da provvedimenti che, ancorché adottati dall'autorità giudiziaria, si basano su una cognizione sommaria e possono poi risultare ingiustificati in sede di accertamento definitivo, la Costituzione, tenendo conto della importanza del ruolo della stampa in un regime democratico, ha disciplinato il conflitto fra l'interesse al sequestro e l'interesse alla circolazione della stampa: la norma costituzionale di raffronto, mentre consente al legislatore ordinario di dar prevalenza al primo (purché attraverso un'espressa previsione) nel caso di delitti, direttamente stabilisce la prevalenza del secondo in ogni altra ipotesi.». In conclusione il giudice aveva ritenuto che il sequestro fosse ammissibile solo quando la pubblicazione delle immagini integrasse gli estremi dei sequestri. Dando quindi un'interpretazione costituzionalmente orientata dell'art. 700 c.p.c. la Corte concludeva nel senso che «il giudice, nonostante l'ampia discrezionalità attribuitagli, non può trovare nel predetto articolo la fonte di un potere che, per le cose innanzi dette, il terzo comma dell'art. 21 gli preclude. Si può perciò concludere che, poiché la disposizione denunziata, se correttamente interpretata, non è in contrasto con la norma costituzionale di raffronto, la questione, anche in questa parte, deve essere dichiarata non fondata» (§ 5 del *considerato in diritto*).

[26] Nella sentenza del 1973, difatti, si sottolinea che il materiale non era ancora stato pubblicato (e dunque si autorizza l'inibitoria), mentre nel 1970 l'art. 700 c.p.c. era diretto verso stampati già messi in circolazione.

[27] Sentenza n. 38/1973, cit., § 5 del *considerato in diritto*: «L'applicazione in tali casi dell'art. 700 cod. proc. civ. ai fini di proteggere il diritto alla riservatezza e di evitare pregiudizi imminenti e irreparabili al decoro e alla reputazione degli interessati e dei loro congiunti, mentre non può identificarsi con l'esercizio di un'attività di censura, costituisce un mezzo efficace per attuare la protezione provvisoria di diritti della personalità rientranti in quelli inviolabili che la Costituzione salvaguarda, tenuto anche conto della estrema importanza di tali diritti, della gravità e dell'irreversibilità del danno che la violazione di essi arreca agli interessati e che può incidere irrimediabilmente sulla loro posizione sociale e su quella dei loro congiunti, dell'impossibilità di ripararlo adeguatamente, dell'esigenza di un pronto intervento per impedire che il pregiudizio si verifichi».

[28] Si tratta del caso [2016] UKSC 26, *PJS v News Group Newspapers Ltd.*

[29] Si tratta sostanzialmente di un'inibitoria cautelare anticipata, adottata sulla base della Sec. 12, n. 3 dello *Human Rights Act 1998*: «*No such relief is to be granted so as to restrain publication before trial unless the court is satisfied that the applicant is likely to establish that publication should not be allowed*». Sul tema della libertà di espressione nel Regno Unito dopo l'approvazione dello Human Rights Act 1998 v. E. Barendt, *Freedom of Expression in the United Kingdom Under the Human Rights Act 1998*, in *Indiana Law Journal*, 3, 2009, 851 ss. (852 per una comparazione fra la *freedom of expression* di derivazione convenzionale e il *free speech* tutelato dal *common law*).

Mance, ma anche di alcune significative obiezioni avanzate nella *dissenting opinion* di Lord Toulson.

L'opinione di maggioranza evidenza l'illecita e grave intrusione nella vita privata del ricorrente, che legittima il ricorso ad una misura cautelare anticipatoria per limitare la libertà del tabloid e impedire di continuare a divulgare la notizia. Fra i vari punti di interesse, occorre segnalare che la Corte Suprema scarta l'argomento dell'interesse pubblico alla notizia, sottolineando che esso – nel suo significato giuridico – non sussiste[30]. Sottolinea poi l'obbligo di assicurare al ricorrente leso un rimedio effettivo, pur nel convulso sistema delle comunicazioni digitali e via Internet, anche a costo di apparire come una Corte reazionaria, poiché il rifiuto dell'ingiunzione condurrebbe ad un ancor più grave violazione dei diritti da proteggere[31].

La *dissenting opinion* di Lord Toulson si appunta esattamente, e suggestivamente, sul tema della comunicazione digitale. Il magistrato osserva, infatti, che l'ingiunzione avrebbe valore solo per il Galles e l'Inghilterra, permettendo dunque a soggetti esterni alle due giurisdizioni di continuare a divulgare l'informazione. Ma poi, e in maniera assorbente, l'inibitoria richiesta sarebbe ormai tardiva: la notizia è già diventata di dominio pubblico e, dunque, la costrizione della libertà di informazione apparirebbe come retroattiva, ma solo di apparenza appunto si tratterebbe[32]. Dunque, la misura cautelare prevista dalla legge avrebbe senso e comporterebbe un ammissibile sacrificio per la libertà di informazione solo ove la notizia non avesse già avuto diffusione nel pubblico[33].

Ora, senza aderire all'opinione di Lord Toulson, è evidente che si tratta di considerazioni di grandissimo peso: come si può pensare di fermare un'informazione, se questa è ormai caduta nel *mare magnum* di Internet e magari migliaia di persone se ne sono appropriate salvandola su dischi fissi in qualunque parte del globo? Conseguentemente, come si può garantire una tutela alla persona che vede la propria storia e la propria vita "date in pasto" alla curiosità del mondo intero?

---

30 *Lord Mance's Opinion*, § 21: «*criticism of conduct cannot be a pretext for invasion of privacy by disclosure of alleged sexual infidelity which is of no real public interest in a legal sense*».

31 Ivi, § 45: «*the only consideration militating in favour of discharging the injunction is the incongruity of the parallel - and in probability significantly uncontrollable - world of the internet and social media, which may make further inroads into the protection intended by the injunction. Against that, however, the media storm which discharge of the injunction would unleash would add a different and in some respects more enduring dimension to the existing invasions of privacy being perpetrated on the internet. At the risk of appearing irredentist, the Supreme Court has come to the conclusion that, on a trial in the light of the present evidence, a permanent injunction would be likely to be granted in the interests of the appellant, his partner and especially their children*».

32 *Lord Toulson's Opinion*, § 86: «*In the world in which PJS lives, knowledge of the story must be commonplace and it is apparent from the evidence that the circle of those who know is much wider. The story in its essential details has been published in a major Scottish newspaper, it has been widely accessible on websites and twitter, and anyone who seriously wanted to know PJS's identity will have had ways of finding it. Confidentiality in a meaningful sense can survive a certain amount of leakage, and every case must be decided on its own facts, but in this case I have reached a clear view that the story's confidentiality has become so porous that the idea of it still remaining secret in a meaningful sense is illusory. Once it has become readily available to anyone who wants to know it, it has lost the essence of confidentiality. The court must live in the world as it is and not as it would like it to be. [...]. In my judgment that is good sense and good law.*».

33 Ivi, § 89: «*The evident underlying purpose of the subsection is to discourage the granting of an injunction to prevent publication of information which is already widely known. If the information is in wide, general circulation from whatever source or combination of sources, I do not see that it should make a significant difference whether the medium of the intended publication is the internet, print journalism or broadcast journalism. The world of public information is interactive and indivisible*».

La distanza temporale fra la pronuncia italiana e quella inglese mette in luce la drammaticità del quesito: se negli anni '70 il giudice ordinario italiano aveva il tempo materiale non solo per fermare la pubblicazione, ma addirittura per sollevare la questione di costituzionalità, nel 2016 il giudice britannico si domanda se ha ancora senso un suo intervento, che risulterebbe sempre e comunque tardivo rispetto alla velocità di diffusione dell'informazione.

La chiosa adesiva del *Chief Justice* Lord Neunberg è, però, istruttiva e risuona come un monito: i giudici non possono rinunciare a garantire una tutela a chi vede violati i propri diritti, anche laddove questa tutela appaia complessa, magari inutile e possa essere pesantemente criticata in taluni *milieux*[34]. E, salvo che i legislatori non provino ad intervenire per reprimere gli abusi (con la somma difficoltà che presenta il bilanciamento in astratto fra diritti fondamentali rivali), spetta proprio ai giudici dare una risposta ai casi concreti, utilizzando gli strumenti a loro disposizione, e creare nuovi standard di giudizio compatibili con la realtà sociale[35]. Se vi rinunciassero, l'evoluzione tecnologica dei mezzi renderebbe sostanzialmente illimitata e illimitabile la libertà di informazione, a discapito degli altri beni di rilievo costituzionale. E ciò tanto più dal momento in cui non esistono più solo fonti limitate di un'informazione "qualificata", ma ciascun utente di Internet può trasformarsi, in qualunque momento, in un giornalista.

4. Una libertà adespota? La sentenza *Sergejs Buivids* della CGUE (C-345/17) e il giornalismo diffuso

Nel 2019 la Corte di Giustizia dell'Unione Europea (CGUE) ha reso una sentenza – in realtà passata quasi inosservata dalla dottrina[36] – di assoluta rilevanza per il nostro tema. La decisione *Sergejs Buivids* del 14 febbraio 2019 (C-345/17) risponde a una questione pregiudiziale posta dalla Corte Suprema della Lettonia e si segnala (a) perché mostra la scissione fra libertà di informazione e libertà di opinione, che le piattaforme web rendono oggi (all'apparenza, paradossalmente) più definita; (b) perché mette in bilanciamento il diritto di informare con il diritto alla protezione dei dati personali; (c) perché tratta, anche se in maniera discutibile, della problematica individuazione dei titolari della libertà di informazione.

Il caso era il seguente: un cittadino lettone, Sergejs Buivids, veniva fermato dalla polizia e condotto in una caserma per degli accertamenti e per rendere una deposizione. Qui veniva trattenuto per alcune ore e, durante questo tempo, Buivids filmava l'interno

[34] *Lord Neuberger's Opinion*, § 71: «*The courts exist to protect legal rights, even when their protection is difficult or unpopular in some quarters. And if Parliament takes the view that the courts have not adapted the law to fit current realities, then, of course, it can change the law*».

[35] Ivi, § 70: «*the internet and other electronic developments are likely to change our perceptions of privacy as well as other matters - and may already be doing so. The courts must of course be ready to consider changing their approach when it is clear that that approach has become unrealistic in practical terms or out of touch with the standards of contemporary society. However, we should not change our approach before it is reasonably clear that things have relevantly changed in a significant and long-term way*».

[36] Per una nota a prima lettura: v. D. Erdos, *European Data Protection and Freedom of Expression After Buivids: An Increasingly Significant Tension*, in *European Law Blog*, 21 febbraio 2019.

della caserma e alcuni scambi con gli agenti; una volta rilasciato, il video veniva caricato sulla piattaforma YouTube, sollevando così la protesta dei poliziotti ritratti nei fotogrammi e una loro conseguente azione davanti all'Agenzia lettone per la tutela dei dati personali. La decisione, a seguito di vari ricorsi amministrativi, giungeva infine alla Corte Suprema che investiva la Corte di Lussemburgo di due questioni pregiudiziali concernenti gli articoli 3 e 9 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 (oggi, come noto, sostituita dal Regolamento (UE) 2016/679, conosciuto come *General Data Protection Regulation* – GDPR).
La prima risposta che arriva dalla CGUE attiene alla nozione di dato personale e di trattamento. La Corte riconosce, in effetti, che la pubblicazione del video sulla piattaforma online, dove è possibile vedere distintamente le figure degli agenti di polizia, costituisce un trattamento dei dati, posto che l'immagine della persona è in sé un dato personale.
In secondo luogo, la Corte afferma che la finalità giornalistica del trattamento dei dati – che avrebbe reso lecito il trattamento stesso, in deroga alle restanti previsioni – non poteva essere esclusa dalla circostanza che Buivids non fosse un giornalista professionista. Assegnava dunque al giudice del rinvio il compito di verificare se l'unica finalità del trattamento, nel caso concreto, fosse la divulgazione al pubblico di informazioni, opinioni o idee.

(a) Come anticipato, il primo profilo d'interesse riguarda la posizione reciproca fra libertà di informazione e libertà d'espressione. In realtà, facendo applicazione dell'art. 11 della Carta di Nizza, la Corte non individua partitamente la libertà di informazione, la quale, in realtà, avrebbe nella Carta una posizione distinta dalla libertà di opinione, nel più ampio quadro della libertà di espressione. Tuttavia, il caso di specie dimostra come l'evoluzione tecnologica renda quanto meno più riconoscibile il *diritto di cronaca* dal – va ribadito: collegato, ancorché diverso – *diritto di critica*. La pubblicazione di un video su un qualunque *social*, a documentazione di fatti che hanno visto l'autore come protagonista o come testimone diretto, sicuramente costituisce esercizio del primo diritto, ma non necessariamente del secondo. Certo, non può escludersi che la critica sia implicita nella pubblicazione stessa – così pareva nel caso di Buivids – o che tale pubblicazione miri proprio a generare una critica da parte di coloro che ne prendono visione. Però, nel momento in cui viene condivisa con il pubblico solo una serie di "freddi" fotogrammi, in assenza di qualsivoglia commento, è chiaro che la libertà di informazione viene esercitata in maniera autonoma e, altrettanto autonomamente, va valutata rispetto ai suoi limiti o eccessi.

(b) Uno di questi limiti potrebbe essere rappresentato proprio dalla protezione dei dati personali. In tale ambito, però, la normativa europea racchiusa nel GDPR prevede delle importanti eccezioni, venute a confermare quanto già previsto dalla direttiva 95/46/CE interpretata dalla Corte.
Il considerando 153 del GDPR richiama gli Stati ad una conciliazione fra la tutela dei dati personali e l'esercizio – qui distinto – delle libertà di informazione e della libertà

di espressione[37]. L'art. 17 esclude l'applicabilità del diritto alla cancellazione per i trattamenti necessari all'esercizio della libertà di espressione ed informazione[38]. Infine, l'art. 85 dello stesso Regolamento positivizza quindi l'*obbligo* per gli Stati di prevedere deroghe per favorire il trattamento dei dati a scopi giornalistici[39].

Rispetto alla normativa in vigore dal 1995, però, si rileva una modifica di non poco conto: l'art. 9 della direttiva, infatti, si riferiva ad esenzioni e deroghe per trattamenti realizzati «*esclusivamente* per scopi giornalistici o di espressione artistica e letteraria». La venuta meno dell'avverbio enfatizzato non è affatto priva di conseguenze, soprattutto tenuto conto del consistente incremento delle tecnologie digitali dal 1995 ad oggi: il GDPR – pur rinviando agli Stati – consente che godano di una garanzia implicita dell'attività giornalistica (e dunque della protezione massima riconoscibile alla libertà di informazione) tutti quei trattamenti di dati aventi una finalità ibrida, che qualunque utente di Internet può potenzialmente mettere in atto, come si è detto. Tale conclusione è corroborata anche dalla frase finale del considerando 153, che invita gli Stati ad «interpretare in modo esteso i concetti relativi a detta libertà, quali la nozione di giornalismo». E ciò – non si può nascondere – anche per uscire dall'imbarazzo di dover definire, volta per volta, il reale intento del titolare del trattamento[40]. Restando

[37] GDPR, considerando 153: «Il diritto degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali ai sensi del presente regolamento. Il trattamento dei dati personali effettuato unicamente a scopi giornalistici o di espressione accademica, artistica o letteraria dovrebbe essere soggetto a deroghe o esenzioni rispetto ad alcune disposizioni del presente regolamento se necessario per conciliare il diritto alla protezione dei dati personali e il diritto alla libertà d'espressione e di informazione sancito nell'articolo 11 della Carta. Ciò dovrebbe applicarsi in particolare al trattamento dei dati personali nel settore audiovisivo, negli archivi stampa e nelle emeroteche. È pertanto opportuno che gli Stati adottino misure legislative che prevedano le deroghe e le esenzioni necessarie ai fini di un equilibrio tra tali diritti fondamentali. Gli Stati membri dovrebbero adottare tali esenzioni e deroghe con riferimento alle disposizioni riguardanti i principi generali, i diritti dell'interessato, il titolare del trattamento e il responsabile del trattamento, il trasferimento di dati personali verso paesi terzi o a organizzazioni internazionali, le autorità di controllo indipendenti, la cooperazione e la coerenza nonché situazioni di trattamento dei dati specifiche. Qualora tali esenzioni o deroghe differiscano da uno Stato membro all'altro, dovrebbe applicarsi il diritto dello Stato membro cui è soggetto il titolare del trattamento. Per tenere conto dell'importanza del diritto alla libertà di espressione in tutte le società democratiche è necessario interpretare in modo esteso i concetti relativi a detta libertà, quali la nozione di giornalismo».

[38] Art. 17, par. 3: «I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione».

[39] Art. 85 (Trattamento e libertà di informazione ed espressione): «1. Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria. 2. Ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono esenzioni o deroghe rispetto ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione. 3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 2 e comunica senza ritardo ogni successiva modifica». Sul tema v. D. Erdos, *Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication*, in *Computer Law and Security Review*, 3, 2017, 275 ss.

[40] A seguito dell'entrata in vigore del GDPR, il Garante per la tutela dei dati personali ha aggiornato le

all'esempio di Buivids, come si può concretamente distinguere (anche se tale operazione è in effetti richiesta al giudice del rinvio, dovendo egli applicare la direttiva del 1995) se un video è pubblicato a scopi di pura informazione del pubblico o con finalità "revanscistiche" dettate dal fastidio provocato da un trattenimento in caserma per un lungo lasso di tempo?

(c) Se questa è la tendenza del legislatore europeo, essa solleva nondimeno alcune perplessità in ordine all'estensione *erga omnes* dell'attività giornalistica, arrivando quindi al *punctum dolens*: grazie ai *social*, siamo tutti giornalisti? Godiamo tutti del medesimo livello di tutela rispetto al diritto di informare gli altri?
Certo, si potrebbe obiettare che l'estensione non è generale, ma vale solo *ratione materiae,* poiché l'Unione Europea legiferava nella materia dei dati personali. Ma è un'obiezione, in realtà, estremamente fragile: sappiamo bene che al giorno d'oggi, praticamente, qualunque attività di comunicazione che passi dal web realizza un trattamento di dati personali e dunque questo ampliamento non è destinato a rimanere relegato in un settore specifico, ma investirà tutto l'ordinamento nel suo complesso, poiché tocca la stragrande maggioranza delle attività che nell'ordinamento si realizzano, determinandone l'(il)liceità.
S'impone ora una precisazione: non si vuole qui sostenere che la libertà di informazione sia appannaggio dei soli giornalisti. Anche prima del dilagare di Internet esistevano vari strumenti con i quali semplici cittadini potevano portare all'attenzione dei consociati fatti di interesse pubblico, sia in forma immediata (si pensi al volantinaggio), sia in forma mediata (emblematiche le rubriche dedicate alle "lettere al direttore" presenti in moltissime testate).
Resta però il fatto che la professione giornalistica gode di una serie di garanzie assai considerevoli, che la rendono di per sé inidonea a considerarsi un'attività liberamente praticabile, tant'è vero che alcune giurisdizioni costituzionali parlano di un vero e proprio "privilegio del giornalista"[41]. Si pensi, oltre all'estensione maggiore del diritto di cronaca e di opinione (molte volte sancita dalla Corte di Strasburgo[42]) all'organizzazione come professione protetta[43]; al segreto sulle fonti[44] (che riverbera in un vero e pro-

Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica con deliberazione del 19 novembre 2018. All'art. 1 si legge che, in forza dell'art. 21 Cost., i trattamenti posti in essere nell'ambito dell'attività giornalistica «si differenziano nettamente per la loro natura dalla memorizzazione e dal trattamento di dati personali ad opera di banche dati o altri soggetti».

[41] È il caso della Corte Suprema Israeliana, tornata di recente ad evocarlo rispetto ai controlli anti-COVID, che avrebbero potuto condurre ad una violazione del regime di confidenzialità dell'attività di ricerca delle informazioni da parte dei giornalisti: v. *Ben Meir v. Prime Minister* (HCJ 2109/20) (disponibile in inglese nella banca dati *versa.cardozo.yu.edu*). Al p§ 45, la Presidente Hayut ribadisce: «*One cannot overstate the importance of freedom of the press in a democratic state, and preserving this principle is of particular importance during a national crisis of the type we are currently experiencing*».

[42] Si v. le sentenze *Cumpănă e Mazăre c. Romania* (2004), *Belpietro c. Italia* (2013), *Sallusti c. Italia* (2019).

[43] V. M. Cuniberti, *La professione del giornalista*, in G.E. Vigevani – O. Pollicino – C. Melzi d'Eril – M. Cuniberti – M. Bassini, *Diritto dell'informazione e dei media*, Torino, 2019, 263 ss. Per una disamina dei vari profili concernenti l'attività giornalistica v. M. Pedrazza Gorlero, *Giornalismo e costituzione*, Padova, 1988. L'A. dubita dei limiti posti dalla legge all'esercizio della professione giornalistica, ivi inclusa l'esistenza dello stesso ordine professionale (171 ss.), viceversa ritenuta legittima da parte della Corte costituzionale

[44] Si v. già l'art. 2 della legge 29 luglio 1881 *sur la liberté de la presse*: «*Le secret des sources des journalistes est*

prio segreto professionale, fino a divenire, in alcuni ordinamenti, una protezione rafforzata della libertà personale rispetto a perquisizioni ed indagini penali[45]); alla clausola di coscienza che attribuisce al giornalista un particolare potere di recesso dal contratto di lavoro ove muti la proprietà della testata da cui dipende e dunque l'indirizzo della stessa attività di informazione[46]; alle maggiori possibilità di accesso in determinati luoghi per ricercare l'informazione (es. un carcere)[47]. E questi benefici non sono attribuiti come prerogative fini a sé stesse, ma discendono direttamente dal diritto ad informare e ad essere informati, costituendo quindi una garanzia riflessa del diritto passivo all'informazione per tutti i consociati.

Parallelamente, in capo ai giornalisti gravano responsabilità non solo di carattere deontologico, morale e/o (*latu sensu*) politico, ma peculiari responsabilità di stampo penale per i reati compiuti nell'esercizio della loro attività.

Proprio quest'ultimo tema si è recentemente posto all'attenzione della Corte costituzionale italiana.

5. La necessità di cercare nuovi bilanciamenti: l'ordinanza n. 132 del 2020 della Corte costituzionale italiana

Nel giugno 2020 la Corte costituzionale ha reso un'interessante ordinanza (n. 132) con la quale differiva di un anno la decisione su una questione di legittimità sollevata dai Tribunali di Salerno e Bari sugli articoli 13 della legge sulla stampa (l. 8 febbraio 1948 n. 47) e 595, c. 3, c.p. I giudici *a quibus* dubitavano che la pena detentiva comminata ai giornalisti per la diffamazione a mezzo stampa fosse compatibile con l'ordinamento costituzionale multilivello. In particolare, svariate pronunce della Corte Europea dei Diritti dell'Uomo[48] hanno ritenuto non conforme al diritto convenzionale la previsione della detenzione per i giornalisti condannati per il reato di diffamazione a mezzo stampa.

L'ordinanza della Corte riconosce che il diritto italiano stride con l'ormai consolidata giurisprudenza di Strasburgo e dunque, ricorrendo al "metodo Cappato", assegna un anno di tempo al legislatore prima di decidere definitivamente la questione. Ovviamente, la nuova tecnica attendista della Corte ha suscitato le attenzioni primarie della dottrina costituzionalistica, mentre il profilo sostanziale aveva già sollecitato in maniera

protégé dans l'exercice de leur mission d'information du public».

45 L'art. 56-2 del *Code de procédure pénale* francese prevede che le perquisizioni in locali di imprese giornalistiche o di comunicazione possano essere condotti solo dai magistrati personalmente.

46 Che la Costituzione spagnola eleva a vero e proprio diritto costituzionale: v. nota 17.

47 Si v. quanto statuito dal *Tribunal Constitucional* spagnolo nella sentenza n. 6/2020 a proposito dei colloqui di detenuti con cronisti (comunicazioni limitabili solo in presenza di gravissimi motivi, poiché «*las libertades de expresión e información gozan de una protección preferente, forman parte del derecho a la sana crítica a las instituciones y funcionarios públicos, los cuales han de soportarla en el contexto de una sociedad democrática*».

48 *Ricci c. Italia* (2013), *Belpietro c. Italia* (2013), *Sallusti c. Italia* (2019), su cui v. la ricostruzione di M. Cuniberti, *La pena detentiva per la diffamazione tra Corte costituzionale e Corte europea dei diritti dell'uomo: l'ordinanza della Corte costituzionale n.132 del 2020*, in *Osservatorio AIC*, 2, 2020, 121 ss.

maggiore gli studiosi del diritto penale in passato[49].

Per quanto riguarda il nostro tema, il giudice italiano – in realtà – sembra quasi voler ottemperare *obtorto collo* alle indicazioni della giurisprudenza sovranazionale e, del resto, si dimostra molto più attento di quest'ultima nell'enucleare i molteplici problemi che attorniano la definizione della responsabilità penale dei giornalisti e delle conseguenti pene[50]. La Corte EDU, infatti, si limita generalmente a richiamare "casi eccezionali" che possono giustificare la comminazione della pena detentiva a carico dei giornalisti, riferendosi principalmente alle forme di discorsi d'odio, che come tali costituiscono i soli reati d'opinione ammessi nel sistema convenzionale.

Tuttavia, la giurisprudenza *strasbourgeoise* pecca, a ben vedere, di eccessiva semplificazione.

Bisogna innanzitutto ricordare che la CEDU ammette tutte quelle restrizioni alla libertà di espressione che siano «necessarie, *in una società democratica*» alla preservazione di vari beni indicati dall'art. 10. Orbene, la Corte EDU in questa materia rifiuta di verificare se, nell'ordinamento che di volta in volta viene in rilievo, la libertà d'informazione dei giornalisti trovi una sufficiente garanzia. Ovvero, detto diversamente, non si cura che l'ordinamento presenti sufficienti caratteri di democraticità da non sollevare il sospetto che la pena detentiva serva ad "imbavagliare" la stampa. Il che, da un lato, è evidentemente irragionevole, dato che, come è noto e senza bisogno di citare specifici esempi, la Corte giudica Stati molto diversi fra loro in tema di garanzie dei diritti costituzionali (*anche* dei giornalisti). Dall'altro lato, mostra l'incongruenza di un sistema giurisdizionale estremamente casistico e frastagliato[51], che in altre materie (in particolare nella tutela dei diritti politici) sceglie invece di nascondersi proprio dietro alla "solidità democratica" di uno Stato parte (si fa qui riferimento alla sentenza *Saccomanno c. Italia*, peraltro poi sconfessata dalla Corte costituzionale del nostro Paese[52]) proprio per riconoscere il

[49] Cfr. V. Pacileo, *Contro la decriminalizzazione della diffamazione a mezzo stampa. Note a margine del "caso Sallusti"*, in *Diritto penale contemporaneo*, 16 maggio 2013. Favorevole agli indirizzi della Corte EDU invece A. Gullo, *Diffamazione e pena detentiva*, in *Diritto penale contemporaneo*, 13 marzo 2016.

[50] § 7.3 del *considerato in diritto*: «Il punto di equilibrio tra la libertà di "informare" e di "formare" la pubblica opinione svolto dalla stampa e dai media, da un lato, e la tutela della reputazione individuale, dall'altro, non può però essere pensato come fisso e immutabile, essendo soggetto a necessari assestamenti, tanto più alla luce della rapida evoluzione della tecnologia e dei mezzi di comunicazione verificatasi negli ultimi decenni. […] Ciò esige una rimodulazione del bilanciamento sotteso alla disciplina in questa sede censurata, in modo da coniugare le esigenze di garanzia della libertà giornalistica, nel senso ora precisato, con le altrettanto pressanti ragioni di tutela effettiva della reputazione individuale delle vittime di eventuali abusi di quella libertà da parte dei giornalisti; vittime che sono oggi esposte a rischi ancora maggiori che nel passato. Basti pensare, in proposito, agli effetti di rapidissima e duratura amplificazione degli addebiti diffamatori determinata dai *social networks* e dai motori di ricerca in internet, il cui carattere lesivo per la vittima – in termini di sofferenza psicologica e di concreti pregiudizi alla propria vita privata, familiare, sociale, professionale, politica – e per tutte le persone a essa affettivamente legate risulta grandemente potenziato rispetto a quanto accadeva anche solo in un recente passato».

[51] Si ricorderà la sentenza della Corte costituzionale n. 49/2015, che non nascondeva una (seppur garbata) critica alla costruzione della giurisprudenza di Strasburgo, arrivando ad escludere che i giudici italiani dovessero fare immediata applicazione dei principi da questa ricavabili. Sulla sentenza v. la critica di F. Viganò, *La Consulta e la tela di Penelope*, in *Diritto penale contemporaneo*, 2, 2015, 334 ss.; in senso adesivo M. Bignami, *Le gemelle crescono in salute: la confisca urbanistica tra Costituzione, CEDU e diritto vivente*, in *Diritto penale contemporaneo*, 2, 2015, 288 ss.

[52] Il caso *Saccomanno c. Italia* (2012) verteva sul rispetto, da parte della legge elettorale italiana allora vigente (n. 270/2005, il c.d. *Porcellum*) rispetto all'art. 3 del Protocollo n. 1 (diritto di partecipare a

celebre "margine di discrezionalità" che manda gli Stati esenti da responsabilità.
Forse, allora, la Corte costituzionale italiana avrebbe anche potuto trovare un maggiore agio per non assecondare *in toto* la giurisprudenza di Strasburgo ed eventualmente intervenire in maniera diretta, ma puntuale, sulle norme impugnate.
Ha scelto la strada – che, non a torto, è stata definita preoccupante[53] – di concedere al legislatore dodici mesi per intervenire sulla disciplina attualmente vigente. Coscienziosamente, però, lo ha fatto indicando una serie di problemi – a Strasburgo ancora non valorizzati – che al giorno d'oggi si pongono e ci riportano al cuore del nostro tema.
L'informazione errata e diffamatoria, oltre a poter essere messa in circolo da chiunque oramai e non solo più dai giornalisti, ha una capacità lesiva dei diritti della persona estremamente amplificata rispetto a non molti anni fa: lo ha ricordato anche la *Supreme Court* britannica nel caso *PJS*. Le notizie viaggiano senza più alcuna barriera spazio-temporale e incidono profondamente nella vita dei singoli, per i quali il noto diritto all'oblio può costituire solo un magro ristoro *a posteriori*[54].
Ma, ancora, non è solo il versante meramente orizzontale che deve essere tenuto in considerazione. Come ben dice l'ordinanza n. 132, il compito dei giornalisti è "in-formare la pubblica opinione"[55]: grava sugli organi di stampa una responsabilità pubblica, coessenziale alla democrazia, che la rende un enorme potere di fatto (il noto "quarto potere"[56]). Dunque, malgrado il fatto che anche comuni cittadini godano di mezzi amplificati per trasmettere opinioni e comunicare fatti di cronaca ai consociati, è comunque al giornalismo professionista che si guarda per un "di più" nella qualità e nella funzione dell'informazione.
Anche alla luce di questa considerazione, in un ordinamento democratico stabilito, forte di un potere giudiziario indipendente ed autonomo, la narrazione del "giornalista perseguitato" (su cui sostanzialmente si basa la giurisprudenza della Corte EDU) va ridimensionata e riportata alla sua cornice fondamentale. L'art. 21 della Costituzione italiana, in maniera del tutto pragmatica, fa diretto riferimento ai delitti a mezzo stam-

elezioni che garantiscono la libera espressione dell'opinione del popolo sulla scelta del corpo legislativo. La Corte EDU aveva valorizzato in particolare il ruolo dei partiti politici negli ordinamenti democratici (§§ 60 ss.). Come noto, la Corte costituzionale italiana, con la sent. 1/2014, ha ritenuto che il sistema elettorale così congegnato ferisse l'essenza stessa della rappresentanza.

53 D. Casanova, *L'ordinanza n. 132 del 2020 sulla pena detentiva per il reato di diffamazione mezzo stampa: un altro (preoccupante) rinvio della decisione da parte del Giudice costituzionale*, in *ConsultaOnline*, 2, 2020, 635 La preoccupazione sta nel fatto che, così facendo, emerge «il ritratto di una Corte costituzionale che attraverso dei procedimenti creativi enfatizza, probabilmente oltre il ragionevole, la propria anima politica».

54 Sul rapporto fra libertà di informazione e diritto all'oblio v. M. Frau, *La pluridimensionalità del diritto all'oblio e il problema del bilanciamento con la libertà di informazione*, in G. Ferri (a cura di), *La democrazia costituzionale tra nuovi diritti e deriva mediale*, Napoli, 2015, 374: «la libertà di informazione attiva e passiva subisce un progressivo affievolimento in relazione al fattore temporale, lo stesso fattore da cui, con un processo inverso, trae linfa vitale il diritto all'oblio».

55 J. Rivero, *Il regime giuridico dell'informazione in Francia*, cit., 66 esclude, invece, dal campo della libertà di informazione «le attività e le istituzioni che hanno una finalità essenzialmente culturale, quali l'insegnamento, il quale, anche se per caso informa, cerca anzitutto di *formare*» (enfasi dell'A.).

56 La formula evolve da un discorso di Edmund Burke nella Camera dei Comuni che, rivolto verso i giornalisti a cui si dava accesso per la prima volta all'aula come cronisti parlamentari avrebbe detto: "Voi siete il quarto Stato!": cfr. J. Schultz, *Reviving the fourth estate: democracy, accountability and the media*, Cambridge, 1998, 49.

pa, che fondano la possibilità di procedere al sequestro degli stampati (comma terzo), fermo peraltro il più generale divieto delle manifestazioni contrarie al buon costume e il potere-dovere legislativo di reprimere queste violazioni (ultimo comma).
La previsione di una pena detentiva, allora, non è un residuo autoritario, ma è un ulteriore strumento di garanzia affinché chi è investito di un grande potere (ribadiamolo: oggi ancor più considerevole) non ne abusi. E l'argomento, caro alla giurisprudenza sovranazionale, che la minaccia della detenzione inibirebbe l'esercizio della libertà da parte del giornalista è poco consistente: il diritto penale non esiste solo per punire *a posteriori*, ma anche per frenare *a priori* – grazie alla minaccia della sanzione – condotte che attentino a beni giuridici fondamentali[57].
Certo, resta poi doveroso che il giudice possa ponderare le circostanze concrete e la gravità dei fatti nell'irrogare la pena ed è sicuramente facoltà del legislatore introdurre la sola pena pecuniaria, non costituendo la detenzione una scelta costituzionalmente obbligata. Con ciò, però, si compie un'opzione di politica criminale che – al di là dell'afflittività della multa o dell'ammenda, che può non essere affatto banale – indubbiamente tende a derubricare tutti gli altri beni confliggenti con la libertà di informazione, ivi potenzialmente inclusi il diritto a ricevere informazioni veritiere e la "pubblica fede" che i consociati ripongono nell'attività giornalistica, tramite la sottrazione del crimine in questione dall'ambito di applicazione della pena più grave prevista dall'ordinamento. Del pari, non è detto che l'individuazione dei "casi eccezionali" che giustificano la detenzione debba fermarsi al solo *hate speech*: che ne è, ad esempio, della dolosa diffusione di notizie diffamatorie in periodo elettorale al solo fine di indirizzare gli orientamenti degli elettori, attentando così alla "sincerità" dello scrutinio?[58]
Tutto ciò potrebbe offrire anche una lettura *a contrario*. Se "siamo tutti giornalisti" – si potrebbe dire – non è più sostenibile un regime penale più grave per i giornalisti iscritti all'albo. Il problema, in realtà, è che il reato di diffamazione aggravata, anche a mezzo stampa, non è un reato proprio, ma chiunque può realizzare la condotta tipica ed esporsi alla sanzione penale detentiva. Per di più, il diritto di cronaca costituisce una specifica scriminante a vantaggio dei giornalisti[59], i quali mantengono – malgrado la

[57] È, in fondo, anche questo uno dei significati del principio *nullum crimen sine lege*.

[58] In tema è recentemente intervenuto il *Conseil constitutionnel*, con la decisione n° 2020-863 QPC del13 novembre 2020, *Société Manpower France*. In questo caso si verteva sul diverso termine che la legge sulla stampa del 1885 concede, in caso di diffamazione, per provare la verità dei fatti e andare dunque esenti da responsabilità. Il termine generale di 10 giorni viene ridotto ad un solo giorno in caso di diffusione di notizie diffamatorie in periodo elettorale. Nel § 17 il giudice della *Rue Montpensier* afferma che «*la liberté d'expression revêt une importance particulière dans le débat politique et au cours des campagnes électorales. Elle garantit à la fois l'information de chacun et la défense de toutes les opinions mais prémunit aussi contre les conséquences des abus commis sur son fondement en permettant d'y répondre et de les dénoncer, notamment en cas de diffamation*». La decisione, infine, ritiene che la legge abbia bilanciato, in maniera non irragionevole, «*d'une part, la liberté d'expression et de communication et les droits de la défense et, d'autre part, le principe de sincérité du scrutin et le droit à un recours juridictionnel effectif*» (§ 19). Sul "principio di sincerità" v. M. Luciani, *Il principio di "sincerità" nella giurisprudenza costituzionale italiana*, in *Politica del diritto*, 4, 2010, 575 ss.

[59] In Italia, la scriminante dell'esercizio del diritto di cronaca (ricondotta alla causa di giustificazione generale dell'art. 51 c.p.) è stata ora estesa anche ad altri delitti, in particolare quello di ricettazione, in quanto reato integrato allo scopo di procacciare la notizia stessa: v. Cass. pen., sez. II, 7 giugno 2019, n. 38277. Si amplia, dunque, l'area della non punibilità per i giornalisti, rimanendo in dubbio che tale ampliamento possa valere anche per altri soggetti (per i quali è comunque riconosciuto, in maniera più mitigata, l'esercizio scriminante del diritto di cronaca).

concorrenza "amatoriale" degli altri utenti di Internet – una maggiore visibilità.
L'intervento legislativo richiesto, quindi, non può livellare al ribasso la responsabilità penale, senza considerare le differenze che ancora permangono fra i mezzi giornalistici e chi si esprime con un post su Facebook (si pensi a tutte le garanzie evidenziate nel paragrafo precedente).
Infine, non si può sottacere la circostanza che, nel tempo presente, i rapporti fra informazione e tenuta delle democrazie contemporanee mostrano ben altre incrinature rispetto alla responsabilità penale dei giornalisti. Basti qui solo evocare il tema – emerso ancora più tragicamente di recente, con la circolazione di teorie negazionistiche sulla pandemia di COVID-19 – delle *fake news*[60], che talvolta anche alcuni organi di stampa diffondono, incuranti degli obblighi professionali concernenti la verifica e la correttezza delle fonti e della responsabilità pubblica di cui si è già detto, oppure le pratiche commerciali, di dubbia compatibilità deontologica, che le stesse testate giornalistiche adoperano nelle varie reti *social* (ad esempio, i c.d. *clickbaits*[61]).
Insomma, per parafrasare una storica sentenza della Corte italiana resa nei confronti (non del quarto, ma) del "primo" potere[62], la stampa è la vera custode della sua stessa legittimazione.
Ben vengano, allora, anche forme diverse di controllo e di sanzione – ad esempio, di natura disciplinare o anche a carattere più propriamente amministrativo, tramite l'intervento di Autorità già esistenti[63], o ancora con un rinforzo della natura sanzionatoria della responsabilità civile[64] – ma non va mai dimenticato quali beni e con quale intensità si può ferire "in punta di penna".
Ciò serve a ricordare come le direzioni percorribili siano molte e come, oltre a tenere in considerazione i diversi valori in gioco, vadano ponderate specifiche situazioni nazionali e gli ordinamenti nella loro dimensione storica. Oggi non è affatto detto – salvo che lo si assuma come postulato – che il bilanciamento debba essere orientato comunque a maggior beneficio della libertà di informazione e dei suoi principali interpreti, ma ovviamente nemmeno si può ritenere (né si sta qui sostenendo) che la libertà in parola

[60] V., per tutti, G. Pitruzzella – O. Pollicino, *Disinformation and hate speech. A European Constitutional Perspective*, Milano, 2020.

[61] Per *clickbaits* si intendono quelle anticipazioni pubblicate su reti sociali, fornite di titoli suggestivi affinché l'utente vi clicchi e acceda alla pagina web del quotidiano. L'utilizzo di titoli non corrispondenti (o solo parzialmente) al contenuto non si raccorda con i doveri deontologici di continenza, anche perché mira prevalentemente ad aumentare le visualizzazioni delle pagine. In questo modo, come è noto, gli algoritmi dei social network sono condotti ad aumentare la visibilità del contenuto, in proporzione alle visite ricevute.

[62] Si fa riferimento alla celebre sentenza n. 379/1996 sull'autodichia delle Camere. In chiusura della pronuncia, la Corte ricordava al Parlamento che la repressione interna degli abusi si poneva allo stesso organo come problema per la «conservazione della legittimazione degli istituti della autonomia che presidiano la sua libertà».

[63] Sarebbe ipotizzabile un controllo di carattere amministrativo-sanzionatorio da parte dell'Autorità per le garanzie nelle comunicazioni o da parte dello stesso Garante per la tutela dei dati personali.

[64] Si fa qui riferimento al tema dei danni punitivi, tipici di ordinamenti di *common law*, che la Corte di Cassazione ha tuttavia ritenuto compatibili con la funzione della responsabilità aquiliana *ex* art. 2043 c.c., da ritenersi ormai polivalente all'interno dell'ordinamento italiano: v. Cass. civ., sez. un., 5 luglio 2017 n. 16601.

sia divenuta «un lusso che non ci si può più permettere» nell'era del cyberspazio[65].
Dunque, il potere di trovare il punto di questa conciliazione dovrebbe restare nella disponibilità del legislatore nazionale, sottoposto ovviamente agli ordinari controlli di costituzionalità[66], senza che tale bilanciamento venga definito dalla giurisdizione sovranazionale per un intero continente. Data la natura sussidiaria della giurisdizione della Corte EDU, un conto è infatti definire che in un caso specifico lo Stato ha violato la libertà di un giornalista, altro conto è affermare che un sistema penale nel suo complesso non rispetta gli standard convenzionali (forse, peraltro, bisognosi di qualche ripensamento), lasciando però la possibilità di correttivi nazionali (rappresentati dai "casi eccezionali") e così impedendo che si possa parlare di vere e proprie "sentenze pilota" (cosa che la stessa Corte costituzionale italiana, difatti, non fa).

6. La libertà di informazione come libertà politica e la protezione del suo versante passivo

Ricostruire un quadro esauriente, coerente e bilanciato del diritto di informare nell'era *social* è operazione assai ardua, che travalica gli obiettivi e le possibilità di questo scritto. Tuttavia, ci si permette di offrire alcune riflessioni che possono contribuire a questa ricostruzione, ritornando, come spesso avviene di fronte alla complessità crescente dei temi, ai fondamenti. E il fondamento primo è rappresentato dalla natura della libertà di informazione, una natura la cui definizione può – almeno sotto un profilo teorico – orientare l'interpretazione del diritto in questione e costituire il primo passo per una rivisitazione dei bilanciamenti a questo connessi.
Il punto di partenza è questo: la libertà di informazione è una libertà politica. E politica in un doppio significato: è politica perché è una libertà che si fa valere *contro il potere* – ovviamente anche quello democraticamente legittimato – per sottoporlo ad un continuo controllo da parte della comunità di riferimento, per ottenerne interventi o mutamenti di indirizzo, per alimentare il dibattito pubblico e la critica attorno al suo utilizzo[67]. La libertà di informazione costituisce, dunque, il principale strumento a garanzia del cittadino affinché chi detiene il potere ne renda conto (c.d. *accountability*).
E poi è una libertà politica, perché è una libertà *comunitaria*: concerne la *polis* in sé, e

[65] L. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier*, in *The Humanist*, 51, 1991: «*The real basis for First Amendment values isn't the false premise that information and ideas have no real impact, but the belief that information and ideas are too important to entrust to any government censor or overseer. If we keep that in mind, and only if we keep that in mind, will we be able to see through the tempting argument that, in the Information Age, free speech is a luxury we can no longer afford*».

[66] Pare opportuno qui citare la decisione n° 2016-738 DC del 10 novembre 2016, *Loi visant à renforcer la liberté, l'indépendance et le pluralisme des médias,* con la quale il *Conseil Constitutionnel* ha censurato l'art. 4 della legge deferita – che rafforzava il segreto giornalistico intervenendo sulla legge del 1885, estendendone la portata. In particolare il giudice ha ritenuto (§ 23) che: «*le législateur n'a pas assuré une conciliation équilibrée entre, d'une part, la liberté d'expression et de communication et, d'autre part, le droit au respect de la vie privée et le secret des correspondances. Il n'a pas non plus assuré une conciliation équilibrée entre cette même liberté et les exigences inhérentes à la sauvegarde des intérêts fondamentaux de la Nation, la recherche des auteurs d'infractions et la prévention des atteintes à l'ordre public nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle*».

[67] V. anche il collegamento fra libertà di informazione e diritto di partecipazione alla vita pubblica: A. Lamberti, *Libertà di informazione televisiva e diritti fondamentali*, cit., 154.

contribuisce a creare e a rinsaldare il senso di appartenenza, mettendo a parte i membri della comunità di tutti quei fatti che interessano la convivenza sociale[68], come individui singoli, portatori di specifici interessi, e al tempo stesso come componenti del gruppo[69].
Pare interessante evocare un'importante pronuncia della *High Court* australiana del 1997 (*Lange v Australian Broadcasting Corporation*, nota anche come *Political Free Speech Case*) nella quale la suprema giurisdizione del *Commonwealth* ha ricondotto la libertà dell'informazione, in particolare politica, all'essenza stessa del governo rappresentativo[70]. Il caso riguardava un procedimento per diffamazione avviato da un uomo politico neozelandese, già Primo Ministro dello Stato oceanico, contro un'emittente televisiva australiana che in un suo programma di approfondimento aveva dedicato attenzioni poco gradite agli affari privati dell'uomo.
Quella che potrebbe sembrare una posizione datata – o quanto meno scontata – ci riporta esattamente a quei fondamenti prima evocati: negli ordinamenti costituzionali, le libertà comunicative di natura pubblica sono funzionali all'esistenza della democrazia come sistema di governo di un popolo, tanto più nella dimensione della democrazia sociale, dove la qualità della vita e la libertà degli individui dipendono in massima parte dall'azione dello Stato. Dunque «le persone devono essere nella condizione di comunicare liberamente fra loro rispetto a temi che possono incidere sulla loro scelta nelle elezioni federali o nei referendum costituzionali o che possono gettare luce sul rendimento dei Ministri e sulla condotta del potere esecutivo»[71].
Il recupero di questo insegnamento pare oggi ineludibile.
Nel profluvio di informazioni che ciascuno di noi può attingere e diffondere tramite una connessione Internet e un *device,* è fondamentale distinguere quali di queste sono fornite nell'esercizio di una libertà di comunicazione pubblica e quali, invece, godono di una minore protezione. Solo quelle che si ricollegano ai due profili prima evocati devono considerarsi prodotto del diritto di cronaca: informazioni, dunque, che attengono direttamente alla gestione della cosa pubblica e che possano avere un interesse generale per una determinata comunità chiaramente individuabile[72].

---

[68] Si ricordi la felice espressione di P. Barile, *Libertà di manifestazione del pensiero*, cit., § 13: «[La libertà di cronaca] è in sostanza un comportamento che impegna la convivenza sociale: potrebbe dirsi che la cronaca è la fotografia della vita di ogni giorno di una piccola o grande comunità».

[69] I soggetti sono quindi compartecipi di quell'opinione *pubblica,* che è tale «non solo perché è del pubblico (diffusa tra i molti, o tra i più), ma anche perché investe oggetti o materie che sono di natura pubblica: l'interesse generale, il bene comune e, in sostanza, la *res publica*» (G. Sartori, voce *Opinione pubblica,* in *Enciclopedia del Novecento*, Roma, 1975).

[70] «*Freedom of communication on matters of government and politics is an indispensable incident of that system of representative government which the Constitution creates by directing that the members of the House of Representatives and the Senate shall be "directly chosen by the people" of the Commonwealth and the States, respectively*». La Corte cita poi A.H. Birch, *Representative and Responsible Government: An Essay on the British Constitution,* Toronto, 1964, 17: «*we need to add that the chamber must occupy a powerful position in the political system and that the elections to it must be free, with all that this implies in the way of freedom of speech and political organization*».

[71] *Lange v Australian Broadcasting Corporation,* [1997] HCA 25 (traduzione nostra).

[72] Gli esempi di casi esorbitanti da questi limiti possono essere i più disparati. Giusto per farne alcuni, non potrà considerarsi legittimo esercizio della libertà di informazione lo sfogo fatto per denunciare un servizio scadente in un locale o in un esercizio commerciale, così come la divulgazione di informazioni sulla vita privata di una persona (ad es., le abitudini di un vicino di casa ritenute fastidiose). La lamentela per un disservizio della Pubblica Amministrazione dovrebbe, in linea di massima, godere della tutela

Questa natura politica della libertà di informazione mette in luce un ulteriore profilo: la qualità e il livello di tutela del diritto passivo all'informazione (la *freedom of information* in senso anglosassone).

La sterminata estensione del lato attivo della libertà di informazione non beneficia lo sviluppo del suo lato passivo, rappresentandovi semmai – quando non una minaccia – perlomeno un ostacolo.

Ci troviamo, infatti, nella situazione quasi paradossale in cui si ricevono una quantità infinita di notizie, eppure esistono rilevanti ambiti della vita pubblica – che, in funzione di quanto detto poc'anzi, dovrebbero essere i primi oggetti delle informazioni – nascosti in un cono d'ombra, difficile da lumeggiare. Nel "rumore" generale, cioè, vi sono gangli di potere (perfettamente istituzionale e legittimato) che non sono stati toccati dalla rivoluzione digitale e, anzi, si richiede precisamente che vengano protetti da questa.

Se è vero che in ogni ordinamento esistono spazi di "riservatezza pubblica", legittimamente sottratti, in tutto o in parte, all'informazione (si pensi alla disciplina dei segreti o alle forme di pubblicità attenuata dei lavori parlamentari), non è men vero che in altri casi le zone d'ombra si siano consolidate in assenza di specifiche previsioni. Le attività dei capi di Stato, ad esempio, godono di un alone di mistero che spesso non è consacrato nelle norme, ma che poi viene normativizzato dalla tradizione e dalla giurisprudenza[73].

E se questo esempio pare troppo singolare, si pensi altresì alla creazione dei testi normativi fuori dalle aule parlamentari (gli atti normativi dell'Esecutivo, di qualunque categoria), di cui spesso non si conoscono né le tappe della formazione, né gli apporti esterni alla loro fabbricazione, sino a che non sono pubblicati od oggetto di altri atti sottoposti a forme pubblicitarie (si pensi ai pareri del Consiglio di Stato in Francia o in Italia).

Infine, non si può poi dimenticare che, nell'universo digitale, la selezione delle informazioni rilevanti e garantite si trova ad essere rimessa (almeno in prima battuta) non a pubblici poteri, ma a soggetti privati. E ciò è stato consacrato dalla sentenza *GC c.*

costituzionale, salvo che il presunto disservizio non si riveli come imputabile al singolo soggetto privato (es. domanda incompleta, inesistenza del diritto alla pretesa fatta valere). In questo caso, viene meno l'interesse della collettività, pur essendo l'informazione destinata a creare una critica nei confronti dei pubblici poteri.

[73] In Italia, traccia di questo si rinviene nella sent. 1/2013 sulla riservatezza del Capo dello Stato (definita "iper-riservatezza: A. D'Andrea, *Attività informale e iper-riservatezza del Presidente della Repubblica: il via libera della Corte con qualche slancio di troppo*, in *Giurisprudenza Costituzionale*, 1, 2013, 77 ss.). Si v., anche in riferimento alle nuove possibilità comunicative del Presidente della Repubblica, le osservazioni di P. Faraguna, *Il Presidente della Repubblica. Un'istituzione pesante alle prese con la leggerezza del web*, in D. Chinni (a cura di), *Potere e opinione pubblica. Gli organi costituzionali dinanzi alle sfide del web*, Napoli, 2019, 59 ss. Nel Regno Unito, le relazioni del Sovrano con gli esponenti politici (ed in particolare governativi) sono coperte, per la forza della tradizione, dal più completo riserbo. Nel 2015, la Corte Suprema britannica ha deciso che le lettere inviate dal Principe Carlo ai Ministri non erano coperte dalla convenzione costituzionale di stretta confidenzialità che copre gli atti del solo Sovrano, esponendosi così alla *disclosure* prevista dal *Freedom of Information Act* ([2015] UKSC 21*, R (on the application of Evans) and another v. Attorney General*). Il principio della riservatezza delle comunicazioni del Sovrano è stato ribadito di recente dalla *High Court* australiana, in relazione a missive scambiate fra la regina e il Governatore Generale dell'isola negli anni '70 (*Hocking v. Director-General of the National Archives of Australia*), sebbene in quest'ultimo caso la Corte abbia infine fatto prevalere la legislazione statale sulla ricerca archivistica.

Commission nationale de l'informatique et des libertés resa il 24 settembre 2019 dalla Grande Sezione della CGUE (C-136/17), che – avanzando nella traiettoria del caso *Google Spain*[74] – ha attribuito ai c.d. "giganti del web" il compito di vagliare le richieste di deindicizzazione di contenuti anche alla luce dell'art. 11 della Carta di Nizza, cioè della libertà di ricevere informazioni da parte degli utenti europei[75].

Dunque, l'attribuzione di potestà sostanzialmente pubblicistiche così penetranti ad operatori privati, chiamati a ponderare concorrenti interessi in gioco, richiede in maniera ancora più pressante che si riscoprano e si presidino i confini della libertà di informazione. Confini che diverranno poi il parametro di valutazione dell'azione privata da parte del potere pubblico (sia esso un giudice o un'autorità amministrativa indipendente[76]).

7. Conclusioni

Al termine di questo itinerario, è difficile tratteggiare delle vere e proprie conclusioni, vista la velocità con cui il cangiante quadro dei mezzi di comunicazione evolve, trascinando con sé anche i problemi giuridici legati alla libertà di informazione.

Il dato che sicuramente emerge, però, è che i legislatori hanno sostanzialmente lasciato campo libero ai giudici per regolare i bilanciamenti fra diritti e valori che la società dell'informazione impone di rivedere.

Da un lato, non sfugge la complessità dell'azione richiesta ai decisori politici, che dovrebbero mettere in discussione anche consolidati sistemi normativi (si pensi alla tutela penale della reputazione), senza essere in grado di identificare un assetto che possa soddisfare le innumerevoli istanze in gioco. Talvolta, allora, l'inerzia del legislatore può divenire una scelta consapevole, lasciando egli ai giudici le operazioni di bilanciamento nei casi concreti, secondo un approccio casistico ormai sempre più diffuso e a volte persino invocato dalla dottrina.

Dall'altro lato, anche laddove il legislatore ha tentato di intervenire, la sua azione politica è stata direttamente censurata dal giudice costituzionale, perché eccessivamente squilibrata rispetto ai diversi interessi da ponderare. È emblematico il caso della *Loi Avia* francese contro i discorsi d'odio in Internet, che il *Conseil Constitutionnel* ha sostanzialmente demolito con la dichiarazione di illegittimità di quasi due terzi delle disposi-

[74] Nel caso *Google Spain* la CGUE ha fatto riferimento agli artt. 8 e 9 della Carta dei diritti fondamentali, ma non all'art. 11, nell'individuare i diritti fondamentali che devono prevalere in linea di principio di fronte ad una richiesta di deindicizzazione dai motori di ricerca.

[75] «Le disposizioni della direttiva 95/46 devono essere interpretate nel senso che il gestore di un motore di ricerca […] deve […] verificare, alla luce dei motivi di interesse pubblico rilevante di cui all'articolo 8, paragrafo 4, della suddetta direttiva e nel rispetto delle condizioni previste in quest'ultima disposizione, se l'inserimento di detto link nell'elenco dei risultati, visualizzato in esito ad una ricerca effettuata a partire dal nome della persona in questione, si riveli strettamente necessario per proteggere la libertà di informazione degli utenti di Internet potenzialmente interessati ad avere accesso a tale pagina web mediante una ricerca siffatta, libertà che è sancita all'articolo 11 della Carta».

[76] La doppia natura – giudiziaria e amministrativa – del controllo pubblico sul sistema dell'informazione è stabilita da tempo: v. R. Pinto, *La liberté d'opinion et d'information. Contrôle juridictionnel et contrôle administratif*, Parigi, 1955.

zioni legislative (undici articoli su diciannove)[77].

Ciononostante, è giusto richiedere al legislatore di porre in essere tentativi di intervento, ragionati e non meramente istintivi, provando a disegnare un quadro regolatorio ampio, che non può esaurirsi nelle sanzioni penali (pur necessarie, in una qualche misura), ma che dall'altro non può ammettere una recessione dei pubblici poteri dalla tutela di diritti fondamentali oggi divenuti più fragili (si pensi anche al "diritto all'anonimato"[78]), ma comunque non sacrificabili in nome di una libertà di certo preziosissima, eppure molto insidiosa.

[77] Décision n° 2020-801 DC del 18 giugno 2020, *Loi visant à lutter contre les contenus haineux sur internet.*

[78] Sullo spinoso tema dell'anonimato in Internet v. M. Manetti, *Libertà di pensiero e anonimato in rete*, in *Il diritto dell'informazione e dell'informatica*, 2, 2014, 139 ss. Secondo l'A. l'anonimato ha avuto «un valore paradigmatico» per l'affermazione della libertà di pensiero ed anche nell'ambiente di Internet costituisce una «difesa della persona da forme di controllo pervasive», oggi realizzabili tramite la profilazione e l'accumulo dei dati.

The commodification of our digital identity: limits on monetizing personal data in the European context

Milena Mursia, Carmine Andrea Trovato

Abstract

Personal data have an immense economic value and are used by firms to power their business models. However, this fact is insufficient to argue that personal data can be lawfully traded on the market, similarly to a commodity. The extent to which personal data can be traded and monetized is the object of an intense debate. The aim of this paper is to explore whether personal data can be considered a counter-performance in an agreement, that is exchanged on the market for products/services and/or money, assessing whether this perspective is consistent with the fundamental rights' nature of the right to the protection of personal data and with personality rights in Europe, and the limits under the European General Data Protection Regulation.

I dati personali hanno un immenso valore economico e sono utilizzati dalle società per alimentare i propri modelli di business. Tuttavia, questa circostanza non è in sé sufficiente per poter affermare che sia lecito quindi commercializzare i dati personali sul mercato, analogamente a una merce. Il limite entro cui i dati personali possono essere scambiati e monetizzati sul mercato è oggetto di un intenso dibattito. Lo scopo di questo lavoro è esplorare se i dati personali possano essere considerati una contro-prestazione contrattuale, cioè se possano essere scambiati sul mercato per prodotti/servizi e/o denaro. Viene valutato se questa prospettiva sia coerente con la natura del diritto alla protezione dei dati personali quale diritto fondamentale e con i diritti della personalità in Europa, e quali siano i limiti imposti dal Regolamento Generale sulla Protezione dei Dati.

Table of contents

1. Introduction. – 2. The commercial use and monetization of personal data. – 3. The European right to the protection of personal data. – 3.1. Data protection as a fundamental right. – 3.2. Data protection as a personality right. – 4. Personal data as a counter-performance: a GDPR analysis. – 5. Conclusion.

[*] Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Keywords

Data monetization - personal data - personality rights - GDPR – counter-performance

1. Introduction

Personal data have an immense economic importance in today's digital economy. The European Commission estimated in 2017 that the value of personal data in Europe might grow to approximately Eur 1 trillion annually in the following three years.[1]
Personal data are being commercialized and monetized by companies whose business models are centered on processing them. Such companies often provide products/services at "zero-price" in exchange of individuals' personal data.[2] For example, according to a Wall Street Journal analysis, the most popular Facebook apps gather volumes of personal data from users and their friends (on birthdays, sexual preferences, work history, education), and use them to attract advertisers, app makers, to show targeted ads or sell them to third parties.[3] Therefore, individuals "pay" in personal data by providing information about themselves.[4] Other companies purchase personal data directly from individuals (so-called "personal data economy models").[5] Indeed, apps such as Datum, Wibson, Datacoup, Ocean Protocol, Weople, advertise the possibility for users' to retake control of their personal data by selling them and prompt individuals to have a cut of the sale of their personal data.[6] In addition, other companies require users to pay a (higher) price in order to avoid the collection of personal data for advertising purposes (so-called "pay for privacy models").[7] The theoretical assumption that «allows and underpins such mechanisms is the construction of a "user-centric" economic system of personal data that conceives the individual as an owner of a wealth that can be shared».[8]
Thus, personal data are being commercialized on the market like a commodity[9] and it

[1] European Commission, Fact Sheet - *Questions and Answers – Data protection reform package*, 2017, accessed 26 June 2020.

[2] Organisation for Economic Cooperation and Development ("OECD"), *Quality considerations in digital zero-price markets. Background note by the Secretariat*, 28 November 2018.

[3] J. Angwin – J. Singer-Vine, *Selling You on Facebook*, in *wsj.com*, 7 April 2012.

[4] *Ibid.*

[5] S. Elvy, *Paying for privacy and the personal data economy*, in *Columbia Law Rev.*, 117(6), 2017, 1369 ss.; V. Ricciuto, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato* in N. Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milan, 2019, 128-129.

[6] G. Barber, *I Sold My Data for Crypto. Here's How Much I Made*, in *wired.com*, 17 December 2018; I. de Michelis di Slonghello – L. Bolognini, *An Introduction to the Right to Monetize (RTM)*, in *istitutoitalianoprivacy.it*, 9 April 2018, suggest introducing a right of monetization of individuals' personal data.

[7] S. Elvy, *Paying for privacy and the personal data economy*, cit., 1369.

[8] V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno,* in *Diritto dell'Informazione e dell'Informatica,* 4, 2018*,* 718.

[9] V. Janecek – G. Malgieri, *Data Extra Commercium*, in S. Lohsse - R. Schulze - D. Staudenmayer (eds.), *Data as Counter-Performance—Contract Law*, Berlin, 2019.

is an established fact that they do have an economic value. Indeed, this has also been confirmed in different occasions by the Italian Competition and Market Authority ("AGCM"). For instance, in declaring the unfairness of certain contractual clauses provided for in the standard terms of WhatsApp, the AGCM has recently recalled in support of the solution adopted the «well-established orientation of the European Commission to recognize the nature of non-pecuniary counter-performance of the personal data of social media users, both in terms of consumer protection and in the assessment of mergers between companies. Such economic value is therefore suitable to configure the existence of a consumer relationship between the Professional and the user».[10] Also, the AGCM with decision of 29 November 2018 no. 27432, in considering that Facebook Ireland Ltd. and its parent company Facebook Inc had infringed the Italian Consumer Code by engaging in the misleading practice of emphasizing the "free" nature of the service, while the personal data collected was instead being used for commercial purposes, recognized the existence of a commercial transaction between Facebook and the users and thus an exchange of performances in the use of the social network.[11] Moreover, the fact that personal data are supplied by consumers as a sort of "payment" for digital services and digital content has also been recognized by the EU legislator in Directive 2019/770[12] and Directive 2019/2161[13] (see Paragraph 4 below in this respect).

That said, the acknowledgment of the economic value of personal data and that personal data can be traded in exchange for products and services does not in itself justify commodification of personal data. Indeed, whether and the extent to which personal data can be traded and monetized has been the object of an intense debate.[14] On the one hand, the tradability of personal data raises concerns given the EU's fundamental right of data protection and its nature; on the other, it is arguable that individuals should have the right to control their personal data[15] to a point where they can

[10] Autorità Garante della Concorrenza e del Mercato, *Decision CV154*, 11 May 2017; G. D'Ippolito, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Il diritto dell'informazione e dell'informatica,* 3, 2020, 634-674. The Authority's decision follows the position expressed by the national authorities responsible for the enforcement of consumer protection legislation in Common position of national authorities within the "CPC Network concerning the protection of consumers on social networks", 17 March 2017, which call for careful consideration of the possible unfairness of certain clauses contained in the general conditions drafted by the operators of social networks.

[11] See also decision of *Tar Lazio* (Administrative Court of Lazio), 10 January 2020, no. 261/20, which partly upheld the decision of the AGCM and reiterated that personal data are considered as an economic asset, and thus consumers «must be made aware of the exchange of performances» in the use of the social network.

[12] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJL136/1 ("Directive 2019/770").

[13] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7 ("Directive 2019/2161").

[14] J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, in *twobirds.com,* August 2019.

[15] European Commission, *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.

decide to "pay" with their personal data or otherwise dispose of them. In essence, the fundamental right to data protection should be balanced with other interests and fundamental rights, such as the free flow of data and the freedom to conduct a business and to contract[16] or have control over personal interests under principles of personal autonomy.[17]

The aim of this paper is to explore whether personal data can be exchanged for valuable assets (for example, products/services, other incentives) or money. In other words, can the processing of personal data be considered a counter-performance in an agreement and can individuals receive consideration in exchange of their personal data (the so-called data dividend)[18] - both acts resulting in personal data commercialization and monetization? The focus of the analysis will be Europe, in particular, the approach to data protection of the Council of Europe and the European Union.

Paragraph 2 will briefly analyse the personal data-centered business models and their related benefits and disadvantages for users. Paragraph 3 comprises two sub sections, the first sub of which will explore whether the commodification of personal data is consistent with the nature of the right to the protection of personal data. Thus, it will examine the fundamental right to data protection enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR")[19] and the Charter of Fundamental Rights of the European Union ("Charter")[20], and the dual nature of personal data, as a projection of an individual's personality and as an economic good.[21] The second sub section then will investigate whether and how[22] personal data can lawfully be traded under the General Data Protection Regulation ("GDPR")[23], having regard to the relevant opinions of the European Data Protection

[16] Garante per la protezione dei dati personali, *Relazione annuale 2019*, 23 June 2020, 124-125.

[17] N.R. Koffeman, *(The right to) personal autonomy in the case law of the European Court of Human Rights*, in *scholarlypublications.universiteitleiden.nl*, June 2010, citing the European Court of Human Rights ("ECtHR") case law, according to which personal autonomy (or self-determination) is considered both a principle of law «underlying the interpretation of the ECHR guarantees» (*Pretty v The United Kingdom* (2002) 35 EHRR 1, § 61), and a right itself, as a component of the right to a private life under Article 8 European Convention for the Protection of Human Rights and Fundamental Freedoms (*Evans v The United Kingdom* (2008) 46 EHRR 34, § 57). In *Pretty,* § 62, it is defined as «the ability to conduct life in a manner of one's own choosing»; P. De Hert – S. Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action* in S. Gutwirth – Y. Poullet – P. de Hert (eds.), *Reinventing data protection*?, Dordrecht, 2010, 14-15. Moreover, H. J. Snijders, *Privacy of Contract* in K. Ziegler (ed.), *Human Rights and Private Law: Privacy as Autonomy*, Oxford, 2007, 108: «personal autonomy can be concretised as the right to freely enter into contracts».

[18] Garante per la protezione dei dati personali, *Relazione annuale per il 2018. Discorso del Presidente Antonello Soro*, 7 May 2019.

[19] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended), Rome, 4 November 1950.

[20] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

[21] *Diritto mercato e tecnologia*, interview with G. Finocchiaro, *La nuova sovranità privata e l'ambivalenza del dato personale. Intervista a Giusella Finocchiaro*, in *blogstudiolegalefinocchiario.it*, 3 December 2019.

[22] F.G. Viterbo, *Freedom of contract and the commercial value of personal data*, in *Contratto e impresa Europa,* 2016, 593 ss., 596.

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Supervisor ("EDPS") and the European Data Protection Board ("EDPB") and certain decisions of the national data protection authorities and courts. More specifically, it will evaluate whether the legal basis of consent and contract (respectively Articles 6(1)(a) and 6(1)(b) GDPR) can justify the tradability of personal data.[24]
This paper will conclude that the nature of data protection as a fundamental right and as a personality right does not *per se* exclude the alienability of personal data, however this is limited to the conditions of the GDPR. In this regard, it shows that there is room to interpret the legal bases under Article 6 GDPR in ways that could allow the commercialization and monetization of personal data.

2. The commercial use and monetization of personal data

Several business models are based on the collection and analysis of users' personal data;[25] these monetize personal data[26] and generate revenues. More specifically, personal data are used by companies for a variety of commercial purposes, some concern direct monetization through the sale of personal data, others indirect monetization, such as for security, product/service improvement and development, improvement of the customer experience, including a personalized customer experience.[27] One important use of personal data consists in the collection of users' interests, preferences or other characteristics to place targeted online advertising, which funds a considerable number of online services.[28]
Here, personal data-centered businesses will be divided into three models: (i) zero-price[29]; (ii) personal data economy[30]; (iii) pay for privacy.[31] This section will describe these, in turn, highlighting some of the benefits and disadvantages for the users deriving from the collection and use of their personal data[32] - some of which, as examined in the following sections – have influenced the legal position on the alienability of

[2016] OJ L119/1.

24 V. Janecek – G. Malgieri, *Data Extra Commercium*, cit., 7.

25 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1371.

26 European Commission, *Commission Staff Working Document Impact Assessment Accompanying the document Proposals for Directives of the European Parliament and of the Council (1) on certain aspects concerning contracts for the supply of digital content and (2) on certain aspects concerning contracts for the online and other distance sales of goods* COM(2015) 634 final: «Digital content may be supplied either against a price or against (personal and other) data provided by consumers as a counter performance…the great majority of contracts for the supply of digital content involve collection of data of an economic value, which can be monetised by the suppliers».

27 Competition and Markets Authority ("CMA"), *The commercial use of consumer data - Report on the CMA's call for information*, June 2015; J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 38.

28 CMA, *The commercial use of consumer data,* cit., 6.

29 OECD, *Quality considerations in digital zero-price markets,* 4.

30 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1369.

31 *Ibid.*

32 CMA, *The commercial use of consumer data,* cit., 7.

personal data.

As to the zero-price models, according to an economic theory the provision of personal data can be considered an implicit component of the price that the users pay for the purchase of the primary service[33] (typically, digital content[34] or digital service[35]). Such digital content/service is generally advertised as for free, while actually users provide their personal data in exchange.[36] Certain authors argue that, notwithstanding the fact that there is no trade of currency, this is still a real commercial transaction on the basis that «the argument that free goods are not sold […] does not make economic sense»[37] and that personal data are indeed the price users are paying.[38] The latter position, as demonstrated above, is also shared by the European Commission.

The personal data economy models are advertised as empowering individuals to obtain value from their personal data by selling or providing access to their personal data to data buyers.[39] For instance, certain apps allow individuals to earn value through direct marketing, profiling, personalized offers and by allowing third parties to enrich their databases with the account holders' personal data.[40]

Finally, paying for privacy models require individuals who do not want to consent to the collection of their personal data for targeted advertising/marketing purposes to pay (higher) fees for accessing the product/service, whose providers offer lesser charges/discounts to individuals who instead provide their consent for such purposes.[41]

Users, companies and the economy in general benefit from the collection and use of personal data.[42] From the users' point of view, the benefits concern personalised services, broader options, improvement of existing services, more pertinent advertising and offers that may reduce the search cost for users.[43] Also, the described business models increase the users' awareness of the value (broadly understood from a qualita-

---

33 Autorità Garante della concorrenza e del mercato, *Autorità per le garanzie nelle comunicazioni*, *Garante per la protezione dei dati personali*, "*Indagine Conoscitiva Sui Big Data*", 10 February 2020.

34 J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 36: «Digital content, in short, means data produced and supplied in a digital form. Forms of digital content may include computer programs, games, music, videos, applications, cloud storage and potentially social media».

35 According to article 2(2) of Directive 2019/770: «'digital service' means: (a) a service that allows the consumer to create, process, store or access data in digital form; or (b) a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer», for example social media platforms and cloud computing services.

36 J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 36.

37 OECD, *Quality considerations in digital zero-price markets,* cit., 5.

38 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1385: data are not money or currency, but this label is used to describe the situation where individuals provide personal data to obtain zero-price products/services; J. Lanier, *You Are Not a Gadget: a Manifesto*, 2011.

39 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1375.

40 For instance Weople, described at *weople.space/en/#functions*.

41 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1387-1392.

42 CMA, *The commercial use of consumer data,* cit., 7.

43 P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, in *cerre.eu*, 25 January 2016; CMA, *The commercial use of consumer data,* cit., 50-51.

tive and quantitative point of view) of their personal data.[44]

However, it is questioned whether these business models are beneficial to individuals, as significant concerns arise in relation to data protection. First, users do not clearly know the ultimate value of their personal data and thus do not fully understand the extent to which they give away their personal data in exchange for "free" products/services or for other incentives.[45] For instance, the value of their personal data may exceed the value of the product/service they receive "for free".[46] Moreover, individuals may not be aware of and/or fully understand the use of their personal data.[47] This information asymmetry is also exacerbated by the use of nudging[48] and dark patterns[49], techniques exploiting users' psychological biases[50] that lead them to privacy intrusive choices and/or to share their personal data.[51] For example, when a user is offered the possibility to obtain a discount (or other "short-term financial benefit") in exchange of her consent to data processing, the real cost of this transaction is difficult to understand. Here, according to the research, as the short-term benefit (discount) is tangible and instant, while the potential give-away of privacy is long term and unrealized, the user will likely choose the short-term benefit. Also, users are more inclined to disclose personal data when they feel they are "in control" of them (so-called "control paradox"). However, control is often not effective as users are manipulated through dark patterns.[52]

---

44 S. Elvy, *Paying for privacy and the personal data economy*, cit., 1393.

45 S. Athey – C. Catalini _ C. Tucker, *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk*, in *National Bureau of Economic Research Working Paper Series*, No. 23488, 2017. The paper investigates distortions in consumer behavior which may limit the ability of consumers to safeguard their privacy. Indeed, the effect small incentives have on disclosure may explain the privacy paradox: People say they care about privacy but are willing to relinquish private data to firms quite easily when enticed to do so through small incentives. In this study, students were offered a pizza in exchange for disclosure of some personal data.

46 Ivi, 1385.

47 OECD, *Quality considerations in digital zero-price markets,* cit., 25, according to an experimental study concerning a social networking service «74% of participants opted not to consult the terms of service, and 98% did not identify a provision that allowed the supplier to share data with employers and law enforcement agencies (Obar and Oeldorf-Hirsch, 2018)».

48 Norwegian consumer council, *Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*, in *edri.org*, 27 June 2018, 6. Nudging «describes how users can be lead toward making certain choices by appealing to psychological biases. Rather than making decisions based on rationality, individuals have a tendency to be influenced by a variety of cognitive biases, often without being aware of it».

49 Ivi, 7: dark patterns are identified when «deliberately misleading users through exploitative nudging»

50 Norwegian consumer council (n 43) 6: «individuals have a tendency to choose smaller short-term rewards, rather than larger long-term gains»; OECD, *Quality considerations in digital zero-price markets,* cit., 26-27, referring to the "free effect" with regard to the fact that «valuations for free goods are boosted beyond their benefit-cost differences» and to the "privacy paradox" referring to the fact that even though users consider privacy important, they tend not to make decisions with privacy in mind.

51 Norwegian consumer council, cit., 3.

52 Ibid. 32: for example, Facebook's GDPR popup «You control whether we use data from partners to show you ads» is misleading since users are not given substantial control over the data collection, but only the possibility to decide which ads they will see.

Nevertheless, despite the fact that personal data is fluid, intangible and dynamic[53], it is argued that it is economically possible to quantify its monetary value.[54] Indeed, not only do the above business models show this in different ways, but there are also various specific methods to calculate the value of personal data.[55] Moreover, the overall information asymmetry between individuals and entities processing personal data – both with regard to the value of personal data and the uses of personal data - could be addressed by making existing fairness and transparency rules more effective (both from a privacy point of view[56] and from a consumerist point of view[57]) and/or by introducing new ones, thus raising the awareness of individuals about their data processing.

In this last regard, it is suggested (and agreed with) that individuals should have a

[53] Competition and Markets Authority ("CMA"), *The CMA's Response to the UK Government's Call for Views on the Draft Directives on the Online Sales of Digital Content and Tangible Goods*, 15 February 2016; J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 37.

[54] J. Debussche – J. César, *EU data economy: legal, ethical & social issues*, cit., 37; G. Malgieri – B. Custers, *Pricing privacy the right to know the value of your personal data*, in *Computer Law & Security Review*, 34(2), 2017, 289 ss.

[55] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, 2 April 2013, 18-32, identifies possible methodologies, one based on market valuation of personal data (in this case values can be derived from «financial results per data record», «market prices for data», «cost of data breach», «data prices in illegal markets») and one on individual's valuation of personal data, which focuses on «surveys and economic experiments», and «data on willingness of users to protect their data»; G. Malgieri, *Data Extra Commercium*, cit., 9-14: it is necessary to (i) clarify how to «express monetary value» of personal data, (ii) identify which object is priced and the pricing factors, and (iii) the pricing system («how to attach the value to the object»). As to (i) the value of personal data can be expressed in monthly terms, i.e., in terms of euro or dollars per month, and per person. As to (ii), the objects which are being priced are datasets and the factors affecting the price are «size, completeness, accuracy, being up-to date, rareness and uniqueness, and identifiability». Finally, the methods to determine the actual value of personal data in (iii) are various, some already identified by the OECD (see above) in market valuation and individual's valuation.

[56] Articles 5, 13 GDPR. According to F. Schaub - R. Balebako - A. Durty - L.F. Cranof, *A Design Space for Effective Privacy Notices,* Symposium on Usable Privacy and Security (SOUPS '15), Ottawa, Canada, Jul 2015. Other proposals at *usableprivacy.org/publications*. In recent years, some have begun to speak of «machine readable information notices», i.e., privacy notices that can be interpreted by a machine in a way that facilitates individuals' understanding of the complexity of how technologies work and how they continue to evolve. This could be a way of informing the data subject about compliance with all agreed conditions much more effectively than reading a textual information notice. We are still at the beginning of this process, but there are already concrete proposals to raise people's awareness.

[57] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJL 95/29 requires the use of plain, intelligible language. National investigations have addressed concerns of transparency and fairness in terms and conditions of websites and social media platforms. For example, the Autorità Garante della Concorrenza e del Mercato (Italian Competition and Market Authority), decision 29 November 2018 no. 27432, found that Facebook Ireland Ltd. and its parent company Facebook Inc infringed the Italian Consumer Code by engaging in the misleading practice of emphasizing the "free" nature of the service, while the personal data collected was instead being used for commercial purposes, thus considering this service as a commercial transaction between Facebook and the users; this decision was partly upheld by the *Tar Lazio* (Administrative Court of Lazio), 10 January 2020 no. 261/20, which stated that, given that personal data are considered as an economic asset, operators need «to comply with […] obligations of clarity, completeness and non - misleading information provided by the consumer protection legislation» and consumers «must be made aware of the exchange of performances» in the use of the social network.

right to know the quantitative value of their personal data.[58] More specifically, data controllers should inform individuals of the price of their personal data calculated on objective parameters.[59]

As to the additional drawbacks deriving from the application of these business models, it is also contended that these may determine unfair access to privacy and discriminatory behavior.[60] Indeed, privacy could potentially become a luxury available only to those who can afford it, while low-income users would accept subjecting themselves to an increased data collection, either for a discount, other benefit or remuneration.[61]

In contrast, other authors suggest that users are actually capable of deciding to trade their personal data "for convenience" and make their own choices on the related issues[62]; moreover these models could help users from different socio-economic contexts[63] and grant them a better control over their data as property rules would allow each individual to decide what information to disclose and protect «both those who value their privacy more […] and those who value it less».[64]

That being said, from an economic perspective individuals may indeed trade personal data and the protection of personal data similarly as a service and monetize them.[65] What remains unclear is the legal position on the lawfulness of such practices and the legal implications of recognizing them.[66] Indeed, the *Garante per la protezione dei dati personali* ("Italian DPA") has recently asked the EDPB to express an opinion on certain business models based on the commercialization of personal data, given the

[58] G. Malgieri, *Data Extra Commercium*, cit., 14-16.

[59] *Ibid.* Also, the new California Consumer Privacy Act of 2018, Civil Code §1798.100-1798.199 ("CCPA") and Title 11. Law Division 1. Attorney General Chapter 20. California Consumer Privacy Act Regulations §999.300-999.341 ("Proposed Regulations") provide that a business may offer financial incentives (i.e., «program, benefit, or other offering, including payments to consumers, related to the collection, retention, or sale of personal information») or a price or service difference to individuals for the collection of their personal data (CCPA §1798.125. (b)(1)). In such a case, individuals shall receive a «notice of financial incentive» which, among others, includes: «an explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: a) a good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and b) a description of the method the business used to calculate the value of the consumer's data» (Proposed Regulations §999.307 (b)(5)(a)-(b)).

[60] S. Elvy, *Paying for privacy and the personal data economy*, cit., 1400-1406.

[61] *Ibid.* see also Garante per la protezione dei dati personali, *Monetizzazione dati fra le sfide più delicate,* 5 October 2020: «*Ma i dati personali, prima che una risorsa economica, costituiscono un bene giuridico, oggetto di un diritto "di libertà" che come tale non può essere alienato. Una delle sfide più delicate riguarda proprio la monetizzazione dei dati. Se, infatti, si legittimasse la remunerazione del consenso al trattamento, si rischierebbe la rifeudalizzazione dei rapporti sociali, ammettendo che per necessità si possa essere disposti a cedere, con i dati, la propria libertà*».

[62] S. Elvy, *Paying for privacy and the personal data economy*, cit., 1404.

[63] *Ibid.*

[64] L. Lessig, *Code and Other Laws of Cyberspace*, New York, 1999; N. Purtova, *Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation*, in *European Journal of Legal Studies* 2010.

[65] P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, cit., 6.

[66] EDPB, *Minutes, 13th Plenary meeting*, 10 September 2019, received by the EDPB Secretariat with e-mail of 15 May 2020, includes as a point of discussion the «remuneration to data subjects/app users in exchange for their personal data».

controversial issue of the "merchantability" of personal data which are being attributed economic value.[67]
The next section explores the right to data protection to assess whether its intrinsic nature represents a limit to the merchantability of personal data.

3. The European right to the protection of personal data

The personal data monetization models described consider personal data as a "currency".[68] However, according to the EDPS, under EU law personal data cannot be reduced to a "mere economic asset", given the fundamental right's nature of the protection of personal data.[69]
The latter position is grounded in the natural law view that every human being is a bearer of innate rights that the State does not assign but simply recognizes. Therefore, as rights are inextricably linked to human nature, they are inviolable both by the State itself and by other citizens and cannot be reduced to a commodity.[70]
This section will explore data protection as a fundamental right and as a personality right to assess whether these qualifications determine a ban or restrictions on the merchantability of personal data.

3.1. Data protection as a fundamental right

"Privacy rights" in Europe encompass the right to the respect for private life (the "right to privacy") and the right to the protection of personal data.[71] These are protected as fundamental rights at European level and in national laws of EU Member States[72]: the right to privacy under Article 8 of the ECHR and Article 7 of the Charter, and the right to the protection of personal data under Article 8 of the Charter.
The right to privacy is considered an "opacity tool"[73] or a "defensive mechanism"[74], meant to protect one's personal sphere (to be intended broadly as covering the «home,

[67] Garante per la protezione dei dati personali, *Dati in cambio di soldi: il Garante privacy porta la questione in Europa. Sotto la lente dell'Autorità la app "Weople"*, 1 August 2019, concerning the request to the EDPB to express an opinion on "Weople"; however, the EDPB sent a letter to Weople, stating that the «request for an opinion […] was withdrawn by the Italian Supervisory Authority, and therefore the EDPB is no longer drafting such an opinion» [EDPB Secretariat, *Response to Hoda letter*, 21 January 2020].

[68] EDPS, *Opinion 8/2018 on the legislative package "A New Deal for Consumers"*, 5 October 2018.

[69] *Ibid.*

[70] See for example, J. Locke, *Two Treatises of Government,* Cambridge, 1988) and J. M. Finnis, *Natural Law and Natural Rights*, Oxford, 2011.

[71] P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, cit., 34.

[72] Ivi, 35-36.

[73] N. Purtova, *Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights*, in *Neth Q Human Rights*, 2010, 179 ss., spec. 182-183.

[74] Ivi, 180.

family life and correspondence, bodily integrity and decisional autonomy»)[75] from the intrusion and interference of others (the State, but also private parties).[76] On the contrary, the right to data protection is a «transparency tool»[77], «a dynamic kind of protection»[78], meant to give individuals control on how personal data are collected and used.[79] In this sense, personal data protection is broader than privacy because it addresses problems and needs underlying the processing of personal data regardless of their relationship with privacy[80] (i.e., need for transparency; automatic processing concerns), on the other, it is more narrow because it only concerns «the processing of personal information, with other aspects of privacy protection being disregarded».[81]

Based on these premises, certain authors have criticized the qualification of the right to data protection as a fundamental right, arguing that data protection interests might not justify restrictions to the freedom of contract of individuals[82], for example a prohibition to waive data protection rights.[83] In fact, the processing of personal data does not always relate to the private sphere of individuals and thus less fundamental interests are concerned.[84] However, this position is flawed as it does not take into account the evolution of privacy rights in Europe. Indeed, despite the two rights being different, they are related[85], as the right to the protection of personal data is considered intrinsic to the right to privacy under the ECHR.[86] The concept of privacy has progressively broadened - from the «right to be left alone»[87], to the right to maintain control over the flow of one's personal data and to determine how to shape «one's own private sphere».[88] Therefore, data protection in Europe is an autonomous fundamental right.[89]

That said, the fundamental right to data protection is not absolute and shall be balanced with other fundamental rights and interests. Indeed, according to the GDPR,

---

75 Ivi, 181.

76 Ivi, 187.

77 Ivi, 197.

78 S. Rodotà, *Data Protection as a Fundamental Right* in S. Gutwirth – Y. Poullet – P. de Hert (eds.) *Reinventing data protection?*, Berlin, 2010, 77 ss., spec. 79.

79 N. Purtova, *Private Law Solutions in European Data Protection,* cit., 197.

80 Ricciuto, cit., 103.

81 P. Hustinx, *EU Data Protection Law - Current State and Future Perspectives*, 9 January 2013.

82 N. Purtova, *Private Law Solutions in European Data Protection*, cit., 180.

83 C. Cuijpers, *A Private Law Approach to Privacy; Mandatory Law Obliged?*, 2007, 304, 312-313.

84 *Ibid.*

85 P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, cit., 34.

86 N. Purtova, *Private Law Solutions in European Data Protection*, cit., 181, recalling *I v Finland* (2009) 48 EHRR 31, §§ 35-36: «The processing of information relating to an individual's private life comes within the scope of Article 8».

87 S. Rodotà, *Data Protection as a Fundamental Right,* cit., 80 referring to the famous article of S. D. Warren – L. D. Brandeis, *Right to Privacy* in *Harv L Rev*, 4, 1891, 193 ss.

88 *Ibid.*

89 Article 16, Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 ("TFEU") now constitutes the legal ground for EU institutions to effectuate the right to data protection throughout the EU.

while the right to the protection of personal data should be «designed to serve mankind», «it must be […] balanced against other fundamental rights, in accordance with the principle of proportionality».[90] In particular, it refers to the fundamental right to the respect for private life[91] (which also includes the principle of autonomy/self-determination[92] and informational self-determination[93]) and the freedom to conduct a business (which also includes the freedom of contract[94]). Also, the GDPR, by ensuring uniform rules throughout the EU, pursues the economic interests related to the free movement of personal data[95], such as «the proper functioning of the internal market».[96] Such free movement of personal data shall not be «restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data».[97]

Moreover, it is arguable that the data subject in the GDPR also plays the role of a contractor and that the data subject's consent to data processing also indicates a willingness to negotiate. Otherwise, it would not be possible to explain Article 8(3) GDPR on the child's consent, which provides that paragraph 1 of the same article, setting the minimum age for a lawful expression of the child's consent, «shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child». If the European legislator had considered the consent to the processing of personal data totally unrelated to the discipline of contracts and merchantability, there would have been no need to save «the general contract law of Member States».[98]

Therefore, there is no dispute that the GDPR provides a dual approach[99] to the protection of personal data: on one side, it protects persons with regard to the processing

[90] Recital 4 GDPR.

[91] Article 7 Charter corresponding to Article 8 ECHR.

[92] See note 12 above.

[93] The ECtHR in *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* (2018) 66 EHRR 8, § 137 found that informational self-determination is part of the right to private life. P. De Hert – S. Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg,* cit., 19: this is the capacity of the individual to «have control […] of the use of personal information»; A. Rouvroy – Y. Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy* in S. Gutwirth - Y. Poullet – P. de Hert (eds.), *Reinventing data protection?*, Berlin, 2010, 45 ss., spec. 51-52: a libertarian and individualistic interpretation of the informational self-determination allows individuals to be empowered to a point where they can alienate their right to data protection.

[94] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17: Article 16 Charter "freedom to conduct a business" also covers the freedom of contract.

[95] Recitals 9-10 GDPR; A. Mantelero, *The Future of Consumer Data Protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics* in *Computer Law and Security Review*, 30, 2014, 643 ss.

[96] Recital 13 GDPR.

[97] *Ibid*; Article 1(3) GDPR.

[98] V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*", cit., 723.

[99] The need to balance the fundamental rights and the internal market economic considerations was also present in the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, Recital 3, Article 1.

of their personal data, and on the other hand, other fundamental rights and interests, aiming at the free movement of personal data[100] throughout the EU Member States, underpinned by its harmonised level of protection there.
Personal data are thus protected both as aspects of one's identity and as economic goods subject to processing and circulation.[101] Hence, an interpretation of the fundamental right to data protection in light of the GDPR does not equate to a ban on the merchantability of personal data premised on an alleged preeminence of natural persons with regard to the processing of personal data.
On the contrary, it allows (and actually mandates) the balance of the need to protect natural persons with regard to the processing of their personal data and the need to encourage freedom of economic initiative and to conduct a business, as well as the development of new services necessary to guarantee pluralism and competitiveness of the digital single market.[102] Indeed, it is against this background that the recent Proposal for a Regulation European Data Governance should be read, which aims at fostering «the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU».[103]
One further step should be made in the analysis of the right to data protection, that is the deep connection between personal data and personhood.

3.2. Data protection as a personality right

The origins of data protection in Europe are founded in the framework of personality rights.[104] It is argued that personality rights origin from the right to privacy under Article 8 ECHR.[105] As mentioned, Article 8 ECHR progressively evolved from a negative right, providing protection from arbitrary interference, into a positive one; indeed, the scope of the right to privacy has gradually broadened and interpreted as a personality

[100] Article 1 GDPR; F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018.

[101] N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, in Id. (ed.), *Persona e mercato dei dati,* cit., 35 ss., 91.

[102] Garante per la protezione dei dati personali, *Relazione annuale 2019*, cit., 124-125.

[103] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) [2020], COM(2020) 767 final 2020/0340 (COD).

[104] G. Resta, *I diritti della personalità*, in G. Alpa – G. Resta (ed), *Le persone fisiche e i diritti della personalità*, Torino, 2006, 361, 363, "personality rights" are a private-law category of civil law countries in Europe, originated from the German scholars of the nineteenth century; G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, in *Tulane European and Civil Law Forum,* 26, 2011, 34, this notion refers to a bundle of rights «aimed at the protection of the integrity and inviolability of the individual». In common law the concepts of privacy and defamation are the closest equivalents for the protection of non-economic interests of personality rights, while the right of publicity protects the economic interests.

[105] B. Van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"* in *Utrecht Journal of International and European Law*, 31(80), 2015, 25 ss. As to Article 7 Charter "right to private life", the Explanations of the Charter specify that «The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR», thus the reasoning should be the same.

right, covering the protection of all aspects of a person's identity and development[106], including «a positive freedom to control personal information».[107] As to the right to data protection, this too has its origin in Article 8 ECHR[108] and has evolved from a negative right, concerned with the obligations of data controllers[109], into a right that protects personal interests of individuals.[110] Thus, arguably, the right to data protection falls under the scope of personality rights.[111] More specifically, the right to data protection is directly related to the protection of human dignity (Article 1 of the Charter) and contributes to the «constitutionalisation of the person».[112] Personal data are linked to one's being, compose a person's digital identity as if it were a projection of the person herself, «a part of her».[113] Thus, data protection in Europe represents a tool for the protection and development of individual's personality.[114] This determines a less market-oriented approach to data protection in Europe compared to other legal systems, such as the USA.[115] Therefore, what needs to be explored is the extent to which it is possible to negotiate attributes of individuals' personality - personal data being intangible aspects.

Attributes of an individual's personality (surely intangible ones, for instance image and name) are in practice often exploited on the market[116], however the traditional position of private law scholars is to consider personality rights as absolute, inalienable and not

[106] B. Van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, cit., 44: a case falls under Article 8 ECHR when a person is affected in her «identity, personality or desire to flourish to the fullest extent». The right to privacy is interpreted «as a right that guarantees the development and expression of one's identity and personality» [*Biriuk v. Lithuania,* app no. 23373/03 (2008) § 38; *Varapnickaite-Mazyliene v. Lithuania*, app. no. 20376/05 (2012) § 43].

[107] B. Van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, cit., 44.

[108] Explanations of the Charter, cit.

[109] As provided by Article 4(7) GDPR, "data controller" means «the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law».

[110] B. Van der Sloot, *Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"*, cit., 46.

[111] Ivi, 26; H. Pearce, *Personality, Property and Other Provocations: Exploring the Conceptual Muddle of Data Protection Rights under EU Law* in *Eur Data Prot L Rev*, 4, 2018, 190 ss., spec. 193.

[112] S. Rodotà, *Data Protection as a Fundamental Right*, cit., 80.

[113] G. Alpa, *La "Proprietà" dei dati personali*, in N. Zorzi Galgano (ed.), *Persona e mercato dei dati,* cit., 11 ss., spec. 17; J.E.J. Prins (Corien), *Property and Privacy: European Perspectives and the Commodification of Our Identity*, in *Information Law Series*, 16, 2006, 223 ss., spec. 234.

[114] S. Rodotà, *Data Protection as a Fundamental Right*, cit., 80.

[115] A. Mantelero, *The Future of Consumer Data Protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics,* cit., 11: a different approach more widely accepted in the USA is to grant individuals property rights over personal information; P. Schwartz, *Property, Privacy, and Personal Data,* in *Harv L Rev*, 2004, 2056 ss., spec. 2057 referring to scholars who, given personal data have become a commodity, «have advocated propertization of personal information» and the free alienability.

[116] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 42.

subject to the statute of limitations.[117] With regard to the monetization and tradability of personal data, the EDPS stated that «there might well be a market for personal data, just like there is, tragically, a market for live human organs, but that does not mean that we can or should give that market the blessing of legislation».[118] According to the writers, the traditional view and the EDPS' statement and analogy are not properly worked through and should be clarified by introducing proper distinctions. First, personality rights have both economic and non-economic aspects; for instance, with regard to intangible attributes, honor, privacy and personal identity represent personal non-economic values, while one's name, image and personal data are intangible expressions of a person, having an economic value.[119] The latter can be commercially exploited by third parties.[120] Secondly, it is necessary to distinguish between physical attributes of personality, such as one's body and body parts, and non-corporeal attributes, such as one's image, name and personal data. Only the physical attributes cannot be commercially exploited and form the source of profits.[121] One could argue in fact that only the exploitation of physical attributes of one's personality could endanger a person's integrity, the value of human dignity and the value of equality, as differences in wealth could negatively affect people's choice to dispose of their body.[122]. More simply, our society seems more open to accepting some forms of exploitation of incorporeal aspects of personal identity, including personal data. Indeed, this is also confirmed by legislation which provides different rules for physical and incorporeal attributes of personality; for instance, Article 3 Charter introduces a «prohibition on making the human body and its parts as such a source of financial gain»[123], while no similar ban is stated with

[117] G. Resta, *I diritti della personalità,* cit., 362.

[118] EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 14 March 2017 ("EDPS 2017").

[119] S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Turin, 2018, 16.

[120] Ivi, 17 and 80 referring to the intellectual property approach to justify the tradability of incorporeal attributes of personality. Regardless of the approach chosen, incorporeal attributes of personality have an economic and tradable content; G. Resta *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 42, 50 referring to the principle of personal autonomy which «lies at the core of the continental system of personality protection» and on which basis the courts have recognized that «every individual should have the right to freely decide who, under what conditions and for which purposes may lawfully exploit aspects of his/her personality».

[121] N. Zorzi Galgano (ed.), *Le due anime del GDPR e la tutela del diritto alla privacy*, cit., 63; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 20: physical attributes are subject to the principle of gratuitousness (they can be donated), thus in this sense they are off the market.

[122] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 58. An exception could be found in a person's hair, which instead can be sold; however, technically, hair is not a live part of a person's body and, anyhow, the commercialization for an economic return does not put a person's dignity or self at risk.

[123] A similar approach is adopted in Italy (Article 5 Civil Code: «acts of disposition of one's own body are prohibited when they cause a permanent damage in physical integrity, or when violate the law, public order or morality») and France (Article 16-1 and 16-5 Civil Code: «the human body, its elements, and its products may not form the object of a patrimonial right» and «agreements that have the effect of bestowing a patrimonial value on the human body, on its elements, or on its products are null»- translation is found at Légifrance-Catalogue des traductions, "Code civil" (21 December 2015). Specific rules govern clinical trials: the Regulation (EU) No 536/2014 of the European Parliament and

regard to personal data under Article 8.[124] Thus, if personal data do not fall within the non-patrimonial scheme typical of personality rights (especially physical attributes of personality rights), then personal data can be the object of negotiation. However, this does not mean that the freedom to contract intangible aspects of personality is not subject to any limitation. Indeed, intangible attributes of personality rights can be traded and exploited by third parties with individuals' consent, but they cannot be waived[125], the commercial transaction is subject to restrictive interpretation[126] and consent is always revocable.[127] This last feature is not inconsistent with the finding of a binding commercial relationship, as it is common to conceive agreements where one or more parties have the right to withdraw at any time.[128]

In conclusion, in Europe data protection enjoys the status of a fundamental right.[129] This qualification does not entail a prohibition to trade and economically exploit personal data; however, given that data protection is rooted in the context of personality rights, personal data cannot be considered a mere commodity, and the scope of negotiation is subject to some restrictions, aimed at avoiding the risks of violation of the personal sphere.[130] The GDPR sits within this framework and, as it will be better examined below, introduces a specific regime conceived for the peculiar interests involved, under which the use (so called "processing"[131]) of personal data can take place.[132]

4. Personal data as a counter-performance: a GDPR analysis

As described in Paragraph 2, personal data have an economic value and are often

of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC [2014] OJ L158/1 states that «no incentives or financial inducements are given» to «incapacitated participants», «minors» or «pregnant women». Also, Article 28, in general, states that «no undue influence, including that of a financial nature, is exerted on subjects to participate in the clinical trial». Certain EU Member States prohibit compensation *tout court* (for instance Italy, Legislative Decree 24 June 2003, no. 211, Article 1), others require the involvement of an ethics committee.

124 G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 58.

125 H. Zech, *Data as a tradeable commodity* in A. De Franceschi (ed.), *European contract law and the Digital Single Market*, Cambridge, 2016, 51 ss., spec. 67.

126 G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 61-64, argues that this derives from the fact that the economic and non-economic aspects of personality are deeply connected.

127 As to the processing personal data see Article 7(3) GDPR.

128 S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 102-104.

129 P. Larouche – M. Peitz – N. Purtova, *Consumer Privacy in Network Industries, a CERRE Policy Report*, cit., 49; N. Purtova, *Private Law Solutions in European Data Protection*, cit., 181.

130 G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 39.

131 Article 4(2) GDPR.

132 G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 62.

exchanged for digital services/content, or for incentives, such as discounts or remuneration. Thus, personal data are considered as a de facto "price", "consideration" or "counter-performance" within a contractual relationship.[133] This reality has been taken into account by the EU legislation concerning consumer rights.[134] For instance, as mentioned in Paragraph 1 above, the Directive 2019/770 and the Directive 2019/2161 expand the protection for consumers to online contracts supplying digital services and digital content which are not paid with money, but for which consumers provide personal data[135], therefore acknowledging "payment" with personal data. While the in-depth analysis of these legal instruments is out of the scope of this paper, it is interesting to note that the language of the Directives changed compared to the initial proposals, as all references to the concept of providing personal data as a "counter-performance" have been removed and it is now specified that data protection is a fundamental right and «personal data cannot be considered as a commodity».[136]

This change reflects the dichotomy between data protection law, which restricts data collection and the possibility of tying the access to a service on the provision of consent to the processing of personal data, and consumer law, which otherwise tends to recognize the above consent as a counter-performance and to protect the transparency of market transactions. It is this ambivalence that has been noted by the EDPS which, in its opinions has expressed profound doubts on the concept of personal data as a counter-performance[137] and on whether individuals can "pay" with their personal data.[138] Overall, these opinions are not fully convincing. The reasoning for recommending the linguistic change is based on two main arguments: one is that data protection is a fundamental right and cannot be reduced to a "mere economic asset"[139], and the other regards the difficulties for individuals in understanding the value of their personal data.[140] However, it has already been argued that the first reason is not absolute and trenchant (see Paragraph 3), and the second issue could be solved by strengthening/introducing transparency rules (see Paragraph 2).

Moreover, the EDPS' concern – this instead being understandable - is to avoid the idea that personal data could always be processed with no limits when they are considered a counter-performance in an agreement.[141] On the contrary, the GDPR shall always be taken into account for the use of personal data in the digital economy.[142] Indeed, while the data protection law substantially regulates the personal data market, establishing if

133 G. Malgieri, *Data Extra Commercium*, cit., 7.

134 *Ibid.*

135 European Commission, *A New Deal for Consumers: Commission strengthens EU consumer rights and enforcement*, 11 April 2018.

136 Directive 2019/770, Recital 24.

137 EDPS 2017, cit.; EDPS, *Opinion 8/2018 on the legislative package "A New Deal for Consumers*, 5 October 2018 ("EDPS 2018").

138 EDPS 2018, cit., 3.

139 EDPS 2017, cit., 7; EDPS 2018, cit., 13.

140 EDPS 2017, cit., 9-10; EDPS 2018, cit., 13.

141 EDPS 2017, cit., 13.

142 EDPS 2018, cit., 12; EDPS 2017, cit., 3.

and when the exchange of personal data is allowed, consumer law regulates the modalities of such exchange, guaranteeing its transparency, regardless of its lawfulness. In other words, consumer protection instruments do not seem to be equipped to indicate whether it is lawful to exchange personal data on the market, but only indicate how such an exchange should be conducted. Therefore, in order to understand whether or not an exchange of personal data understood as a contractual counter-performance is lawful, it is necessary to have regard not to consumer law, but to data protection regulations and in particular, the GDPR.[143]

Thus, turning to the GDPR, this does not explicitly deal with trade and monetization of personal data; indeed, the difficulty in such situations is identifying a suitable legal basis, capable of guaranteeing the balance between the adequate protection of persons and the free flow of personal data.[144] This section will analyze the legal basis of contract (Article 6(1)(b) GDPR) and consent (Article 6(1)(a) GDPR) to examine whether they allow personal data to be exchanged as a counter-performance. To consider personal data as a counter-performance means to identify a synallagmatic/bilateral exchange between the user's personal data and the provider's service and thus to consider the processing of personal data as a condition to access the service.[145]

According to Article 6(1)(b) GDPR, personal data may be processed if "necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". The main issue is to assess the meaning of "necessary". According to the EDPB, the concept of "necessary" is to be interpreted strictly, as referring exclusively to those personal data that are "genuinely necessary" for the performance of the contract.[146] The following factors can be taken into account to assess when this is the case: (i) the «nature of the service being provided»[147] and the «distinguishing characteristics»[148]; (ii) the «rationale of the contract (i.e., its substance and fundamental object)»[149] and (iii) the «mutual perspectives and expectations of the parties to the contract»[150]; how the service is promoted or advertised.

That said, as mentioned, certain business models consider the processing of personal data as an alternative to a monetary payment in a contract, thus personal data are often compared to money ("payment" with personal data). In such cases, one could argue that personal data are indeed necessary for performing the contract, similarly as

143 S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *questa Rivista*, 3, 2019, 131 ss.

144 Garante per la protezione dei dati personali, *Relazione annuale 2019*, cit., 124-125.

145 S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., 181.

146 Article 29 Working Party ("WP29"), *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014; EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 8 October 2019.

147 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 10.

148 *Ibid.*

149 *Ibid.*

150 *Ibid.*

credit card details are necessary when a user decides to pay by credit card on an online website.[151] However, this view is strongly opposed by the EDPS as there is a risk of commodifying personal data.[152] While it is agreed that the analogy between personal data and money should be avoided (as mentioned in Paragraph 3 personal data are not fully commodifiable), the notion of "necessity" should be interpreted on a case-by-case basis. Depending on the nature of the service there may be different situations where it is arguable that the processing is necessary for the performance of a contract. For instance, a user of an online retailer may expect that among the «distinguishing characteristics»[153] of that service is the personalization of content[154], also in light of the fact that it is promoted as an «intrinsic element»[155] of such online service. Therefore, in that case it could be arguable that the processing of personal data for such purpose is necessary for performing the contract.[156] Moreover, Article 6(1)(b) GDPR - subject to a case-by-case analysis - could be a suitable legal basis for data processing in personal data economy models. In these situations, it is arguable that the substance of the agreements[157] usually coincides with carrying out online behavioural advertising or marketing to extract value from individual's personal data. Therefore, the processing of personal data for such purposes could be considered necessary for performing the agreement.[158] Again, the EDPB's opinion on this is strict: it is advanced that the processing of personal data for online behavioural advertising is *normally* not necessary for the performance of a contract and this conclusion is supported by the existence of the absolute right to object to direct marketing, including the related profiling, under Article 21 GDPR.[159] One could think that the EDPB's concern is that the contractual legal basis could entail the waiver of right to object under Article 21 GDPR – which would not be lawful. However, in the writers' opinion, the right to object under Article 21 GDPR could still be granted and enforced at any time; the exercise of such right would simply lead to the termination of the contract, which in fact could not be performed without the data processing opposed by the individual.

Finally, a further interpretation of the concept of "necessity" could be developed. It could be argued that the processing of personal data may be based on Article 6(1)(b)

151 WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, cit., 16.

152 EDPS 2018, cit., 14.

153 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 10.

154 Such as the recommendation of products users might like.

155 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 10.

156 However, see EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 16, whose opinion is very strict.

157 29WP, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, cig., 17 referring to the importance «to determine the exact rationale of the contract…, as it is against this that it will be tested whether the data processing is necessary for its performance».

158 This situation is different from the one described by 29WP (n 137) 17.

159 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 14-15.

GDPR when it is "financially necessary" to perform a contract (for example, a "free" social network collects personal data for online behavioural advertising to fund its service). However, the EDPB's opinion is that the processing of personal data which supports the provision of a service is «*in itself* not sufficient to establish that it is necessary for the performance of the contract».[160] Therefore, for the time being, a "financial necessity" concept is still unsupported and the provider's business model is only one of the factors to consider for a data processing to be necessary, together with the others listed above. Nevertheless, if a hypothetical data processing is found "financially necessary" to perform a contract, the data processing would still need to comply with the GDPR general principles, such as fairness and transparency, purpose limitation and minimization principles.[161] Also, ideally, strict transparency obligations should be introduced; for instance, the data controller – in compliance with the accountability principle[162] - would need to adequately reason the "financial necessity", explaining that although the requested service can be provided without that specific processing (i.e., objective necessity[163]), it cannot be financially supported; moreover, it would need to disclose the methods to evaluate personal data, the value of personal data and the amount and type of personal data necessary to support that service and thus perform the contract.

As to the legal ground of consent under Article 6(1)(a) GDPR, this shall be free and revocable.[164] Consent is freely given if individuals have «real choice and control»[165] on the use of their personal data and may refuse consent without detriment and withdraw consent easily at any time.[166] Article 7(4) GDPR specifies that «when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract». Also, Recital 43 GDPR provides that: «Consent is presumed not to be freely given […] if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance».

In other words, there is a presumption that consent to data processing is not freely given - and thus is invalid - when it is a condition for the provision of a service (i.e., consent to data processing as a counter-performance in an agreement).[167] Article 7(4) GDPR has been the object of an intense debate regarding its interpretation. On one side, scholars argue that this provision does not introduce a ban on the possibility to establish a link between the provision of the service and consent to data processing

160 Ivi, 15.

161 Articles 5.1.a-c GDPR.

162 Article 5.2 GDPR.

163 EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, cit., 9.

164 Recitals 32, 42, 43, Articles 4(11), 7 GDPR.

165 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020.

166 Recital 42; Article 7(3) GDPR.

167 G. Malgieri, *Data Extra Commercium*, cit., 7.

and argue for a flexible approach[168], on the other, the EDPB[169] and certain DPA's[170] have a stricter view and observe that «there might be very limited space for cases where this conditionality would not render the consent invalid»[171] and it is likely unusual to rebut the presumption that «bundled consent is not freely given».[172] Clearly, adopting one view or the other affects the extent to which personal data can be commercialized and monetized on the basis of consent.

A careful reading of the EDPB's opinion on Article 7(4) GDPR[173] brings to the following considerations. The EDPB's explicit statement that consent to data processing «cannot become directly or indirectly the counter-performance of a contract»[174] should be interpreted in the sense that consent to the unnecessary processing of personal data cannot be construed always and in any circumstances as «a mandatory consideration in exchange for the provision of a service».[175] However, consent to data processing can be incentivized and still be considered free.[176] Thus, the issue is to distinguish between a non-permissible and a permissible incentive, which would allow individuals to obtain "free" services, or a discount or remuneration, in exchange of their personal data.

The following factors may be considered to assess the freedom of consent: (i) whether there is a «genuine choice»[177] between a service that requires consenting to personal data processing for additional purposes and an «equivalent service»[178] which does not require such consent; (ii) whether those who do not give or withdraw their consent are «unfairly penalized»[179]; (iii) an imbalance of powers between individuals and the data controller[180]; and (iv) the level of transparency of data processing.[181]

As to (i), a genuine choice should concern a "genuinely equivalent service" offered by the same data controller (alternatives offered by third parties on the market are irrelevant[182]). It is arguable that a paid service with no collection of personal data for additional purposes is a genuine alternative to a "free" service with the users' bundled

168 G. Resta – V. Zeno-Zenovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile* 2, 2018, 411 ss., spec. 430; A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, in *JIPITEC*, 8, 2017, 5 ss.; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 96; G. Malgieri, *Data Extra Commercium*, cit., 8.

169 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit.

170 Information Commissioner's Office ("ICO"), *Consent*, 22 March 2018.

171 EDPB, cit., 10.

172 ICO, cit., 10.

173 EDPB, cit.

174 Ivi, 9.

175 *Ibid.*

176 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 12.

177 Ivi, 10.

178 *Ibid.*

179 ICO, *Consent*, cit., 24.

180 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 7-8.

181 Ivi, 14-16.

182 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 10.

consent to additional data processing[183] (for example, a fee to use the wi-fi at the airport with no collection of unnecessary personal data versus a "free" wi-fi at the airport with personal data processing for marketing).[184] The argument that a paid service is a genuine alternative to a "free" service is also supported by the fact that the Article 29 Working Party's revised guidelines on consent do not include anymore the specification that the equivalent service shall not include "further costs".[185] Also, it seems permissible that an online retailer offers a certain discount only to the users that consent to receiving a newsletter, while those who do not want to give their consent would only be able to access the retailer's website and receive general discounts during the end-of-season sale. As to (ii), the refusal or withdrawal of consent should be without detriment[186], that is with no disadvantages[187]. If a user chooses to "pay" with data instead of money and then withdraws her consent, the consequence would be the denial of the "free" service, while the paid alternative would still be available[188]; this however does not amount to a disadvantage, as the loss of a permissible incentive does not entail a detriment for the individual.[189] Moreover, an imbalance of powers (point iii) may occur in situations where (a) there are negative consequences if the individual does not consent, such as "substantial extra costs"[190], or (b) if «there is an element of compulsion, pressure or inability to exercise free will».[191] A reasonable fee or the loss of a discount do not seem to imply "substantial extra costs".[192] Also, arguably the request of a bundled consent in certain contexts, such as by an online retailer or in a recreational context[193], does not imply a negative pressure on the user. On the contrary, it would not be permissible for a health care provider to offer "free" health care only to individuals consenting to targeted advertising, and, as an alternative, a paid health care service to those who do no consent to additional data processing. Indeed, individuals suffering of health issues are in a position of vulnerability and could feel a negative pressure to consent to unnecessary data processing to gain access to free health care.[194] Thus, the nature of the service should also be taken into account: when the service provided in exchange for

183 G. Malgieri, *Data Extra Commercium*, cit. 8.

184 The fee must be "reasonable": in line with the market rates applied in similar cases (e.g. hotels or other accommodation facilities), so that the option to use the wi-fi with monetary payment is an effective alternative and not only a theoretical one.

185 29WP, *Guidelines on Consent under Regulation 2016/679*, 28 November 2017.

186 Recital 42 GDPR.

187 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 11, 22 refers to «lowering the service level».

188 According to S. Thobani (*Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 188) this derives from the fact that consent to data processing is the counter-performance to access the service.

189 EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., 12.

190 Ivi, 8.

191 *Ibid.*: in relationships with public authorities or employers.

192 D. Zetoony, *Does the GDPR prohibit charging more to consumers that do not consent to certain types of processing?*, in *bclplaw.com*, 8 June 2020.

193 A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, cit., 5.

194 29WP, *Opinion 15/2011 on the definition of consent,* WP187, 13 July 2011.

consent to data processing is essential[195] and of particular importance for an individual, consent to data processing could be unduly conditioned.[196] Finally (point iv), not only individuals should receive a clear information notice on the use of their personal data, but also an explanation of the commercial nature of the transaction, where personal data represent the counter-performance in the agreement[197], the consequences of consenting or withdrawing such consent, and the value of their personal data.[198]

That said, different approaches have been adopted regarding the notion of free consent and the interpretation of Article 7(4) GDPR. For instance, the Italian DPA has been consistent in the strict interpretation of free consent in the sense that consent is not free where access to a good or service is subject to giving consent[199]. For instance, recently, it found unlawful to require individuals to give their consent to marketing activities in order to gain access to certain discounts and to enter prize competitions[200]; as to the ICO, it is noteworthy to refer to a case where it warned the Washington Post that its online practice did not comply with the GDPR. More specifically, the Washington Post required its users to choose between (a) consenting to cookies in order to obtain "free" access to a limited amount of articles; (b) paying a basic subscription fee, plus consenting to cookies in order to access to an unlimited number of articles; or (c) paying a higher subscription fee without the need to consent to personal data collection through cookies in order to access to an unlimited number of articles. This consent was not considered freely given as there was no «*free* alternative to accepting cookies on its website» and the Washington Post should ensure access to all levels of subscription without users having to consent to the use of cookies.[201] On the contrary, in a similar case where access to an online newspaper was conditional on consenting to the use of cookies, the Austrian DPA found that consent was freely given as individuals «did not face significant negative consequences since they could choose to subscribe to the site for a small fee or simply choose another online newspaper as a source of information».[202] Finally, an interesting view has been expressed by the Italian Supreme Court[203] which clearly affirmed that the «exchange of personal data»[204] is not

[195] S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 167 referring to remuneration in an employment relationship, banking, financial and health services.

[196] *Ibid.*

[197] This work is focused only on data protection; however, transparency and fairness should be guaranteed also through the application of the consumer protection legislation (see for example note 52).

[198] G. Malgieri, *Data Extra Commercium*, cit., 14-16.

[199] For instance, see Italian DPA, Decision no. 2542348, 4 July 2013, according to which «the consent given is not free when the company conditions the registration to its website and, consequently, also the access to its services, to the user's consent to the processing of personal data for promotional purposes».

[200] Italian DPA, Decision no. 9256486, 15 January 2020.

[201] ICO, Case Reference Number: RFA0768934, 11 October 2018.

[202] H. Andrews Kurth LLP, *Austrian DPA Issues Decision on Validity of Cookie Consent Solution*, in *lexology.com*, 7 January 2019; *Datenschutzbehörde* (Austrian DPA), "*Bescheid vom* 30.11.2018, GZ: DSB-D122.931/0003-DSB/2018", 30 November 2018, accessed 30 July 2020.

[203] Cass. civ. 2 July 2018, no. 17278, in *Guida al diritto,* 2018, 31, 20.

[204] *Ibid.*

prohibited as long as it is «the result of consent which is not coerced»[205]; in this specific case, it found permissible to subject access to a service to consent to unnecessary data processing, provided that such a service is "fungible", i.e., similar alternatives are available on the market, and not "indispensable", that is non-essential for the individual.[206] Following this reasoning, as money is by definition fungible, it should be permissible to offer remuneration in exchange of personal data, as individuals who do not want to give their consent to personal data processing could find alternative ways to obtain remuneration.[207]

In conclusion, strictly speaking, some of these positions do not follow the EDPB's opinion in full[208]; in fact, the ICO refers to the necessity that the genuine alternative is also "free" - while this condition has been removed by the EDPB; and the Austrian DPA and Italian Supreme Court to the existence of alternatives offered by third parties - while the EDPB refers only to the alternatives offered by the same data controller.

Notwithstanding the lack of uniformity, it could be arguable that the GDPR does not prohibit the commercial exchange and monetization of personal data. However, the general limit to creating a link between the performance of a contract/provision of a service and the processing of personal data as a counter-performance is to not unduly condition individuals.

5. Conclusion

Personal data-centered business models are a clear index of the economic value of personal data and that these are being traded and monetized on the market. This paper has acknowledged the benefits and downsides of these businesses and reasoned on the lawfulness of such practices. The possibility to exchange personal data in return for products/services or other incentives (i.e., personal data as a counter-performance in an agreement) depends on the approach to the right to data protection. In Europe, the right to data protection is a fundamental right and a personality right. Thus, there is a tension between the protection of personal data as intangible aspects of a person's identity – our digital soul – which argues for the inalienability of personal data - and the exploitation of their economic value. This tension can be solved by considering that (i) the fundamental right to data protection is not absolute and shall be balanced with the freedom to conduct a business and to contract and the free flow of personal data and that (ii) intangible aspects of personality rights can indeed be traded with the limit of their non complete alienation. This paper then assesses the specific rules governing personal data processing. It analyses the GDPR legal bases of contract (Article 6(1)(b)) and consent (Article 6(1)(a)) as possible grounds to justify the tradability of personal data. Given the current rigid interpretation of the lawful basis for contracts,

205 *Ibid.*

206 *Ibid.,* the service consisted in an online newsletter.

207 S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali,* cit., 168.

208 It is noted that these opinions are not binding.

the legal ground of consent seems to be preferable. This work concludes that, while it is discouraged to ask individuals to provide their personal data in exchange for an advantage or as an alternative to money, there is room to interpret the legal basis under Article 6(1)(a) GDPR (consent) in ways that could allow the commercialization and monetization of personal data if that consent is "freely" given,[209] depending on a case-by-case analysis. In essence, individuals should be given a genuine choice between a service that is conditional on consent to personal data processing for additional purposes and an equivalent service that does not require such consent. Also, the service concerned should not be essential, as individuals would be unduly conditioned. Finally, individuals should be able to choose consciously by clearly understanding the nature, the convenience, and the consequences of these type of agreements. This last aspect requires the enforcement of existing transparency rules and the introduction of new ones. Following this approach, there might be business models offering product/service differentiation based on users' privacy preferences[210] and many more offering personal data remuneration. It would then be left to service providers to conceive solutions which are more attractive for users so to lawfully incentive them to provide their personal data[211] and to data protection authorities to supervise these and prevent risks to individuals' dignity and personality.[212]

[209] G. Malgieri, *Data Extra Commercium*, cit., 8.

[210] R. Auf Der Maur – D. Fehr-Bosshard, *Data Monetization and User Consent: better privacy or more bureaucracy?*, in *vischer.com,* 6 September 2017, 247.

[211] Ivi, 248.

[212] G. Resta, *The new frontiers of personality rights and the Problem of Commodification: European and Comparative Perspectives*, cit., 433-434.

La necessaria applicazione dei principi di *data protection* al diritto di accesso dei consiglieri *ex* art. 43, c. 2, TUEL*

Valentina De Nicola

Abstract

Il contributo intende analizzare la necessità di individuare alcuni limiti all'esercizio del diritto *sui generis* riconosciuto dall'art. 43, c. 2, TUEL ai consiglieri comunali e provinciali, connessi al rispetto del diritto alla riservatezza ed alla protezione dei dati personali, ripercorrendo il cammino della tematica così come analizzata dalla giurisprudenza di merito e di legittimità in Italia a partire dal 2018, ricostruendo il frammentario quadro della disciplina normativa di tale ampio istituto e definendone i limiti e le esclusioni attraverso un'applicazione ragionata dei principi di *data protection*. La tematica, infatti, è stata sino ad oggi affrontata in un'ottica miope, che non consente la completa attuazione dei principi introdotti dal Regolamento (UE) 2016/679, e che ha visto per molto tempo la risoluzione del problema della tutela del dato personale dei soggetti interessati relegata alla semplice tutela, *ex post* rispetto all'esercizio del diritto, della riservatezza personale, richiamando i consiglieri al dovere di segreto in merito alle informazioni ottenute.

This paper aims at analysing the need for limits to the sui generis right, granted by art. 43, para. 2, TUEL to municipal and provincial councillors, on the respect of right to privacy and data protection. This has been considered throughout its history as analysed by the proper law and with its lawfulness in Italy since 2018, gathering all the pieces of regulations and laws of this wide institution, defining its limitations and exclusions, through the appropriate application of the data protection principles. The shortsighted analysis of this topic so far has not allowed for the full implementation of the EU regulation 2016/679 principles and has limited the issue of the personal data protection to the sole protection, ex post to the execution of the law, of personal privacy, bounding councillors to the obligations of confidentiality and secrecy.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Sommario

1. Introduzione. L'esercizio del diritto di accesso del consigliere comunale e l'atteggiamento miope nei confronti della *data protection*. - 2. Profili giuridici del diritto di accesso *ex* art. 43, c. 2, TUEL. - 2.1. L'accesso ai sensi dell'art. 43, c. 2, TUEL come trattamento di dati personali. - 3. Il ruolo del consigliere comunale (e provinciale) nell'organigramma *data protection*: il consigliere come autorizzato al trattamento dei dati. - 3.1. Il consigliere come titolare del trattamento al momento della violazione privacy. - 4. I profili di applicazione del Reg. (UE) 2016/679 all'esercizio dell'accesso *ex* art. 43, c. 2, TUEL. - 5. Il caso concreto: la richiesta di accesso da remoto al protocollo informatico e ad altri gestionali comunali. - 5.1. Una breve disamina dei precedenti giurisprudenziali: la tutela dei dati personali come diritto "tradito". - 5.2. Valutazioni sui profili applicativi dei principi fondamentali del trattamento dei dati personali all'accesso *ex* art. 43 TUEL: artt. 5, 24, 25 e 32 del Reg. (UE) 2016/679. - 5.3. Il cambio di rotta nella giurisprudenza. La sentenza n. 253/2020 TAR Friuli-Venezia Giulia. - 5.4. Il caso specifico: l'utilizzo illegittimo delle informazioni acquisite a seguito dell'esercizio del diritto di accesso. - 6. Riflessioni conclusive: sulla necessità di un bilanciamento tra i due interessi costituzionalmente garantiti, anche alla luce dell' art. 86 Reg. (UE) 2016/679. - 6.1. Conclusioni. Gli strumenti del bilanciamento: l'applicazione dei principi di *data protection* al diritto di accesso *ex* art. 43, c. 2, TUEL.

Keywords

accesso amministrativo – consiglieri - protezione dei dati personali – trasparenza - bilanciamento.

1. Introduzione. L'esercizio del diritto di accesso del consigliere Comunale e l'atteggiamento miope nei confronti della *data protection*

Sebbene la materia della protezione dei dati personali abbia trovato recentemente una grande attenzione da parte di operatori ed interpreti in quasi tutti i settori potenziali di applicazione, un atteggiamento miope nei confronti della stessa si deve registrare, a ben due anni dalla piena applicazione della disciplina comunitaria, con riferimento all'esercizio del diritto di accesso riconosciuto specificamente al consigliere comunale e provinciale dall'art. 43, c. 2, TUEL. Tale diritto, previsto nel nostro ordinamento al fine di facilitare l' espletamento delle funzioni istituzionali riconosciute a tali soggetti qualificati, benché si scontri potenzialmente con la tutela del soggetto che, ai sensi della l. 241/1990, chiameremo "controinteressato", è da sempre definito come diritto ampio, privo di limiti prodromici al suo esercizio, soggetto ad un mero controllo successivo nell' ottica del dovere di segreto che si impone sui soggetti attivi di tale fattispecie. Storicamente il problema della tutela della riservatezza dei soggetti eventualmente coinvolti dall' esercizio di tale diritto, che ci si appresta qui ad analizzare,

è stato risolto in modo molto semplice e lineare dalla dottrina e dalla giurisprudenza interessate: la tutela del diritto alla riservatezza dei terzi eventualmente coinvolti dalla richiesta di accesso non può essere opposta come limite specifico al diritto *ex* art. 43, c. 2, TUEL, considerato che il consigliere è in ogni caso tenuto al vincolo del segreto[1].
In sostanza, la soluzione unitariamente prospettata con riferimento al problema della tutela della riservatezza nel caso di specie concerne una tutela riconosciuta solamente *ex post* rispetto all'esercizio di tale diritto *sui generis*: ci si occupa della riservatezza solo dopo che il consigliere abbia acquisito le informazioni richieste, ponendo l'attenzione sul come eventualmente egli utilizzi questi dati.
Si ritiene sia proprio questa prospettata soluzione, unita alla confusione dei confini tra riservatezza personale e tutela dei dati personali come oggi la conosciamo, ad aver determinato una sorta di blocco nel sistema di corretta applicazione delle norme, tale per cui per molto tempo la *data protection* non sembrava poter trovare spazio adeguato nell'espletamento di tale specifico diritto di accesso.
Considerato però che l'esercizio di tale diritto di accesso comporta delle innegabili ricadute sulla tutela dei dati personali e sulla riservatezza degli interessati dei quali sia fatta menzione nei documenti oggetto di accesso, che non possono essere analizzate e risolte sotto la sola lente dell'obbligo di segreto, oggi si impone ad interpreti ed operatori del diritto una necessaria riflessione in merito. È necessario adottare un atteggiamento di apertura, volto ad indagare quale sia il vero ruolo che l' ordinamento deve essere in grado di riconoscere al diritto alla tutela dei dati personali anche con riferimento a questa fattispecie, rilevato come il diritto alla *data protection* assurga a diritto di rango costituzionale, che per sua natura ha la capacità di porsi in confronto continuo con gli altri interessi costituzionalmente riconosciuti e garantiti[2], e che non può certamente essere eliso aprioristicamente dall' equazione.
La questione è oggi particolarmente pregnante, se si considera anche che le richieste di accesso dei consiglieri seguono il progressivo e radicale processo di digitalizzazione dell'organizzazione e dell'attività amministrativa: sono particolarmente diffuse, infatti, le richieste aventi ad oggetto la possibilità di accedere ai gestionali informatici degli Enti (le istanze più diffuse hanno ad oggetto l' accesso al protocollo informatico ed al programma di contabilità), i quali si compongono anche, senza ombra di dubbio, di dati personali secondo la definizione data dall' art. 4, n. 6, Reg. (UE) 2016/679 al concetto di "archivio"[3]. Risulta sempre più necessario, dunque, procedere ad un'ana-

[1] Si veda, sul punto, TAR Sardegna, sez. II, 20 maggio 2014, n. 360, ma anche la più recente Trib. Trani, sez. Lavoro, 9 gennaio 2020, che ricorda come «Il diritto di accesso del consigliere comunale non conosce né i vincoli, né le limitazioni previsti dall'ordinario accesso di cui alla legge n. 241 del 1990, ed in particolare quelli relativi alla riservatezza dei terzi. La legge non prende dunque in considerazione la posizione di coloro che potrebbero opporsi all'accesso (cui accorda come unica protezione l'obbligo del segreto a carico del consigliere comunale, con possibilità di far eventualmente valere nelle sedi competenti la violazione di tale obbligo) e pertanto non è configurabile in materia alcun contro interessato».

[2] Cfr. A. Soro, *Discorso del presidente, in apertura alla presentazione della Relazione Annuale del 2019*, in *garanteprivacy.it*, laddove il diritto alla protezione dei dati personali è stato definito come «un diritto inquieto, perché in costante evoluzione e mai tiranno, perché capace di porsi sempre in equilibrio con gli interessi giuridici che di volta in volta vengano in rilievo».

[3] Si veda art. 4, n. 6, Reg. (UE) 2016/679 che definisce l'archivio come «qualsiasi insieme strutturato

lisi che tenga conto anche di principi di *data protection*, al fine di poter individuare il necessario e continuo contemperamento tra esigenza di accesso ai documenti ufficiali della Pubblica Amministrazione, da un lato, e la necessità di tutelare i dati personali dei soggetti eventualmente interessati, dall'altro[4].

Non solo. È di fondamentale importanza valutare come i principi concernenti la tutela dei dati personali si relazionino con tale diritto *sui generis*, al fine di evidenziare se lo stesso possa effettivamente dirsi privo di limitazioni prodromiche con riferimento al suo esercizio, o se invece, più coerentemente, esso debba essere riportato all' interno dei binari di cui agli artt. 5, 24, 25 e 32 Reg. (UE) 2016/679.

Tali considerazioni, che non si riflettono in un mero tuziorismo giuridico, si impongono come irrinunciabili considerato che, per l'Ente richiesto, risulta estremamente problematico determinare i limiti eventuali da apporre all'esercizio di tale diritto, stante l'assenza, ad oggi, di linee guida specifiche per effettuare il bilanciamento degli interessi in gioco, rilevato inoltre l'elevato rischio di contenzioso che si prospetta in tali casi a carico delle stesse Amministrazioni (per iniziativa del consigliere, nel caso l'accesso sia negato e/o sia parzialmente consentito, oppure per iniziativa dei controinteressati, nel caso in cui l'accesso sia consentito in modo integrale, senza limitazioni dipendenti dalla protezione dei loro dati personali).

Nel presente lavoro si cercherà pertanto di esporre le ragioni che consentono di affermare la necessaria applicazione dei principi di *data protection* all'esercizio del diritto di accesso *ex* art. 43, c. 2, TUEL, onde ricavare un sistema di tutele integrato che operino non solo *ex post* ma anche *ex ante*, all'atto della richiesta da parte del consigliere, nel pieno rispetto dei principi espressi dal Reg. (UE) 2016/679.

2. Profili giuridici del diritto di accesso ex art. 43, c. 2, TUEL

Prima di procedere con l'analisi ragionata delle motivazioni che consentono di affermare la necessaria applicazione dei principi di *data protection* all'esercizio del diritto di accesso specificamente riconosciuto a favore di consiglieri comunali e provinciali, si ritiene necessario evidenziare qui di seguito i tratti somatici di questo istituto, utili per una più corretta analisi della fattispecie. Il diritto di accesso in commento concerne la previsione normativa di cui all'art. 43, c. 2, del d.lgs. 267/2000 (TUEL), per cui i consiglieri comunali e provinciali, sia di maggioranza che di minoranza, hanno diritto di ottenere dagli uffici del Comune, nonché dalle loro aziende ed enti dipendenti, «tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato»[5]. L' articolo in questione riprende le disposizioni normative in materia di

di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico».

[4] Tale richiamo alla necessità di bilanciamento risulta previsto inoltre *ex professo* dal Regolamento (UE) 2016/679 (di seguito anche "Reg. (UE) 2016/679"), al considerando 154 ed all'art. 86 di cui si dirà in seguito.

[5] Nello specifico, la norma rubricata «diritti dei consiglieri» prevede che «I consiglieri comunali e provinciali hanno diritto di ottenere dagli uffici, rispettivamente, del comune e della provincia,

accesso agli atti, per finalità istituzionali, già individuate espressamente dall' art. 31, c. 5, della legge n. 142/1990, che hanno storicamente delineato un diritto di accesso per i consiglieri, ampio, non sottoposto ad alcuna valutazione preventiva da parte dell' Amministrazione richiesta (che non può indagarne le motivazioni), i cui unici limiti si individuano nel richiamo al riserbo effettuato oggi dallo stesso art. 43 TUEL, e nel disposto giurisprudenziale per cui la richiesta di accesso debba essere tesa «a comportare il minor aggravio possibile per gli uffici comunali e che non debba sostanziarsi in richieste assolutamente generiche ovvero meramente emulative[6]».

Nello specifico, tale diritto *sui generis,* che trova le sue radici nelle prerogative costituzionalmente garantite agli artt. 3 e 97 Cost., risulta ad oggi privo di limitazioni, purché vi sia una stretta inerenza tra il documento e le informazioni che vi sono contenute rispetto allo svolgimento del mandato elettivo dei soggetti qualificati a favore dei quali il diritto è riconosciuto: la *ratio* dello stesso è da rinvenire nel principio democratico dell' autonomia locale e della rappresentanza esponenziale, sicché lo stesso è direttamente funzionale non tanto all' interesse del consigliere, ma alla cura dell' interesse pubblico connesso al mandato conferito, controllando il comportamento degli organi decisionali dell' Amministrazione[7].

Si tratta, all'evidenza, di un diritto dai confini più ampi del diritto di accesso riconosciuto al cittadino nei confronti del Comune di residenza (art. 10 TUEL) o, più in generale, nei confronti della Pubblica Amministrazione, disciplinato dalla legge n. 241 del 1990. La *ratio* di tale maggiore ampiezza si ricava nel particolare *munus* espletato dal consigliere comunale: un diritto di accesso dai confini così ampi viene riconosciuto per permettere al consigliere di valutare con piena cognizione di causa la correttezza e l' efficacia dell' operato dell' Amministrazione, onde poter esprimere un giudizio consapevole sulle questioni di competenza della P.A., «opportunamente considerando il ruolo di garanzia democratica e la funzione pubblicistica da questi esercitata, soprattutto se, come nel caso di specie, il consigliere comunale appartenga alla minoranza, istituzionalmente deputata allo svolgimento di compiti di controllo e verifica dell'operato della maggioranza[8]». Da ciò ne discende la definizione ampia dei limiti riconosciuti dall' ordinamento a tale diritto, tutti intrinsecamente legati alla funzione di garanzia svolta dal consigliere, tale per cui dovranno essere rispettate alcune forme e modalità di esercizio occorrendo valutare di volta in volta se «le istanze di

nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato. Essi sono tenuti al segreto nei casi specificamente determinati dalla legge».

6 Cfr. *ex multis* Cons. Stato, sez. IV 12 febbraio 2013, n. 846, Cons. Stato, sez. V, 29 agosto 2011, n. 4829 e recentemente TAR Campania, sez. VI, 7 novembre 2018, n. 6480. Si tenga anche conto del parere del 9 aprile 2014 fornito dalla Commissione per l'Accesso ai Documenti Amministrativi presso la Presidenza del Consiglio dei Ministri, laddove si prevede che il riconoscimento del diritto di accesso dei consiglieri di cui all'art. 43 TUEL «incontra il limite funzionale per cui tale strumento non dev'essere piegato a strategie ostruzionistiche o di paralisi dell'attività amministrativa, con istanze ripetute che, a causa del loro numero, possano tradursi in un aggravio se non nella paralisi del lavoro negli uffici ai quali sono rivolte».

7 Cfr. Cons. di Stato, sez. V, 2 gennaio 2019, n. 9 e TAR Emilia-Romagna, 20 gennaio 2020, n. 16.

8 Cfr. parere del 28 ottobre 2014 fornito dalla Commissione per l'Accesso ai Documenti Amministrativi presso la Presidenza del Consiglio dei Ministri.

accesso siano irragionevoli, sproporzionate e come tali se abbiano o meno aggravato gli uffici pregiudicandone la funzionalità[9]». Ed ancora, la *ratio* della norma determina conseguentemente l' impossibilità, per l' Amministrazione destinataria, di richiedere al consigliere l' adduzione di una prodromica specifica motivazione per l' accesso, considerato che essa appare «illegittima in quanto volta a costituire un ingiustificato limite all' accesso[10]».

Inoltre, per ciò che più qui interessa, si deve osservare come la risalente e consolidata giurisprudenza amministrativa di merito e di legittimità (*ante* Reg. (UE) 2016/679) si sia sempre espressa confermando come il diritto *ex* art. 43, c. 2, TUEL non incontri alcuna limitazione derivanti da esigenze di riservatezza o privacy dei terzi, in quanto il consigliere è vincolato all'osservanza del segreto[11]; secondo tale interpretazione giurisprudenziale, dunque, è proprio il richiamo al riserbo, operato dall'art. 43, c. 2, TUEL dove prevede che «essi sono tenuti al segreto nei casi specificamente determinati dalla legge» a ricondurre la fattispecie nell' alveo di applicazione della disciplina relativa alla riservatezza personale, evidenziandosi come tale diritto non operi come limite preventivo all' esercizio di accesso ma costituisca un interesse tutelato solamente a posteriori, a mezzo degli strumenti di salvaguardia già riconosciuti con altre specifiche norme dal nostro ordinamento.

L'interpretazione prevalente, prima della piena applicabilità nel nostro ordinamento del Reg. (UE) 2016/679 e della disciplina da esso conseguente in materia di protezione dei dati personali, era meramente incentrata sul concetto di privacy intesa come diritto alla riservatezza (il famoso "diritto ad essere lasciati soli") e faceva leva sull'assunto per cui «l'art. 43, comma 2, D.Lgs. 18 agosto 2000, n. 267, prevede infatti che i consiglieri comunali sono tenuti al segreto nel caso accedano ad atti che incidono sulla sfera giuridica e soggettiva di terzi[12]», essa risolvendosi così in un mero limite all' uso che il consigliere possa fare delle informazioni di cui è venuto a conoscenza, a seguito del positivo esperimento del diritto allo stesso riconosciuto.

Si anticipa in questa sede come, analizzato il diritto alla protezione dei dati personali e definito lo stesso come interesse costituzionalmente garantito, il richiamo al mero segreto non appare più una soluzione sufficiente tesa a garantire il rispetto di questo diritto dai tratti ben più ampi rispetto al diritto alla riservatezza personale, rendendosi necessarie le seguenti riflessioni.

---

[9] *Ibid.*

[10] *Ibid.* La Commissione specifica come «il consigliere comunale non deve motivare la propria richiesta di informazioni e documenti, perché, altrimenti, la P.A. si ergerebbe impropriamente ad arbitro delle forme di esercizio delle potestà pubblicistiche dell'organo deputato all'individuazione ed al perseguimento dei fini collettivi, con la conseguenza che gli uffici comunali non hanno il potere di sindacare il nesso intercorrente tra l'oggetto delle richieste di informazione e le modalità di esercizio della funzione esercitata dal consigliere comunale (in tal senso la Commissione si è già espressa, tra gli altri, con parere del 29 11 2011)».

[11] Si vedano, sul punto Cons. Stato, sez. V 11 dicembre 2013, n. 5931, Cons. Stato, sez. V 17 settembre 2010, n. 6963 e Cons. Stato, sez. V 4 maggio 2004, n. 2716, nonché TAR Lazio, sez. I, n. 171/2013.

[12] Cfr. Cons. Stato, sez. V 4 maggio 2004, n. 2716.

2.1. L'accesso ai sensi dell'art. 43, c. 2, TUEL come trattamento di dati personali

La domanda che necessita di trovare riscontro, oggi, concerne se e come il Reg. (UE) 2016/679 possa trovare corretta applicazione nella fattispecie di diritto di accesso sin qui descritta, e per rispondere si ritine necessario, in primo luogo, ridefinire i connotati del diritto di cui all'art. 43, c. 2, TUEL, analizzandolo sotto la lente di ingrandimento della definizione di trattamento di dati personali fornita dal legislatore europeo.
In particolare, l'art. 4 definisce il trattamento di dato personale come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione». Se si tiene presente che, non di rado, le informazioni e le notizie alle quali i consiglieri accedono possono contenere dati personali, riferiti dunque a persone fisiche secondo la definizione data anche qui dall'art. 4 Reg. (UE) 2016/679[13], attraverso la mera lettura della norma, appare chiaro come l'esercizio del diritto riconosciuto ai sensi dell'art. 43 TUEL determini sicuramente e nella maggior parte dei casi, il trattamento di dati personali appartenenti ai soggetti eventualmente coinvolti.
Più precisamente, laddove le notizie e le informazioni oggetto della richiesta di accesso contengano dati personali, l' espletamento del diritto con riscontro positivo da parte dell' Amministrazione richiesta individuerà un' operazione di comunicazione, contemplata specificamente nel nostro ordinamento all'interno dell'art. 2-*ter* d.lgs. 196/2003[14].
Ciò attrae inevitabilmente il diritto di cui all' art. 43, c. 2, TUEL nell'alveo applicativo della disciplina normativa di *data protection*, determinando la necessità, come già sopra anticipata, di superare e ampliare l'assunto che relega la riservatezza personale al mero dovere di segreto, al fine di applicare correttamente, anche a questo trattamento, tutti i principi che ispirano la tutela dei dati personali.

[13] Si veda, per la definizione di soggetto interessato e per la definizione di dato personale, l'art. 4, n. 1, Reg. (UE) 2016/679.

[14] Si veda, per la definizione di comunicazione l'art. 2-*ter* d.lgs. 196/2003, dove si prevede al c. 4 che «Si intende per: a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione».

3. Il ruolo del consigliere comunale (e provinciale) nell'organigramma *data protection*: il consigliere come autorizzato al trattamento dei dati

Al fine di meglio valutare la fattispecie, si ritiene inoltre necessario analizzare come possa configurarsi il ruolo del consigliere comunale nell'ambito dell'organigramma privacy di cui al combinato disposto degli artt. 4, 28 e 29 del Reg. (UE) 2016/679 nonché dall' art. 2-*quaterdecies* d.lgs. 196/2003.

In premessa, si ritiene opportuno definire, per brevi cenni, la titolarità del trattamento nell' Ente Pubblico ai sensi dell' art. 4, n. 7, Reg. (UE) 2016/679; in particolare, il titolare del trattamento si identifica come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali[15]». La lettura della norma consente di stabilire come, per l' Ente Pubblico, il titolare del trattamento debba essere individuato nell' autorità pubblica, e dunque nella persona giuridica in sé considerata[16]. Allo stesso modo si deve ricordare come, per le persone giuridiche – e dunque anche per gli Enti Pubblici[17] - il titolare del trattamento è individuato nell'Ente stesso, a prescindere dall'organo o dalle persone fisiche che ne esprimono la volontà: lo stesso Garante per la Protezione dei Dati Personali, con la circolare n. 291/S del 13 novembre 1997 doc. n. 39785, ha chiarito come «qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "titolare" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.)» [18].

Effettuate tali prime deduzioni si intende escludere in prima battuta, in modo quasi del tutto automatico ed attraverso un'interpretazione puntuale dell'art. 28 Reg. (UE) 2016/679, che il consigliere possa definirsi quale responsabile del trattamento, posto che, nell'espletamento delle proprie funzioni, quale rappresentante degli organi di governo dell'Ente Pubblico Locale, come individuate dall'art. 36 e ss TUEL, tale soggetto non ricade nella definizione di cui all'art. 4, n. 8, Reg. (UE) 2016/679[19]. Il responsabile del trattamento, infatti, viene individuato dalla normativa europea come

[15] Si veda su punto art. 4, n. 7, Reg. (UE) 2016/679.

[16] Cfr. L. Cairo - G. Roberto, *commento all'art. 4 "Titolare del trattamento"* in *Leggi D'Italia* a sostegno della tesi appena richiamata.

[17] Cfr. M. Di Pirro, *Compendio di Istituzioni di diritto privato (diritto civile)*, XXIII edizione, Napoli, Simone, 2019, 68. L'autore ci ricorda come l'Ente Pubblico è definito come persona giuridica pubblica, che persegue «interessi generali, propri dello Stato, e spesso godono di una posizione di supremazia nei confronti degli altri soggetti con cui vengono in rapporto (i c.d. enti pubblici)».

[18] Si veda sul punto Autorità Garante per la protezione dei dati personali ("Garante Privacy"), in Circolare n. 291/S del 13 novembre 1997 recante direttive in materia di protezione dei dati personali. Rif. nota n. 14/97/MAN, doc. web. n. 39785.

[19] La norma richiamata prevede infatti che il responsabile del trattamento sia definito come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento».

il soggetto, diverso ed estraneo rispetto al titolare del trattamento, chiamato a trattare dati per conto di quest'ultimo, secondo uno schema contrattuale che assume le forme del contratto di mandato ai sensi dell' art. 1703 c.c.: il consigliere deve considerarsi come parte dell' unitarietà della persona giuridica dell' Ente, e non dunque, come un soggetto esterno che agisca per conto dell' Amministrazione.

Come conseguenza diretta dell' affermata unitarietà della persona giuridica per l' Ente Pubblico Locale, si dovrà altrettanto escludere l' ipotesi che vede il consigliere comunale quale titolare autonomo del trattamento, ai sensi dell' art. 4 del Reg. (UE) 2016/679, determinando implicitamente l' individuazione dello stesso quale soggetto autorizzato al trattamento.

Il consigliere, dunque, sembra inserirsi nell'organigramma *data protection* quale soggetto autorizzato al trattamento dal titolare (il Comune o la Provincia), ai sensi del combinato disposto degli artt. 29[20] e 32[21] Reg. (UE) 2016/679 e 2–*quaterdecies,* c. 2, d.lgs. 196/2003[22], considerato che lo stesso opera sotto l' autorità diretta del titolare del trattamento.

Il ruolo dell'incaricato o autorizzato al trattamento sembrava, *prima facie*, scomparso e dalla normativa europea e dal Codice Privacy a seguito delle modifiche intervenute con il d.lgs. 101/2018 che hanno determinato l'abrogazione dell'art. 30 d.lgs. 196/2003[23], ma di fatto, il concetto di soggetto autorizzato al trattamento torna a più riprese anche all' interno del regolamento comunitario: basti ricordare che lo stesso art. 32 al c. 4 stabilisce che «Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri». Si può dunque affermare come sia stata eliminata la previsione normativa di una nomina obbligatoria ad autorizzato al trattamento, ma che tale "ruolo" rimanga ancora del tutto ben delineato sia nel Reg. (UE) 2016/679 che nel Codice Privacy come recentemente modificato[24]; di fatto, richiamato qui anche

[20] Si ricorda che l'art. 29 Reg. (UE) 2016/679 prevede infatti che «Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

[21] Il contenuto dell'art. 32 Reg. (UE) 2016/679 ci permette di rilevare come la definizione di un "organigramma *privacy*" si debba ricomprendere all'interno del comparto di misure organizzative di sicurezza che il titolare del trattamento è tenuto ad implementare.

[22] L'art. 2 – *quaterdecies* c. 2 d.lgs. 196/2003 stabilisce che «Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta».

[23] La norma in questione prevedeva che «Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima».

[24] Medesimi rilievi possono essere ricavati dalla lettura della Relazione illustrativa di accompagnamento al d.lgs. 101/2018, laddove, con riferimento all'art. 2-quaterdecies, si legge come «Tale disposizione permette di mantenere le funzioni e i compiti assegnati a figure interne all'organizzazione che, ai sensi del previgente codice in materia di protezione dei dati personali ma in contrasto con il regolamento, potevano essere definiti, a seconda dei casi, responsabili o incaricati».

il principio di *accountability*, si deve ritenere come il titolare, al fine anche di dimostrare correttamente il percorso di adeguamento alle disposizioni normative in materia di tutela dei dati personali, debba ben provvedere alla formalizzazione di una nomina scritta nei confronti dei soggetti autorizzati al trattamento – consiglieri comunali e provinciali compresi, anche con riferimento all'esercizio delle funzioni di cui all'art. 43, c. 2, TUEL - al fine di individuare le modalità corrette di trattamento del dato. Tale nomina scritta rappresenta, inoltre, una misura organizzativa atta ad istruire e formare in modo specifico i soggetti che provvedano, nell' ambito delle loro mansioni e delle loro funzioni, al trattamento di dati personali sotto l' autorità del titolare del trattamento. A ciò si deve aggiungere il provvedimento, tutt' ora richiamato dall' Autorità Amministrativa Indipendente, che con preciso riferimento alla Pubblica Amministrazione ha statuito come in assenza di una formale designazione come soggetto autorizzato al trattamento, i dipendenti delle pubbliche amministrazioni che, per lo svolgimento dei propri compiti, vengono a conoscenza di dati personali, devono essere considerati come soggetti terzi rispetto alle amministrazioni stesse, con conseguenti rilevanti limiti per la comunicazione e l´utilizzazione dei dati e quindi per la liceità del trattamento. Tale designazione è, infatti, indispensabile, in quanto permette di considerare legittimo il flusso delle informazioni personali nell'ambito degli uffici e tra i dipendenti dell'amministrazione titolare del trattamento[25].

Tale principio, per l'estensione del ruolo di autorizzato al trattamento anche al consigliere comunale, dovrà appunto trovare applicazione anche nei confronti di tale soggetto: la nomina ad autorizzato al trattamento, in questo caso, avrà il fine di istruire correttamente il consigliere in merito al rispetto della normativa in materia di trattamento del dato personale, richiamandolo ai principi che ispirano la tutela dei dati personali in merito al trattamento di dati che venga compiuto nell'espletamento del *munus* di cui all' art. 43 TUEL, onde impartire indicazioni che siano tese ad evitare errori o trattamenti illegittimi delle informazioni. Il consigliere, così, dovrà essere destinatario delle stesse *policy* tese a disciplinare in modo organico tutti i processi che possono in qualche modo toccare la materia della tutela del dato personale e che vengono consegnate ai dipendenti dell'Ente: si pensi ad esempio, ai regolamenti che disciplinano l'uso della strumentazione informatica, o ancora, il codice di comportamento adottato dall'Amministrazione[26].

[25] Si veda a tal fine Garante Privacy, 23 maggio 2000, in Bollettino n. 13, pag. 21 [doc. web n.40229].

[26] Con specifico riferimento all'estensione del Codice di Comportamento della Pubblica Amministrazione ai consiglieri comunali, si vedano le Linee guida in materia di Codici di comportamento delle amministrazioni pubbliche ANAC, sottoposte a consultazione sino al 15.01.2020, che prevedono quanto segue: «Il d.P.R. 62/2013, all'art. 2, co. 3, stabilisce, infatti, che «le pubbliche amministrazioni estendono, per quanto compatibili, gli obblighi di condotta previsti dal presente codice a tutti i collaboratori o consulenti, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo, ai titolari di organi e di incarichi negli uffici di diretta collaborazione delle autorità politiche, nonché nei confronti dei collaboratori a qualsiasi titolo di imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione» […] "Con riferimento ai "titolari di organi", ad avviso dell'Autorità, il legislatore intende riferirsi ai titolari di organi di indirizzo amministrativo che non sono direttamente o indirettamente espressione di rappresentanza politica. Si tratta dei componenti degli organi, monocratici o collegiali, di enti pubblici, economici e non economici, anche nominati o designati da organi politici, che rivestono la carica pubblica al di fuori di ogni rapporto di lavoro. Considerato il rilevo di tali figure, potrebbe non essere opportuno escluderle da una qualunque forma di disciplina di doveri di comportamento con

Infine, preme in ogni caso ricordare come anche i consiglieri, come i dipendenti dell' Ente, sono sempre chiamati al rispetto della riservatezza degli interessati, come confermato anche a più riprese dal Garante per la Protezione dei Dati Personali, che ha rilevato come «i consiglieri comunali che abbiano avuto accesso ad atti dell' amministrazione comunale per ragioni connesse all' espletamento del loro mandato devono rispettare il diritto alla riservatezza degli interessati»[27].

3.1. Il consigliere come titolare del trattamento al momento della violazione privacy

Sempre sulla qualifica *data protection* dei consiglieri, è necessario compiere un' ulteriore riflessione con riferimento a cosa accada laddove tale soggetto violi la disciplina normativa in vigore. Seguendo le regole ordinarie di imputazione della responsabilità all'Ente per ciò che concerne gli illeciti compiuti dai suoi organi e dei suoi dipendenti, possiamo identificare nel consigliere autore di una violazione *data protection* un titolare autonomo del trattamento, con la conseguente applicazione della responsabilità (e dunque delle sanzioni) che si congiungono a tale figura, nel rispetto di quanto previsto dagli artt. 82 e ss Reg. (UE) 2016/679.

Si deve ricordare, infatti, come il rapporto organico, dal quale discende l'imputazione all' Ente Pubblico del fatto e delle sue conseguenze, opera solamente laddove il soggetto che agisce - sottoposto all' autorità dell' Amministrazione - lo fa nell'ambito circoscritto delle proprie funzioni e competenze; si assiste invece alla cesura del rapporto organico nel momento in cui il soggetto agisca perseguendo finalità sue proprie, in contrasto con i compiti istituzionali assegnati, a mezzo di una condotta che non si ispira certamente a principi costituzionali di liceità, di legalità e buon andamento della P.A. Questa attività non si imputa all'Ente, come allo stesso non si imputa la relativa responsabilità.

Estendendo analogicamente, infatti, i principi concernenti l'immedesimazione organica che discendono, per i dipendenti pubblici, dall'art. 28 Cost.[28], possiamo rilevare come l' attività del singolo amministratore, nell' esercizio dei compiti indicati all' art. 42 TUEL, possa essere imputata all' Ente solo laddove la stessa combaci con la volontà di quest' ultimo, rimanendo fermi i principi costituzionali che ispirano l' attività amministrativa: di conseguenza, la Pubblica Amministrazione può essere chiamata a rispondere degli eventuali danni arrecati a terzi solo qualora il proprio dipendente li abbia arrecati nell' esercizio di compiti istituzionali o di compiti legati da "occasionalità

conseguenti responsabilità. Per essi può essere adottata la soluzione di introdurre, nell'atto di incarico, clausole che estendono loro obblighi di condotta previsti dal codice nazionale con relative indicazioni in caso di violazioni. Resta ferma la possibilità che gli enti interessati per detti soggetti possono adottare codici etici dedicati».

[27] Cfr. A tal proposito Garante Privacy, in Relazione 2008 - 2 luglio 2009 Parte II - L'attività svolta dal Garante, p. 21 [doc. web n. 1637571].

[28] La norma prevede che «I funzionari e i dipendenti dello Stato e degli enti pubblici sono direttamente responsabili, secondo le leggi penali, civili e amministrative, degli atti compiuti in violazione di diritti. In tali casi la responsabilità civile si estende allo Stato e agli enti pubblici».

necessaria" con compiti di istituto[29].

Ne discende, dunque, che il consigliere che agisca in violazione dei principi racchiusi nel Reg. (UE) 2016/679, violando il diritto alla protezione dei dati personali dei soggetti eventualmente interessati dalle attività "ispettive", agirà quale titolare autonomo del trattamento; si assiste, qui, ad una sorta di estensione dei principi sanciti all' art. 28 dello stesso regolamento, laddove si prevede, con specifico riferimento al responsabile del trattamento, che «Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione».

La richiamata interpretazione è stata sostenuta dallo stesso Garante per la Protezione dei Dati Personali, che con l' ordinanza di ingiunzione del 4 aprile 2019 ha specificato come il consigliere comunale, che aveva ottenuto l' accesso ad alcuni documenti contenenti dati personali ai sensi dell' art. 43 TUEL, provvedendo poi a comunicarne il contenuto ad un soggetto terzo, dovesse qualificarsi «quale titolare del trattamento» ed allo stesso dovesse essere contestata «la violazione amministrativa prevista dall' art. 162, comma 2-bis, del Codice, che punisce la violazione delle disposizioni indicate nell' art. 167 e, in tal caso, la violazione dell' art. 19, comma 3, per aver effettuato un trattamento illecito di dati personali consistente, nello specifico, nella comunicazione di documentazione (D.I.A. n. 275/09 del 20 ottobre 2009) contenente dati personali del segnalante e acquisita in qualità di consigliere comunale, alla controparte giudiziale di tale segnalante in assenza dei presupposti normativi legittimanti»[30].

Il consigliere diviene dunque centro primario di imputazione della responsabilità nel momento in cui le informazioni ottenute a seguito dell' esercizio del proprio diritto di accesso siano utilizzate a mezzo di condotte che si distaccano dalle funzioni e dalle competenze riconosciute, con condotte che possano determinare la violazione del diritto alla riservatezza ed alla protezione dei dati personali eventualmente contenuti nei documenti e nelle informazioni ottenute da tale soggetto, con una tutela del dato personale che sembra operare, ancora una volta, a posteriori.

Sebbene l'individuazione del ruolo del consigliere nell'organigramma *data protection* sia di necessaria importanza per una disamina completa della fattispecie, si ritiene qui imprescindibile introdurre un tema di non secondaria importanza, relativo alla possibile applicazione dei principi che regolano la tutela dei dati personali all'atto dell'esercizio del diritto di accesso, in una prospettiva cautelativa *by design* e *by default*, come richiesto dall'art. 25 Reg. (UE) 2016/679, assodato che il diritto *ex* art. 43 TUEL si concretizza in un trattamento di dato personale.

[29] Cfr. A. M. Sandulli, *Manuale di diritto amministrativo*, Napoli, 1984, 1117, secondo il quale «non sono riferibili all'Amministrazione […] le azioni che non provengono da soggetti i quali possano essere considerati agenti di essa, […] gli atti personali degli agenti (lettere e negozi privati), […] gli atti viziati da incompetenza assoluta (straripamento di potere) e i comportamenti posti in essere volutamente (dolosamente) in violazione di norme proibitive (diversamente dall'opinione corrente nella dottrina francese, si ritiene che il fatto che costituisca reato doloso istituzionalmente non può essere ascritto all'Amministrazione)».

[30] A tal fine si veda Garante Privacy, ordinanza 4 aprile 2019, Registro dei provvedimenti n. 100 del 4 aprile 2019 [doc. web n. 9117119].

4. I profili di applicazione del Reg. (UE) 2016/679 all'esercizio dell'accesso ex art. 43, c. 2, TUEL

La ridefinizione del particolare diritto di accesso oggetto della presente trattazione come trattamento di dati personali introduce il tema della necessaria disamina relativa alle modalità di corretta applicazione delle norme e dei principi derivanti dal regolamento comunitario e dalla disciplina che da esso discende, in un' ottica volta non solo alla tutela (*ex post*) della riservatezza personale comunemente intesa, ma anche alla tutela *ex ante* dei dati personali riferiti allo stesso soggetto interessato.
Ciò implica un' inversione di prospettiva con riferimento alle valutazioni da compiersi nella fattispecie oggetto di analisi: il tema della protezione dei dati personali è ben più ampio rispetto a quello della riservatezza personale, tale per cui esso non può essere semplicemente escluso dall' equazione richiamando il consigliere al mero dovere di segreto imposto dall' art. 43, c. 2, TUEL. Il processo, concernente l' esercizio di tale specifico diritto di accesso, infatti, dovrà comprendere la compiuta attuazione di tutti i principi che il legislatore europeo prima, e quello nazionale poi, hanno individuato per provvedere alla necessaria tutela dei diritti personali coinvolti.
Si deve necessariamente ricordare in questa sede, infatti, come nella privacy si individui una famiglia di diritti inviolabili dell' uomo, che attengono a bisogni primari dell' essere umano; essa si è evoluta, a partire dal «diritto ad essere lasciati soli»[31] fondato ormai centotrent' anni fa, sino a poter essere definita come insieme di tutele a bisogni connaturati dell' essere umano, come complesso di tutele che vanno a proteggere lo stesso rispetto a delle infrazioni del sé nelle parti aggredibili da terzi. Ed è proprio a questa tutela prodromica e diffusa che tende il Reg. (UE) 2016/679, il quale guarda alla protezione delle persone fisiche attraverso la tutela dei loro dati personali, definendo la *data protection* come elemento integrante il diritto alla libera circolazione delle persone fisiche nell'UE.
La tutela dei dati personali pertanto deve essere considerata come elemento presupposto, strumentale alla tutela di altri diritti fondamentali ed inderogabili dell'essere umano, che deve trovare una necessaria costante applicazione, di talché tale tutela si estende, secondo quanto stabilito dalla normativa applicabile, a tutte le fattispecie che possono ricomprendere il trattamento di dati personali.
In particolare, l' identificazione di un' attività di trattamento di dati personali comporta la necessaria applicazione dei principi di cui al Reg. (UE) 2016/679, rientrando nell'ambito di applicazione materiale previsto dall'art. 2, par. 1, del regolamento stesso: ciò determina, come conseguenza diretta, una necessaria analisi concernente il corretto dispiegamento dei principi di cui agli artt. 5, 6, 24, 25 e 32 anche con riferimento all'esercizio del diritto di cui all'art. 43, c. 2, TUEL, individuando i soggetti attivi e le relative responsabilità connesse a tali adempimenti, e le modalità più coerenti per provvedere all' attuazione del generale obbligo di tutela dei dati personali.
Per ciò che concerne la fattispecie di trattamento oggetto della presente analisi, riprendendo quanto già espresso al paragrafo 3, dobbiamo necessariamente individuare

[31] S. D. Warren – L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 4-5, 15 December 1890, 193-220.

l'Amministrazione richiesta (o l'azienda o l'ente dipendente, a seconda del caso) come titolare del trattamento, soggetto che, all'atto della formazione del documento oggetto della richiesta del consigliere, individua finalità e mezzi del trattamento, e che di conseguenza è soggetto responsabile della corretta applicazione dei principi di *data protection*. Spetterà dunque all' Amministrazione adempiere agli obblighi derivanti dal Reg. (UE) 2016/679, anche all' atto della richiesta di accesso da parte del consigliere: e così dovrà essere garantito il rispetto dei principi di liceità, correttezza e trasparenza del trattamento, di limitazione delle finalità, di minimizzazione, esattezza, integrità e riservatezza dei dati, di limitazione della conservazione e del generale principio di *accountability* ai sensi dell'art. 5[32], nonché dei principi di *privacy by design* e *by default* ai sensi dell'art. 25[33], in aggiunta all'obbligo di individuare e porre in essere le misure tecniche ed organizzative adeguate a garantire la sicurezza del trattamento di cui all'art. 32 Reg. (UE) 2016/679[34].

[32] L'art. 5 Reg. (UE) 2016/679 prevede che «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 titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)».

[33] L'art. 25 Reg. (UE) 2016/679 prevede che «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo».

[34] L'art. 32 Reg. (UE) 2016/679 stabilisce che «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la

Ai fini di una compiuta analisi, si provvede nel prosieguo alla disamina di alcune casistiche specifiche, concernenti le richieste di consiglieri comunali di poter accedere, ai sensi dell'art. 43, c. 2, TUEL, al gestionale di protocollo informatico dell'Ente di appartenenza, nonché ad altre banche dati quali ad esempio il gestionale di contabilità, valutando le impostazioni giurisprudenziali che nel tempo si sono susseguite, al fine di evidenziare l' imprescindibile necessità di provvedere all' attuazione dei principi concernenti la tutela del dato personale anche in tale fattispecie.
L' analisi è volta ad indagare le ragioni che portano a definire la necessaria attuazione di una tutela *ex ante* rispetto all'uso eventuale che il consigliere intenda fare delle informazioni e dei dati personali eventualmente ottenuti, in comparazione rispetto al caso, successivamente valutato, dell'utilizzo illegittimo delle informazioni acquisite a seguito dell'esercizio del diritto di accesso.

5. Il caso concreto: la richiesta di accesso da remoto al protocollo informatico e ad altri gestionali comunali

La giurisprudenza amministrativa è stata recentemente chiamata ad interrogarsi sulla possibile estensione dell' alveo applicativo del diritto di cui all' art. 43, c. 2, TUEL, sino ad arrivare a ricomprendere anche il caso in cui il consigliere comunale richieda di poter accedere, da remoto, a mezzo della creazione di un collegamento VPN con creazione di *user* e *password*, ai sistemi gestionali dell' Ente, in particolar modo al protocollo informatico ed al gestionale di contabilità utilizzato dall' Amministrazione, al fine di valutare se tale diritto di accesso possa essere esercitato anche mediante l'utilizzo, da parte del consigliere, di tali strumenti.
Prima di analizzare compiutamente i passi che, timidamente, stanno permettendo un riavvicinamento alla materia della tutela dei dati personali, si ritiene opportuno procedere con una breve disamina concernente i precedenti giurisprudenziali che a più riprese si sono occupati della fattispecie in esame, utili per comprendere la portata del *vulnus* che si rischia di cagionare escludendo dal ragionamento tale diritto imprescindibile.

capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

5.1. Una breve disamina dei precedenti giurisprudenziali: la tutela dei dati personali come diritto "tradito"

Come sopra accennato, la giurisprudenza di merito e di legittimità in sede amministrativa è stata recentemente chiamata, a più riprese, a pronunciarsi sulla possibilità per il consigliere comunale, di avere accesso da remoto al gestionale di protocollo utilizzato dall' Ente, in applicazione dell' art. 43, c. 2, TUEL. Sul tema si è sviluppato sin da subito un orientamento prevalente, favorevole all' estensione dell' alveo applicativo del diritto di accesso in tal senso, al fine di permettere a tali soggetti qualificati l'espletamento di un accesso più efficace e meno dispendioso per gli uffici dell'Amministrazione.
Precisamente, prima il Consiglio di Stato con sentenza n. 3486/2018 e poi il TAR Salerno, con sentenza n. 545/2019, rilevavano come «ove il consigliere comunale fosse posto in condizione di individuare previamente gli atti il suo esame fosse utile all'esercizio delle sue prerogative, mediante la preventiva consultazione del protocollo informatico dell'Ente, tale modalità consentirebbe un accesso (ai singoli documenti) più efficace e meno dispendioso per l'ordinaria attività degli uffici; per converso, impedire o ostacolare il consigliere nell'individuazione di detti atti, ad esempio aggravando le modalità di consultazione delle fonti e di accesso alle stesse (protocollo dell'Ente), significherebbe impedire o frapporre ostacoli all'esercizio di un diritto»[35]. Sulla scorta di tale impostazione, il Giudice di prime cure, confermando l'orientamento già espresso dal Consiglio di Stato con sentenza appena sopra richiamata, evidenziava come dovesse essere riconosciuto al consigliere che lo richieda, un accesso in sola consultazione al protocollo informatico dell'Ente, con la consegna di credenziali (*username* e *password*) che permettano allo stesso un accesso (meramente valutativo e non esplorativo) anche da remoto.
Ancora, a conferma dell'orientamento appena esposto, si pronunciava il TAR Sardegna con sentenza n. 317/2019, evidenziando come l'accesso da remoto del consigliere comunale ai gestionali del Comune debba essere garantito in quanto strumento di valutazione preliminare, prodromico ad un più consapevole esercizio da parte di tale soggetto qualificato del diritto di accesso stesso, potendo in questo modo il consigliere selezionare in precedenza gli oggetti degli atti di cui chiedere l' esibizione[36].
Gli stessi rilievi venivano compiuti poi dal TAR Basilicata Potenza, che con sentenza n. 599/2019, pronunciandosi in merito ad una richiesta di accesso, da remoto, al pro-

[35] Si vedano sul punto le sentenze Cons. Stato, n. 3486/2018, TAR Campania Salerno, sez. II, 4 aprile 2019, n. 545.

[36] Cfr. sul punto, TAR Sardegna Cagliari, sez. I, 4 aprile 2019, n. 317. Precisamente, il Giudice di prime cure ha ritenuto che «In specie, la richiesta di accedere al protocollo informatico e ai programmi in uso presso il Comune, e quindi di avere il possesso delle chiavi di accesso telematico, rappresenta una condizione preliminare, ma nondimeno necessaria, per l'esercizio consapevole del diritto di accesso, in modo che questo si svolga non attraverso una apprensione generalizzata e indiscriminata degli atti dell'amministrazione comunale (che costituisce il timore manifestato anche in questa sede dal Comune intimato), ma mediante una selezione degli oggetti degli atti di cui si chiede l'esibizione. Peraltro, una delle modalità essenziali per poter operare in tal senso è rappresentata proprio dalla possibilità di accedere (non direttamente al contenuto della documentazione in arrivo o in uscita dall'amministrazione, ma) ai dati di sintesi ricavabili dalla consultazione telematica del protocollo (sia del protocollo generale dell'Ente, che dei registri di protocollo di settore, come quelli concernenti le determinazioni dei diversi responsabili dei servizi)».

tocollo informatico ed al gestionale informatico di contabilità dell' Ente convenuto, rilevava come si debba ritenere che il diritto di accesso dei consiglieri *ex* art. 43, c. 2, TUEL vada «oggi necessariamente correlato al progressivo e radicale processo di digitalizzazione dell'organizzazione e dell'attività amministrativa, risultante dal Codice dell'Amministrazione digitale»[37], con la conseguente applicazione di tale impianto normativo, che prevede per le Pubbliche Amministrazioni l' obbligo di garantire l' accessibilità e la fruibilità dei dati a mezzo delle tecnologie dell' informazione[38], concludendo come «l'Amministrazione comunale ha il dovere di dotarsi di una piattaforma integrata di gestione documentale, nell'ambito della quale è inserito anche il protocollo informatico. Corrispondentemente, il consigliere comunale ha il diritto di soddisfare le esigenze conoscitive connesse all'espletamento del suo mandato anche attraverso la modalità informatica, con accesso da remoto»[39].

Ne discende come gli orientamenti giurisprudenziali di merito e di legittimità analizzati siano concordi nel ritenere che il diritto di accesso dei consiglieri debba ritenersi esteso anche all'accesso al protocollo informatico ed agli altri gestionali informatici dell'Ente. La *ratio* del riconoscimento giurisprudenziale concernente le nuove modalità di esercizio del diritto di accesso, con l' assegnazione al soggetto richiedente di apposito *username* e *password* per utilizzare i gestionali informatici per le finalità specificate dall' art. 43, c. 2, TUEL, si individua dunque nella necessità di evitare un aggravio eccessivo per gli uffici comunali, che devono riscontrare alle richieste di accesso poste dai consiglieri comunali[40].

Gli stessi orientamenti affermano poi all' unisono come l' esercizio di tale specifica tipologia di accesso ai gestionali dell' Ente non possa essere però del tutto privo di limiti: in particolare, «al fine di evitare ogni accesso indiscriminato alla totalità dei documenti protocollati» i Giudici hanno ritenuto come «l'accesso da remoto vada consentito in relazione ai soli dati di sintesi ricavabili dalla consultazione telematica del protocollo, non potendo essere esteso al contenuto della documentazione, la cui acquisizione rimane

[37] Cfr. sul punto, TAR Basilicata Potenza, sez. I, 10 luglio 2019, n. 599.

[38] Cfr. TAR Basilicata Potenza, sez. I, 10 luglio 2019, n. 599, dove precisamente il giudice rilevava come «Deve ritenersi che il diritto di accesso dei consiglieri comunali *ex* art. 43 d.lgs. n. 267 del 2000 cit. del TUEL, cui è funzionalmente connessa la richiesta del ricorrente, va oggi necessariamente correlato al progressivo e radicale processo di digitalizzazione dell'organizzazione e dell'attività amministrativa, risultante dal Codice dell'Amministrazione digitale. Tale disciplina, per quanto di rilievo, impone allo Stato, alle regioni e alle autonomie locali di assicurare "la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale", "utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione" (cfr. art. 2, co. 1), precisando che "i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dei privati" (cfr. art. 50, co. 1)».

[39] Cfr. sul punto, TAR Basilicata Potenza, sez. I, 10 luglio 2019, n. 599.

[40] Si veda sul punto TAR Campania Salerno sez. II, 4 aprile 2019, n. 545, che evidenzia come «ove il consigliere comunale fosse posto in condizione di individuare previamente gli atti il suo esame fosse utile all'esercizio delle sue prerogative, mediante la preventiva consultazione del protocollo informatico dell'Ente, tale modalità consentirebbe un accesso (ai singoli documenti) più efficace e meno dispendioso per l'ordinaria attività degli uffici; per converso, impedire o ostacolare il consigliere nell'individuazione di detti atti, ad esempio aggravando le modalità di consultazione delle fonti e di accesso alle stesse (protocollo dell'Ente), significherebbe impedire o frapporre ostacoli all'esercizio di un diritto».

soggetta alle ordinarie regole in materia di accesso (tra le quali la necessità di richiesta specifica)»[41].

Dunque, l'unica limitazione all'espletamento dell'accesso con riferimento ai gestionali dell'Ente, ed in particolare al protocollo informatico, concerne la sola possibilità di accesso in consultazione, al registro di protocollo.

Appare chiaro come il fattore relativo alla tutela dei dati personali eventualmente coinvolti da tali tipologie di accesso sia stato del tutto tralasciato dai Giudici che si sono pronunciati sul punto: le implicazioni *data protection* non sono in alcun modo state affrontate, non è stato valutato se l' accesso da remoto (nei vari casi di specie) possa dirsi o meno sicuro, non sono stati analizzati i principi di cui agli artt. 5, 24, 25 e 32 Reg. (UE) 2016/679, e di conseguenza non è stata in alcun modo considerata la necessità, per l' Amministrazione Comunale richiesta, di tutelare, anche nel momento dell' esercizio di tale diritto, i dati personali dei soggetti eventualmente coinvolti.

Ciò sebbene permanga il principio affermato dal Garante per la Protezione dei Dati Personali, alla cui stregua l' esistenza del segreto d' ufficio in capo al consigliere sulle informazioni conosciute attraverso l' esercizio delle prerogative di cui all' art. 43 TUEL non esime da responsabilità l' Ente che gli abbia comunicato i dati personali, fuori dei casi consentiti dalla legge (con le rilevanti sanzioni dell' art. 83, par. 5, Reg. (UE) 2016/679 e dell'art. 166, c. 2, d. lgs. 196/2003)[42].

Si ritiene che tale esclusione aprioristica non possa certo dipendere da ipotetici dubbi concernenti l'eventuale presenza, nei gestionali delle Amministrazioni, di dati personali definiti come da art. 4 Reg. (UE) 2016/679: tali strumenti contengono indiscutibilmente informazioni classificabili come dati personali, pertanto la miopia decisoria, che in questi frangenti non ha minimamente preso in considerazione il diritto imprescindibile alla tutela dei dati personali, dipende presumibilmente dall'interpretazione, sopra già discussa, del diritto alla privacy come mero diritto alla riservatezza personale, oggetto di una sola tutela a posteriori rispetto all'avvenuto accesso.

5.2. Valutazioni sui profili applicativi dei principi fondamentali del trattamento dei dati personali all'accesso *ex* art. 43 TUEL: artt. 5, 24, 25 e 32 del Reg. (UE) 2016/679

Ma se l'accesso *ex* art. 43, c. 2, TUEL comporta, di fatto, un' operazione di trattamento di dati personali, la quale si verifica a maggior ragione in presenza di un accesso ai gestionali informatici utilizzati dall' Amministrazione, ciò comporta come L'Ente richiesto non possa prescindere dall'applicazione corretta dei principi e delle tutele previste, anche nella fattispecie oggetto di esame.

In particolare, l' espletamento dell' accesso dovrà in ogni caso garantire il rispetto del principio di minimizzazione e di limitazione delle finalità del trattamento, individuato

[41] Cfr. sul punto, TAR Basilicata Potenza, sez. I, 10 luglio 2019, n. 599.

[42] A tal fine si veda Garante Privacy, ord. 4 aprile 2019, Registro dei provvedimenti n. 100 del 4 aprile 2019 [doc. web n. 9117119].

dall' art. 5 Reg. (UE) 2016/679, che determina l' indispensabile limitazione dei dati trattati a quanto necessario per il raggiungimento delle finalità sottese al trattamento, imponendo di circoscrivere l'ambito delle operazioni ai soli dati personali appunto indispensabili per la realizzazione dello scopo perseguito, ricorrendo a dati anonimizzati o, se non sia possibile, quantomeno pseudonimizzati, al fine di ridurre il più possibile l'impatto del trattamento sulla sfera privata del singolo. L' affermazione è sicuramente forte, soprattutto se si pensa che il rispetto di un principio così delineato potrebbe di fatto inserire una sorta di obbligo di motivazione da addurre, da parte del consigliere, al momento della richiesta, ma la stessa si ritiene dovrà essere valutata al solo fine di tutelare correttamente le informazioni personali coinvolte, e non per l' eventuale disconoscimento del diritto di accesso. Tale canone è poi valorizzato con la previsione di principi quali la *privacy by design* e *by default* alle quali deve conformarsi il trattamento, per sua stessa configurazione.

La lettura integrale della fattispecie permette di ritenere che le opzioni di accesso del consigliere ai gestionali dell'Ente possano e debbano essere ben apprezzate anche per ciò che concerne i profili di sicurezza e tutela dei dati personali coinvolti nel trattamento, ai sensi degli artt. 5, par. 2, 24 e 32 Reg. (UE) 2016/679 e più in generale nel rispetto dell' intera normativa in materia di protezione dei dati personali, con la conseguenza che la scelta della modalità di accesso (da remoto, oppure a mezzo della previsione di una postazione specifica pressi gli uffici dell' Amministrazione) non possa essere rimessa alla semplice richiesta del consigliere.

Coerentemente rispetto ai principi *data protection*, infatti, sarà compito del titolare del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi del trattamento, individuare quali siano le modalità più corrette per l' espletamento di tale accesso, al fine di garantire la sicurezza delle informazioni personali coinvolte nel trattamento, prevedendo apposite misure di sicurezza tecniche ed organizzative, così come disposto dall' art. 32 del Reg. UE 2016/679.

In particolare, con riferimento all'accesso al sistema informatico dell'Ente, si deve rilevare quanto segue. Il trattamento di dati personali determina, sempre ed in modo intrinseco, un rischio congenito per i soggetti interessati da tale trattamento: laddove vi sia trattamento di dati personali, vi sarà sempre il rischio che questi possano essere violati ed il solo modo per mitigare del tutto tale rischio è quello di eliminare in modo completo i dati personali, e dunque interrompere il trattamento. Partendo da tale imprescindibile assunto, è innegabile che la possibilità di un accesso al sistema informatico dell' Ente, esercitato localmente o da remoto, così semplicemente inteso, senza alcun tipo di regolamentazione, e senza il necessario richiamo alla necessità, per l' Amministrazione, di dotarsi delle necessarie misure tecniche ed organizzative a tutela dei dati trattai, potrebbe essere foriero di rischi maggiori per gli stessi.

Resta ben inteso, quindi, che tale rischio dovrebbe essere correttamente valutato dal titolare del trattamento, il quale dovrebbe anche analizzare le possibili misure correttive da adottare al fine di ricondurre a sicurezza l'espletamento del diritto di accesso.

Dall'analisi appena compiuta risulta come sia necessaria una lettura del caso di specie orientata all'applicazione dei principi di *data protection*, elementi che non possono essere

tralasciati in quanto hanno ricadute innegabili sulle modalità corrette di esercizio del diritto di cui all' art. 43, c. 2, TUEL.

5.3. Il cambio di rotta nella giurisprudenza. La sentenza n. 253/2020 TAR Friuli-Venezia Giulia

Sebbene si debba ritenere che la richiesta di accesso agli atti, esercitata ai sensi dell'art. 43, c. 2, TUEL, possa estendersi sino alla possibilità, per il consigliere comunale, di accedere con proprie credenziali da remoto al registro di protocollo informatico dell' Ente, si deve evidenziare come a tale richiesta non corrisponda un diritto dello stesso consigliere di accesso da remoto: questa è, per l' appunto, una delle possibilità che possono essere previste per permettere il corretto espletamento del diritto soggettivo pubblico ivi in commento. Un primo input concernente la necessaria considerazione delle modalità specifiche di espressione di tale diritto lo ritroviamo nella Relazione della commissione per l' accesso ai documenti amministrativi sulla trasparenza dell' attività della pubblica amministrazione, per l' anno 2016, che, a sostegno della tesi poc' anzi esposta sottolineava come «non v'è d'altra parte dubbio che l'attività informativa debba essere ordinariamente svolta presso gli uffici dell'Amministrazione, come la norma stessa suggerisce, cosicché il consigliere non può vantare alcun "diritto" all'accesso al sistema informatico con connessione da remoto: né, secondo ragionevolezza il diritto del consigliere risulterebbe frustrato o compresso se esercitato in una postazione collocata presso gli uffici dell'Ente, il quale ha d'altra parte pieno titolo a garantire prioritariamente la sicurezza del sistema»[43]. Sono pertanto valutabili, dall'Ente, altre opzioni per permettere al consigliere comunale il corretto accesso al proprio sistema informatico: l'istanza di accesso da remoto del consigliere non determina, di contro, un immediato obbligo dell'Amministrazione ad adeguarsi a tale richiesta, ma si deve ritenere che, a seguito di specifica analisi del titolare del trattamento, il Comune possa prendere in considerazione altre possibilità, alternative a quella prospettata, che permettano, eventualmente, il corretto espletamento dell'accesso ai sensi dell'art. 43 TUEL senza determinare l'accesso da remoto al sistema informatico dell'Ente.

Tale rilievo è stato recentissimamente recepito anche a livello giurisprudenziale, con tre specifici interventi che hanno progressivamente dedotto come l' individuazione delle modalità di esercizio effettive di un tale diritto di accesso ad un gestionale dell' Ente non rientri nella disponibilità decisoria del consigliere stesso, quanto più dell' Amministrazione, unico soggetto titolato a compiere alcune valutazioni (anche riferite alla sicurezza dei dati e delle informazioni) che può stabilire come tale facoltà possa e debba essere esplicata.

La prima pronuncia, che ha evidenziato come la spinta verso la digitalizzazione dei servizi debba coinvolgere anche le modalità di esercizio del diritto di accesso di cui all' art. 43, c. 2, TUEL senza però che l' accesso ai gestionali informatici comporti «la elu-

[43] Cfr. sul punto, Relazione della commissione per l'accesso ai documenti amministrativi sulla trasparenza dell'attività della pubblica amministrazione – anno 2016, atti parlamentari, XVII legislatura, Doc. LXXVIII n. 5, p. 194.

sione dei principi di fondo che conformano l' esercizio del relativo diritto, nei termini stabiliti dagli artt. 22 e 24 della legge n. 241 del 1990[44]», è quella del TAR Molise, che con la sentenza n. 285/2019. Il Giudice amministrativo, pronunciandosi con riferimento ad una richiesta avente ad oggetto l'accesso da remoto con credenziali personali al programma di contabilità dell' Ente, affermava come «il rilascio delle credenziali di accesso all' area "Contabile e Patrimonio" del sistema Urbi Smart, nei termini richiesti dai ricorrenti, consentirebbe ai consiglieri regionali di accedere alla generalità indiscriminata dei documenti relativi alla contabilità dell' ente in mancanza di apposita istanza. Tale forma di accesso "diretto" si risolve in un monitoraggio assoluto e permanente sull' attività degli uffici, tale da violare la *ratio* dell'istituto, che, così declinato, eccede strutturalmente la sua funzione conoscitiva e di controllo in riferimento ad una determinata informazione e/o ad uno specifico atto dell' ente, siccome ritenuti strumentali al mandato politico, per appuntarsi, a monte, sull' esercizio della funzione propria dell' area "Contabile e Patrimonio" e sulla complessiva attività degli uffici, con finalità essenzialmente esplorative, che eccedono dal perimetro delle prerogative attribuite ai consiglieri regionali»[45].

Un primo passo verso la ridefinizione delle modalità effettive di esercizio di tale particolare diritto concerne la necessità di evitare un controllo esplorativo, posto in essere dal consigliere che acceda ai gestionali informatici dell' Ente.

Sulla scia di tale interpretazione, è stato lo stesso Consiglio di Stato, con sentenza n. 3345/2020, a compiere un ulteriore avanzamento nelle modalità di analisi della fattispecie, sottolineando, prima di tutto, come i giudizi aventi ad oggetto le richieste di accesso ai sistemi informatici dell' Amministrazione avanzate dai consiglieri concernono, solo in apparenza, giudizi «sull' accesso a atti o documenti», quanto piuttosto essi devono essere definiti come giudizi «sull' accessibilità indistinta al sistema informativo integrato, gestionale e direzionale, dell' amministrazione»[46].

Con un fondamentale distacco rispetto alla propria precedente interpretazione, già sopra richiamata, il Consiglio di Stato ha ben sottolineato come le richieste di accesso ai gestionali informatici degli Enti da parte dei consiglieri non possa tradursi automa-

[44] Cfr. sul punto, TAR Molise, sez. I, 3 settembre 2019, n. 285. Il Giudice di prime cure rilevava come «Vero è che l'accesso previsto dall'art. 43 del T.U.E.L. - pacificamente estensibile ai consiglieri regionali - deve essere letto ed applicato in conformità alla progressiva digitalizzazione che ha interessato negli ultimi anni l'attività degli uffici pubblici, ciò che rende sicuramente ammissibile l'accesso mediante l'utilizzo di sistemi informatici. È però parimenti vero che la concreta modalità dell'accesso con l'impiego di applicativi informatici non deve determinare la elusione dei principi di fondo che conformano l'esercizio del relativo diritto, nei termini stabiliti dagli artt. 22 e 24 della legge n. 241 del 1990».

[45] Cfr. sul punto, TAR Molise, sez. I, 3 settembre 2019, n. 285.

[46] Cfr. Cons. Stato, sez. V, 26 maggio 2020, n. 3345; nella sentenza è stato ben rilevato come «L'oggetto della contestazione in giudizio, infatti, è non un diniego all'accesso ad un singolo documento amministrativo (ovvero a più, determinati, provvedimenti amministrativi), come è nelle controversie in siffatta materia (art. 116 Cod. proc. amm.); ma è, in termini sostanziali, il diniego di un'innovazione organizzativa radicale, che prescinde da singoli atti o documenti, e che consiste nella disponibilità da parte del consigliere regionale delle credenziali di accesso alla documentazione digitale o digitalizzata di tutta l'attività amministrativa regionale: tale da metterlo in condizione di avere immediato ingresso, a discrezione e senza una ragione particolare, a qualsivoglia – anche se allo stato indeterminato e indeterminabile - passato, presente o futuro atto o documento amministrativo contemplato dal sistema in discorso».

ticamente nel riconoscimento di tale modalità di accesso, in quanto la stessa è tale da determinare, per tali soggetti qualificati, la possibilità di acquisire «un patrimonio conoscitivo che potenzialmente è pari alla latitudine dell' intera amministrazione regionale», anche per finalità meramente esplorative, eccedenti rispetto ai confini imposti dalla *ratio* della norma a tale particolare diritto[47]. Le ragioni di tale evoluzione interpretativa vanno individuate nel passaggio successivo della sentenza, che rappresenta, per l' organo giudicante, una prima presa di coscienza avente a riguardo la necessità di provvedere, all' atto dell' esercizio del diritto di accesso dei consiglieri, ad un equo bilanciamento con tutti gli opposti e meritevoli interessi eventualmente coinvolti da tale operazione, con richiamo espresso al «rispetto della vita privata», previo il riconoscimento dell' impossibilità di presumere sempre e comunque che tali esigenze di bilanciamento siano compatibili con «l' indiscriminata accessibilità qui in questione»[48].

E così, il Giudice definiva «ragionevole, adeguato e corrispondente al generale principio di proporzionalità che per ciascuna delle varie tipologie di accesso previste dall' ordinamento [..] siano stabiliti presupposti e modalità specifiche, poiché diversi sono gli interessi di volta in volta in contrapposizione e diversa è la ragione dell' accesso», rilevando come per il diritto *sui generis* in esame «non concretizza una prerogativa personale ma uno strumento per l' esercizio delle funzioni consiliari, di sindacato politico o legislative» individuando dunque il limite intrinseco al diritto di accesso del consigliere proprio nella menzionata utilità di tale strumento.

Sulla scorta di tali orientamenti, un ulteriore fondamentale passo volto al riconoscimento della necessità di ricomprendere, nell' esercizio del diritto *ex* art. 43, c. 2, TUEL, le tutele richieste dalla normativa in materia di protezione del dato personale, è stato compiuto dal TAR Friuli-Venezia Giulia, che con sentenza n. 253/2020, ha ricondotto la fattispecie ad una lettura integrale, orientata anche alla protezione delle informazioni che possono potenzialmente essere acquisite dal consigliere.

La questione sottoposta all'attenzione del Giudice di prime cure concerneva la richiesta, avanzata da un consigliere comunale alla propria Amministrazione, di poter accedere da remoto, con creazione di *username* e *password*, al protocollo informatico ed al programma di contabilità: la richiesta era stata declinata dall' Ente, il cui sistema informatico è gestito dalla Regione, sulla base dell' assenza di disponibilità economica per poter provvedere all' apertura di una VPN specifica per il richiedente, al quale era

[47] Cfr. Cons. Stato, sez. V, 26 maggio 2020, n. 3345, dove il Giudice rileva come «qui non è in contesa la facoltà di accesso del consigliere regionale ad atti dell'amministrazione regionale – facoltà ampiamente evidenziata dalla giurisprudenza amministrativa (sin da Cons. Stato, V, 17 settembre 2010, n. 6963; V, 5 settembre 2014, n. 4525) – ma l'ingresso senza più forma, riscontro e vaglio in una strumentazione digitale che continuativamente permetta l'accesso a tutti – nei sensi detti - gli atti dell'amministrazione regionale».

[48] Cfr. Cons. Stato, sez. V, 26 maggio 2020, n. 3345; nella sentenza si legge che «[…] va comunque ricordato che le regole legali dell'accesso espressamente o implicitamente commisurano una ragionevole proporzione e un equilibrio tra gli opposti e meritevoli interessi coinvolti dall'accesso a documenti amministrativi. La definizione di tali regole corrisponde alla natura fondamentale di interessi che possono esservi antagonisti, come quello al rispetto della vita privata (cfr. Corte cost., 21 febbraio 2019, n. 20) […] o comunque al rispetto dell'immanente principio di buon andamento della pubblica amministrazione (art. 97 Cost.) che eleva a principio costituzionale la congruenza, l'adeguatezza e l'efficacia dell'azione amministrativa: ciò che, per la realtà delle cose, non è dato presumere sempre e comunque compatibile con l'indiscriminata accessibilità qui in questione».

stato però proposto di provvedere all' accesso ai gestionali indicati a mezzo di una postazione a ciò specificamente adibita presso la sede dell' Amministrazione. Il ricorso presentato dal consigliere è stato respinto in quanto privo di pregio, laddove il Giudice ha dichiarato come «nella fattispecie in esame non viene assolutamente in rilievo il diritto del ricorrente medesimo di ottenere dagli Uffici del Comune, quale consigliere comunale, "tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato" ai sensi dell'art. 43, c. 2, del d.lgs. n. 267 del 2000 […], ma unicamente la pretesa dell'interessato, non assistita da alcun corrispondente obbligo di legge gravante sull'ente civico, di esercitare il diritto in questione nella modalità a lui più gradita e della cui effettiva e stretta funzionalità alle esigenze proprie di mandato il Collegio dubita fortemente, dato che, come si avrà modo di evidenziare in seguito viene in rilievo l' indistinta accessibilità all' intero sistema informatico dell'Amministrazione comunale, che nulla ha a che vedere con l'obbligo di cui all'art. 2, comma 1, del d.lgs. 7 marzo 2005, n. 82, gravante sulle PP.AA., di assicurare "la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale"»[49].

L'organo giudicante ha rilevato chiaramente come alla richiesta di accesso da remoto al sistema informatico dell'Ente non consegua alcun obbligo *ex lege* gravante in tal senso sullo stesso, considerato che le valutazioni concernenti le modalità più corrette al fine di permettere l'esplicazione del diritto di cui all'art. 43, c. 2, TUEL sono, in questo caso, rimesse al solo Comune, che, «a prioritaria tutela del pubblico interesse cui devono essere preordinati tutti gli atti e le iniziative assunte» non può in alcun modo prescindere dall' analisi della «fattibilità pratica dell' attivazione della postazione di accesso da remoto» e della sussistenza di eventuali non trascurabili «problematiche di carattere economico tecnico, di tutela della sicurezza del sistema informatico in uso e di trattamento dei dati personali contenuti e/o comunque veicolati dal sistema stesso»[50].

Così il Giudice di merito sottolineava come le modalità di corretto esercizio del diritto di accesso da parte del consigliere comunale possano essere individuate dalla sola Amministrazione richiesta, rilevato inoltre che «questo giudice non può in alcun modo invadere spazi intangibili di discrezionalità, né, tanto meno, sostituirsi all'Amministrazione in valutazioni di carattere organizzativo/funzionale che solo ad essa competono e che – si ribadisce – fuoriescono dal perimetro proprio della speciale forma di accesso spettante ai consiglieri comunali *ex* art. 43 d.lgs. 267/2000»[51]. Il TAR Friuli-Venezia Giulia, infine, rilevava, con specifico riferimento alla tutela dei dati personali che possono ben essere contenuti all'interno della documentazione che quotidianamente transita attraverso il programma di protocollo informatico, come «molti atti che vengono "veicolati" attraverso il protocollo comunale, anche se resi disponibili in forma di mera sintesi, possono rendere immediatamente consultabili "dati", anche personalissimi, che non possono considerarsi in alcun modo attratti nella sfera di necessaria conoscenza e/o conoscibilità che deve essere assicurata ai consiglieri comunali, sì da rendere, conseguentemente, ingiustificato il "trattamento" che in tal modo verrebbe effettuato [ ]

[49] Cfr. Sul punto, TAR Friuli-Venezia Giulia, sez. I, 9 luglio 2020, n. 253.

[50] *Ibid.*

[51] *Ibid.*

peraltro in assenza delle necessarie garanzie, essendo palese che il "segreto" cui sono tenuti i consiglieri comunali ai sensi dell' art. 43, comma 2, ult. periodo, d.lgs. cit. nulla ha a che vedere con le garanzie che devono, per l' appunto, presidiare il trattamento dei dati personali»; ne consegue come non si possa ritenere che la conoscenza di tali informazioni ricada nelle esigenze di mandato che rappresentano, come già detto, il limite intrinseco all' esercizio del diritto di accesso in commento[52].

L'organo giudicante ha evidenziato chiaramente come nell' identificazione delle modalità per rendere effettivo l' accesso, spetti al solo Comune compiere alcune prodromiche valutazioni, che dovranno comprendere inevitabilmente anche l' individuazione delle misure tecniche ed organizzative volte alla tutela dei dati personali coinvolti, stante l' impossibilità di ricondurre le garanzie richieste dal Reg. (UE) 2016/679 al semplice dovere di segreto.

Con ciò, vengono confermati i ruoli *data protection* come descritti nel paragrafo 3, tale per cui il Comune, in qualità di titolare del trattamento e dunque soggetto chiamato al rispetto del principio di *accountability*, alla richiesta del consigliere che voglia accedere, ai sensi dell'art. 43, c. 2, TUEL ai sistemi informatici dell' Ente, avrà il compito di mettere in atto misure tecniche e organizzative adeguate, per «garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento»[53] ciò sempre «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»[54].

Il consigliere comunale, autorizzato al trattamento, dovrà dunque attenersi alle indicazioni fornite dall' Ente per l' esercizio del proprio diritto sui generis, rilevata la necessità per tale soggetto, seppur qualificato, di attenersi alle istruzioni ricevute dal titolare del trattamento ai sensi del combinato disposto degli artt. 29 e 32 Reg. (UE) 2016/679 e dell'art. 2-*quaterdecies* d.lgs. 196/2003[55].

---

[52] *Ibid.* Di particolare interesse è poi il decalogo effettuato dal Giudice di prime cure, con riferimento alla tipologia di atti, e dunque di dati personali, che possono quotidianamente transitare all'interno del protocollo informatico dell'Ente, che si riporta qui di seguito: «Ritenuto, invero, in via meramente esemplificativa e non esaustiva, di richiamare l'attenzione su tutti gli atti riferibili ai compiti svolti dal Comune per servizi di competenza statale (si pensi ad es. alle comunicazioni riguardanti annotazioni sugli atti di anagrafe), sulle richieste e/o comunicazioni riguardanti la cessione del quinto dello stipendio, sugli atti provenienti da altre PP.AA. relativi a indagini in corso, sulle istanze e/o gli atti relativi alla fruizione degli istituti previsti e disciplinati dalla legge 5 febbraio 1992, n. 104 (Legge quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate) e/o dal decreto legislativo 26 marzo 2001, n. 151 (Testo unico delle disposizioni legislative in materia di tutela e sostegno della maternità e della paternità, a norma dell'articolo 15 della legge 8 marzo 2000, n. 53), sugli atti relativi ai TSO, sugli interventi assistenziali su disposizione del Tribunale per i minorenni, etc. etc.); Ritenuto *ictu oculi* evidente che trattasi di atti, come potrebbero esserlo, ad esempio, anche quelli afferenti a procedure di gara in corso dei quali è preclusa la diffusione allo scopo di evitare fenomeni distorsivi della concorrenza [n.d.r. il riferimento è all'art. 53, comma 2, lett. a) e b), e comma 3, del d.lgs. n. 50/2016], che non sono nemmeno latamente riconducibili alle esigenze di mandato, le quali trovano la propria ragione d'essere e, al contempo, il proprio limite nelle attribuzioni (tassative) del Consiglio comunale (cfr. art. 42 d.lgs. n. 267/2000) e nel correlato e complementare diritto d'iniziativa e/o di presentare interrogazioni o mozioni che la legge riconosce ad ogni consigliere comunale (cfr. art. 43, comma 1)».

[53] *Ex* art. 5, par. 2, Reg. (UE) 2016/679.

[54] *Ex* art. 32 Reg. (UE) 2016/679.

[55] Ad integrazione di quanto evidenziato, si ricordi anche che nella sentenza TAR Friuli-Venezia

5.4. Il caso specifico: l'utilizzo illegittimo delle informazioni acquisite a seguito dell'esercizio del diritto di accesso

Prima di procedere con le valutazioni conclusive, è sembrato opportuno concentrare la nostra attenzione anche alla seconda fattispecie eventuale, ovverosia quella concernente l' eventuale utilizzo illegittimo che il consigliere possa fare delle informazioni ricevute a seguito dell'esercizio del diritto di cui all'art. 43, c. 2, TUEL.
In merito, come già ampiamente dedotto, gli orientamenti del Garante per la Protezione dei Dati Personali sono stati uniformi nell' affermare come «il trattamento dei dati contenuti negli atti dell´amministrazione comunale, connesso all´espletamento del loro mandato, può essere effettuato dai consiglieri comunali che abbiano esercitato il diritto di accesso a tali atti, nel rispetto del diritto alla riservatezza degli interessati»[56], individuando con ciò la tutela a posteriori riconosciuta alla sfera personale dei soggetti interessati, connessa al richiamo al segreto effettuato dallo stesso art. 43, c. 2, TUEL.
E così, partendo da un principio ormai cogente nel nostro ordinamento, tale per cui «la comunicazione e la diffusione dei dati personali da parte di privati e di enti pubblici economici può prescindere dal preventivo consenso dell' interessato nel caso in cui il trattamento sia effettuato in adempimento di un obbligo previsto dalla legge, da un regolamento o da una norma comunitaria»[57], il consigliere non potrà utilizzare i dati entrati in suo possesso per finalità estranee all' effettivo esercizio delle funzioni consiliari individuate all' art. 42 TUEL, tali da ledere la riservatezza degli interessati coinvolti[58].
Tale è stato appunto l' orientamento interpretativo prevalente, che ha essenzialmente

Giulia, sez. I, 9 luglio 2020, n. 253 il Giudice ha rilevato come «è pacifico e innegabile che l'esercizio del diritto in questione non risulta, allo stato, in alcun modo compromesso o limitato, dato che il Comune ha, comunque, assicurato all'odierno ricorrente che "ove richiesto, potrà essere messa a Sua disposizione presso gli uffici dell'Ente una postazione pc alla quale potrà accedere tramite utilizzo di apposite credenziali per la consultazione telematica delle notizie necessarie in ragione dell'esercizio delle sue funzioni" (così l'atto impugnato - all. 2 fascicolo ricorrente), al punto da appalesare finanche l'inammissibilità per carenza di interesse della richiesta qui dal medesimo avanzata».

[56] Cfr. Garante Privacy, Registro dei provvedimenti del 28 febbraio 2008 [doc. web n. 1501081].

[57] Cfr. Garante Privacy, 29 maggio 1998, in *Bollettino* n. 4, pag. 9 [doc. web n. 42144].

[58] Cfr. Garante Privacy, Registro dei provvedimenti del 28 febbraio 2008 [doc. web n. 1501081]. Sul punto «Una segnalazione inviata da un Comune lamentava l'avvenuta pubblicazione, su sito web non direttamente riconducibile al comune medesimo, di dati personali concernenti contributi erogati dall'Amministrazione per l'acquisto di libri di testo per l'anno scolastico 2005/2006, e, in particolare, l'ammontare del contributo nonché, in taluni casi, le coordinate del relativo conto corrente bancario. Le risultanze istruttorie hanno evidenziato che la lista dei destinatari dei contributi era stata divulgata via Internet dal capogruppo consiliare di minoranza (cui una copia era stata precedentemente consegnata in ragione di asserite motivazioni concernenti l'esercizio del proprio mandato politico) e che tale divulgazione consentiva l'immediata accessibilità a chiunque alle citate informazioni tramite mera ricerca nominativa dei beneficiari, anche con l'ausilio di eventuali motori di ricerca. In proposito, si è rilevato che i consiglieri comunali che abbiano avuto accesso ad atti dell'amministrazione comunale per ragioni connesse all'espletamento del loro mandato devono rispettare il diritto alla riservatezza degli interessati. Poiché il trattamento dei menzionati dati è risultato, allo stato degli atti, in violazione dei princìpi di liceità, finalità e pertinenza e non eccedenza (art. 11, comma 1, lett. a), b) e d), del Codice), è stato disposto il blocco del relativo trattamento nelle more della definizione di ulteriori accertamenti da parte dell'Autorità» come dedotto dalla stessa Autorità Garante nella Relazione 2008 - 2 luglio 2009 Parte II - L'attività svolta dal Garante, 3. Il Garante e le pubbliche amministrazioni, [doc. web n. 1637571].

rilevato come il diritto di accesso del consigliere non incontri il limite della riservatezza, la quale opera indistintamente da tale diritto *sui generis*, a posteriori, con riferimento alle azioni eventualmente compiute dal soggetto qualificato[59].

Laddove le informazioni acquisite vengano utilizzate in violazione di tale diritto, il consigliere ne risponderà in qualità di titolare del trattamento, stante quanto già esplicitato al paragrafo 3.1., ricadendo sullo stesso tutte le responsabilità derivanti da tale qualificazione soggettiva e dalla relativa violazione.

Ne discende la definizione di una responsabilità che non tiene conto dell' atto di accesso, ma solamente delle condotte ad esso successive, con la configurazione di una tutela a metà, privata della corretta applicazione dei principi posti a fondamento della tutela del dato personale: è qui necessario provvedere ad una ricostruzione del sistema di tutele, al fine di procedere al menzionato bilanciamento tra i due interessi costituzionalmente garantiti, affinché la protezione dei dati personali cominci ad operare all' atto del primo trattamento, rappresentato appunto dall' accesso.

6. Riflessioni conclusive: sulla necessità di un bilanciamento tra i due interessi costituzionalmente garantiti, anche alla luce dell' art. 86 Reg. (UE) 2016/679

Una preliminare riflessione conclusiva, avente ad oggetto la necessità di introdurre il concetto di bilanciamento tra interessi costituzionalmente garantiti anche nella fattispecie oggetto della presente trattazione, discende come conseguenza diretta dall'analisi del diritto di accesso *ex* art. 43, c. 2, TUEL da un lato e del diritto alla tutela dei dati personali dall'altro, i quali si qualificano entrambi, senza ombra di dubbio, come diritti di rango costituzionale.

In particolare, già al paragrafo 2 del presente lavoro si è avuto modo di evidenziare come il diritto di accesso riconosciuto dal nostro ordinamento ai consiglieri comunali e provinciali affondi le sue radici negli artt. 3 e 97 Cost. come espressione del principio democratico di autonomia locale e della rappresentanza esponenziale, qualificando dunque lo stesso quale interesse costituzionalmente garantito.

La stessa tutela di rango costituzionale viene riconosciuta anche al diritto alla riservatezza personale, oggi meglio e più ampiamente declinato, anche a seguito dell' entrata in vigore del Reg. (UE) 2016/679, nel diritto alla tutela del trattamento dei dati personali. Tale diritto è stato storicamente inteso e definito come un diritto fondamentale, un diritto della personalità, che non trova un riconoscimento esplicito nel sistema normativo ma che può essere ricavato per via interpretativa dal combinato disposto degli articoli 2, 13, 15 e 21 della Costituzione[60].

[59] Si veda, ad integrazione delle sentenze già ivi richiamate, anche Cons. Stato, sez. V, 2 marzo 2018 n. 1298.

[60] L'art. 2 e l'art. 13 Cost. nello specifico, laddove il primo rappresenta il riconoscimento di tutti i diritti inviolabili dell'uomo e il secondo è madre di tutte le libertà riconosciute dal nostro ordinamento, costituiscono l'alveo all'interno del quale la Corte Costituzionale, sin dal 1973, ha visto svilupparsi e crescere il seme della tutela della riservatezza personale, sino al riconoscimento definitivo ottenuto a mezzo della formulazione dell'art. 117 Cost. Si ricordi sul punto quanto affermato nella celebre sentenza

Come già ampiamente definito al paragrafo 4 del presente lavoro, la privacy oggi individua una famiglia di diritti inviolabili dell'uomo, che attengono a bisogni primari dell' essere umano, evolutasi a partire dal «diritto ad essere lasciati soli», per arrivare a definire un insieme di tutele integrato a bisogni connaturati dell' essere umano, costituzionalmente garantiti.

I connotati di rilievo costituzionale riconosciuti ad ambedue gli interessi impongono la necessità, laddove questi entrino in conflitto, di provvedere ad un loro bilanciamento, a mezzo di un confronto continuo tra gli stessi, volto a determinare un punto di equilibrio nella fattispecie concreta, realizzando il minor sacrificio possibile del diritto pregiudicato.

A differenza però di tutte le altre casistiche nelle quali si può produrre un conflitto tra tutela del dato personale e tutela di un altro interesse costituzionale[61], la fattispecie concernente il diritto di accesso ex art. 43, c. 2, TUEL non ha trovato, sino ad oggi, nel nostro ordinamento, alcun richiamo specifico alla necessità di provvedere a tale bilanciamento; nessuna menzione al bilanciamento è fatta dal TUEL, e così nessuna menzione viene compiuta dallo stesso d.lgs. 196/2003 a seguito della sua riformulazione del 2018.

La fattispecie, dunque, sembra in un qualche modo essere stata dimenticata, come suggerito anche nei precedenti paragrafi, a causa della confusione dei confini tra tutela del dato personale e riservatezza personale, ma la stessa merita qui di essere analizzata in tal senso.

In particolare, si richiama in questa sede l' art. 86 Reg. (UE) 2016/679, che recita «I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l' autorità pubblica o l' organismo pubblico sono soggetti, al fine di conciliare l' accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento»[62]. Il richiamato

Corte Cost., 5 aprile 1973, n. 38, ove la Consulta ha avuto modo di evidenziare come «Non contrastano con le norme costituzionali ed anzi mirano a tutelare e a realizzare i fini dell'art. 2 affermati anche negli artt. 3, secondo comma, e 13, primo comma, che riconoscono e garantiscono i diritti inviolabili dell'uomo, fra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza**,** intimità e reputazione, sanciti espressamente negli artt. 8 e 10 della Convenzione europea sui diritti dell'uomo, gli artt. 10 del codice civile».

[61] Si pensi semplicemente al conflitto tra tutela del dato personale e trasparenza amministrativa.

[62] La norma è espressione dei principi definiti dal considerando (154) che prevede come «Il presente regolamento ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali. L'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico. I dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti. Tali disposizioni legislative dovrebbero conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali e possono quindi prevedere la necessaria conciliazione con il diritto alla protezione dei dati personali, in conformità del presente regolamento. Il riferimento alle autorità pubbliche e agli organismi pubblici dovrebbe comprendere, in tale contesto, tutte le autorità o altri organismi cui si applica il diritto degli Stati membri sull'accesso del pubblico ai documenti. La direttiva 2003/98/CE del Parlamento europeo e del Consiglio (14) non pregiudica in alcun modo il livello di tutela delle persone

concetto di bilanciamento, dunque, permea il Reg. (UE) 2016/679, in quanto fonte sovraordinata per i principi di diritto comunitario, determina una necessaria interazione del contemperamento in tutte le ipotesi di accesso ai documenti ufficiali in possesso dell' autorità pubblica, e così anche al caso *sui generis* previsto dall'art. 43, c. 2, TUEL.
Risulta allo stesso modo incompleta la disciplina delineata dal legislatore nazionale nella nuova formulazione dell'art. 59 d.lgs. 196/2003, rubricato "Accesso a documenti amministrativi e accesso civico", che dimentica di tenere in debito conto le ulteriori ipotesi speciali di accesso ai documenti amministrativi quale quello in commento, occupandosi solamente dell' accesso documentale, civico e civico generalizzato; nonostante ciò, rilevata la forza normativamente riconosciuta al regolamento comunitario quale fonte normativa sovraordinata, non possiamo che concludere come il diritto *ex* art. 43, c. 2, TUEL dovrà sempre trovare un corretto bilanciamento con gli altri interessi costituzionali in gioco, primo tra tutti il diritto alla protezione dei dati personali, anche in assenza di una specifica disposizione normativa che indichi tale necessità di contemperamento.
L'applicazione trasversale della normativa transnazionale in materia di *data protection* erode così la forza sinora incontrastata del diritto di accesso dei consiglieri, richiamando gli operatori e gli interpreti al necessario contemperamento continuo tra interessi, e tratteggiando così alcuni innegabili limiti per l' esercizio di tale facoltà.
Come si avrà modo di meglio evidenziare qui di seguito, gli strumenti di tale fondamentale bilanciamento dovranno essere rilevati nei principi fondamentali di cui agli artt. 5, 24, 25 e 32 Reg. (UE) 2016/679: in particolare, l'attitudine al bilanciamento che caratterizza il diritto alla tutela dei dati personali deriva, come conseguenza diretta, dall' applicazione dei principi di necessità e proporzionalità[63], nonché dei principi cardine, regolatori della materia.

fisiche con riguardo al trattamento dei dati personali ai sensi delle disposizioni di diritto dell'Unione e degli Stati membri e non modifica, in particolare, gli obblighi e i diritti previsti dal presente regolamento. Nello specifico, tale direttiva non dovrebbe applicarsi ai documenti il cui accesso è escluso o limitato in virtù dei regimi di accesso per motivi di protezione dei dati personali, e a parti di documenti accessibili in virtù di tali regimi che contengono dati personali il cui riutilizzo è stato previsto per legge come incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali».

[63] Si deve ricordare in tale sede il richiamo effettuato dal considerando 4 del Reg. (UE) 2016/679, che prevede come «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità». La Corte Costituzionale, inoltre, con la sentenza 21 febbraio 2020, n. 20, ricorda come «la Corte di giustizia dell'Unione europea ha ripetutamente affermato che le esigenze di controllo democratico non possono travolgere il diritto fondamentale alla riservatezza delle persone fisiche, dovendo sempre essere rispettato il principio di proporzionalità, definito cardine della tutela dei dati personali: deroghe e limitazioni alla protezione dei dati personali devono perciò operare nei limiti dello stretto necessario, e prima di ricorrervi occorre ipotizzare misure che determinino la minor lesione, per le persone fisiche, del suddetto diritto fondamentale e che, nel contempo, contribuiscano in maniera efficace al raggiungimento dei confliggenti obiettivi di trasparenza, in quanto legittimamente perseguiti (sentenze 20 maggio 2003, nelle cause riunite C-465/00, C-138/01 e C-139/01, Österreichischer Rundfunk e altri, e 9 novembre 2010, nelle cause riunite C-92/09 e 93/09, Volker und Markus Schecke e Eifert)».

6.1. Conclusioni. Gli strumenti del bilanciamento: l'applicazione dei principi di *data protection* al diritto di accesso *ex* art. 43, c. 2, TUEL

L'attrazione del diritto di accesso dei consiglieri all'interno dell'orbita del Reg. (UE) 2016/679 comporta la necessaria applicazione di tutti i principi fondamentali, posti alla base delle tutele riconosciute ai dati personali, sin dal primo momento di attuazione di tale trattamento.

In tal senso l'applicazione concreta dei principi di *data protection* anche alla fattispecie qui analizzata si configura come *conditio sine qua non* per la realizzazione dell'equilibrio tra i due interessi.

E così, l' Ente destinatario delle richieste, titolare del trattamento, dovrà assicurare anche all' atto dell' esercizio del diritto di accesso del consigliere che i fondamentali principi di cui all' art. 5 Reg. (UE) 2016/679 siano rispettati. In particolare, l' Amministrazione dovrà compiere alcune valutazioni preliminari al riconoscimento del diritto di accesso, volte ad indagare la corrispondenza tra i dati richiesti e le finalità di esercizio di tale facoltà da parte del consigliere: di conseguenza, un primo limite intrinseco all' esercizio di tale diritto *sui generis* si ricava dall'applicazione necessaria dei principi di minimizzazione e limitazione delle finalità, primi strumenti di bilanciamento che ci ricordano come i dati personali debbano essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati con modalità che non siano incompatibili con tali finalità, e debbano essere mantenuti adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, legandosi tale principio a quello, ugualmente fondamentale, di *privacy by design e by default*, con la conseguenza che il titolare del trattamento sarà chiamato ad usare tanti e quali dati quanti ne siano necessari per le finalità che sono state individuate nelle linee direttrici dei principi di trattamento.

Non corrisponde così al vero l' affermazione per la quale il diritto all' informazione qui in commento è privo di limitazioni con riferimento al suo esercizio, considerato che le richieste dovranno essere vagliate alla luce dell' art. 5 Reg. (UE) 2016/679; tale rilievo era già stato compiuto dallo stesso Garante per la Protezione dei Dati Personali nel 2009, laddove con una specifica nota aveva rilevato come «spetta all´amministrazione destinataria della richiesta accertare il fondamento della pretesa all´informazione *ratione officii* del consigliere comunale, con valutazione eventualmente sindacabile dal giudice amministrativo»[64].

L' accessibilità alle informazioni contenenti dati personali, siano essi definiti quali dati personali comuni, relativi a categorie particolari di dati oppure concernenti reati e condanne penali[65], dovrà superare il vaglio dei principi di finalità e minimizzazione, e le

[64] Cfr. Garante Privacy, in Relazione 2008 - 2 luglio 2009 Parte II - L'attività svolta dal Garante, 3. Il Garante e le pubbliche amministrazioni, [doc. web n. 1637571], laddove l'Autorità ricordava anche come «resta ferma la necessità che i dati personali così acquisiti dagli aventi diritto siano utilizzati effettivamente per le sole finalità realmente pertinenti al mandato, rispettando il dovere di segreto nei casi specificamente determinati dalla legge, nonché i divieti di divulgazione dei dati personali».

[65] L'applicazione di tali principi non dipende, infatti, dalla tipologia di dati personali coinvolti nelle richieste del consigliere: essi si applicano anche con riguardo ad informazioni che contengano solo dati personali comuni, implicando la necessaria riconduzione delle richieste alle "esclusive" finalità di

stesse dovranno essere così inerenti le funzioni collegate al *munus* di questi soggetti qualificati. Ne discende un' implicita necessità per l' Amministrazione di verificare l'oggetto della richiesta, circoscrivendo l'ambito delle operazioni ai soli dati personali appunto indispensabili per la realizzazione dello scopo perseguito dal consigliere richiedente.

Non solo. L'applicazione dei principi di cui all' art. 25 Reg. (UE) 2016/679 conferma ancora una volta come le tutele volte alla protezione dei dati personali debbano essere individuate ed implementate «sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento», e dunque all' atto stesso dell' esercizio del diritto di accesso, al fine di «garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento».

In questo modo, si ridurrà anche la possibilità che a seguito del conseguimento delle informazioni, il consigliere possa porre in essere condotte in grado di violare i diritti riconosciuti e garantiti dal Reg. (UE) 2016/679 e dal d.lgs. 196/2003: egli avrà infatti diritto di accedere, in ragione della propria funzione istituzionale, a tanti e quali dati personali siano effettivamente necessari allo svolgimento del mandato elettivo, e gli stessi potranno così essere successivamente utilizzati in funzione del *munus* qui richiamato[66].

Ulteriori riflessioni si rendono opportune con riferimento all'applicazione delle disposizioni di cui agli artt. 24 e 32 Reg. (UE) 2016/679 come diretta conseguenza del principio di *accountability*, al fine di riprendere ed approfondire qui i rilievi prima facie esposti dalla sentenza TAR Friuli-Venezia Giulia n. 235/2020 sopra esposta per esteso. In particolare, spettando al solo Ente destinatario della richiesta l' individuazione delle modalità più corrette per permettere al consigliere di esercitare il diritto di cui all'art. 43, c. 2, TUEL, le valutazioni rimesse al titolare del trattamento dovranno necessariamente tenere conto dei profili di sicurezza e tutela dei dati personali coinvolti nel trattamento, ai sensi dell'art. 32 Reg. (UE) 2016/679 e più in generale nel rispetto dell'intera

rilevante interesse pubblico «direttamente connesse all'espletamento di un mandato elettivo», con la conseguente estensione delle riflessioni effettuate dal Garante con provvedimento Garante Privacy, Registro dei provvedimenti n. 369 del 25 luglio 2013 [doc. web n. 2536172], pronunciandosi in merito alla richiesta di ostensione di una cartella clinica e di certificazioni sanitarie, contenenti categorie particolari di dati, da parte di un consigliere regionale.

[66] Gli stessi rilievi si possono compiere anche sulla base di precedenti giurisprudenziali, come ad esempio le annotazioni del Garante per la Protezione dei Dati Personali, che nella Relazione 2007 - Garanzie e sicurezza nel trattamento dei dati: l'attività dell'Autorità - 16 luglio 2008 rilevava come «Sono stati forniti chiarimenti a un comune sulla condotta tenuta da un consigliere comunale il quale, dopo aver esercitato l'accesso ai dati contenuti nell'anagrafe della popolazione residente, ottenendo l'elenco di cittadini minorenni ricompresi in una determinata fascia di età, aveva successivamente trasmesso tale elenco a una società sportiva. Quest'ultima aveva utilizzato i dati personali in questione inviando ai minori una comunicazione promozionale in ordine all'attività esercitata e pubblicizzando, altresì, la proposta di adesione alla medesima tramite la richiesta di pagamento di una quota associativa. L'Ufficio ha rilevato che, in linea generale, il comune aveva agito correttamente nei confronti della richiesta di accesso formulata dal consigliere comunale ai sensi dell'art. 43 del d.lgs. n. 267/2000, in quanto all'ampia e qualificata pretesa non sono opponibili profili di riservatezza, a condizione che i documenti e le informazioni richiesti siano pertinenti all'esercizio del mandato. Non è apparsa invece conforme al quadro normativo di riferimento la trasmissione ad un soggetto privato dei dati anagrafici legittimamente ottenuti, in quanto tale comunicazione non risultava direttamente funzionale alla cura di un interesse connesso al mandato conferito al consigliere comunale (Nota 28 novembre 2007)».

normativa in materia di riservatezza dei dati personali.
Di conseguenza, sarà compito del titolare del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi del trattamento, individuare quali siano le modalità più corrette per l' espletamento di tale accesso, al fine di garantire la sicurezza delle informazioni personali coinvolte nel trattamento. Tali valutazioni saranno richieste in modo particolarmente pregnante ogniqualvolta il consigliere chieda di poter accedere da remoto ai gestionali informatici dell'Ente; l'identificazione delle misure sia tecniche (come ad esempio i sistemi volti ad assicurare su base permanente la sicurezza e la resilienza dei servizi di trattamento e il ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico *ex* art. 32, par. 1, lett. *b)* e *c)*) che organizzative è rimessa completamente al titolare del trattamento, il quale dovrà caso per caso valutare quali misure possano essere maggiormente adeguate, in rapporto ai rischi nello specifico evidenziati per i diritti e le libertà dei soggetti interessati, derivanti dal trattamento delle loro informazioni personali. Ne consegue che, con riferimento alle richieste di accesso al protocollo informatico, ad esempio, laddove l'Ente ritenga di non possedere una struttura informatica adeguatamente protetta, tale da poter permettere l'esplicazione di un accesso da remoto (e da pc personale) in totale sicurezza, con evidenti rischi per la sicurezza dei dati personali eventualmente coinvolti, sarà ben possibile per lo stesso provvedere all' individuazione di modalità di accesso alternative: ad esempio, la messa a disposizione di una postazione del Comune, attrezzata *ad hoc* per permettere l'accesso nominativo, in sola consultazione al solo registro di protocollo, come prospettato dallo stesso TAR Friuli-Venezia Giulia.
In tale contesto merita una menzione la necessaria valutazione, al fine di individuare le misure tecniche ed organizzative da adottare, dell'elemento richiamato nell'art. 32 Reg. (UE) 2016/679 concernente i "costi di attuazione". Specificamente, in un'ottica di interpretazione congiunta delle diverse normative che disciplinano, nel nostro ordinamento, l'accesso in via digitale ai dati della Pubblica Amministrazione, la presente analisi non può prescindere dalla valutazione delle disposizioni contenute nel CAD (Codice dell' Amministrazione Digitale, d.lgs. 82/2005). Tale testo impone a tutte le Pubbliche Amministrazioni di assicurare «la disponibilità, la gestione, l' accesso, la trasmissione, la conservazione e la fruibilità dell' informazione in modalità digitale», «utilizzando con le modalità più appropriate le tecnologie dell' informazione e della comunicazione»[67]; con riferimento a tale indicazione, l'attenzione deve essere rivolta in modo particolare alla previsione di cui all'art. 50, c. 1, dello stesso CAD, che impone che «i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l' uso delle tecnologie dell' informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall' ordinamento, da parte delle altre pubbliche amministrazioni e dei privati». Tale previsione normativa determina, inoltre, il fondamento giuridico dell' esercizio dell'accesso, ai sensi dell'art. 43, c. 2, TUEL, con possibilità di ingresso nel sistema informatico dell' Ente (ed in particolare al registro del protocollo informatico) come già visto.
La fruibilità dei dati della Pubblica Amministrazione in forma digitale è normativa-

[67] Si veda l'art. 2 c. 1, CAD d.lgs. 82/2005.

mente prevista, ma si deve ritenere come la valutazione concernente l' implementazione dei sistemi con i quali tale accessibilità deve essere garantita debba essere rimessa ad un' opportuna analisi dell' Ente nel caso di specie: tale orientamento corrisponde anche con quello recentemente espresso dal TAR Campania Salerno nella già menzionata sentenza n. 545/2019. Il Giudice di prime cure ha affermato infatti come «la complessiva disciplina risultante dal richiamato CAD impone che la fruibilità dei dati e delle informazioni in modalità digitale debba essere garantita con modalità adeguate (in finalità informativa) ed appropriate (alla tecnologia disponibile), sicché grava sull' amministrazione l' approntamento e la valorizzazione di idonee risorse tecnologiche che, senza aggravio eccessivo sulle risorse pubbliche, appaiano in grado di soddisfare, in una logica di bilanciamento, le esigenze rappresentate dalla trasparenza amministrativa»[68]. Pertanto, le valutazioni condotte dal titolare del trattamento, e dunque dall' Amministrazione interpellata, dovranno determinare un' analisi globale della situazione, monitorando sia gli aspetti di accessibilità previsti dal CAD sia le esigenze di tutela dei sistemi ed in ultima istanza (non per importanza) le necessità di protezione dei dati personali coinvolti nel trattamento, tenendo conto anche delle imprescindibili condizioni economiche dell'Ente.

Tutto ciò dedotto, nell' auspicio che il Garante per la Protezione dei Dati Personali possa pronunciarsi chiaramente in merito alla necessità di un bilanciamento tra gli interessi in gioco nella fattispecie qui analizzata, non si può che concludere affermando l'indispensabile applicazione dei principi concernenti la *data protection* anche al diritto di accesso *ex* art. 43, c. 2, TUEL, con una rimodulazione dei confini di tale diritto *sui generis*, volti ad un corretto bilanciamento con la protezione dei dati personali, al fine di definire un sistema integrato di tutele che possa operare non soltanto *ex post*, ma sin dal primo momento di tale trattamento.

[68] Cfr. TAR Campania Salerno, sez. II, 4 aprile 2019, n. 545.

Quando il datore di lavoro diviene un algoritmo: la trasformazione del potere del datore di lavoro in algocrazia. Quale spazio per l'applicazione dei principi costituzionali?*

Camilla Della Giustina

Abstract

Il mondo del lavoro ha subito delle profonde trasformazioni a seguito dell'applicazione degli sviluppi tecnologici. Particolare attenzione viene dedicata alla fattispecie della determinazione della prestazione lavorativa ad opera di un algoritmo. La riflessione che viene proposta, in questo breve contributo, concerne il rapporto che intercorre tra l'algocrazia e il rispetto dei principi costituzionali dettati in materia di diritto del lavoro.

The world of work has undergone profound changes as a result of the application of technological developments. Particular attention shall be paid to the specific case of the determination of work performance by an algorithm. The reflection that is proposed, in this short contribution, concerns the relationship between the algocracy and the respect of the constitutional principles dictated in the matter of labor law.

Sommario

1. Introduzione. - 2. Le coordinate del rapporto tra diritto del lavoro e rivoluzione tecnologica. - 3 Il principio lavorista. - 4. Il principio lavorista applicato alla *gig economy*: un ossimoro?. - 5. Conclusioni.

Keywords

algocrazia – principi costituzionali – principio lavorista – evoluzione tecnologica – *gig economy*

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

«La rivoluzione informatica ha fatto guadagnare un sacco di tempo libero agli uomini. Il problema è che gli uomini lo passano con il computer»
(Anonimo)

1. Introduzione

Le controversie incardinate dai rider o la *querelle* giudiziaria che ha visto coinvolto Uber pongono delle problematiche e delle riflessioni che oltrepassano la questione qualificatoria che si pone in merito alla posizione contrattuale di questi ultimi. Gli interrogativi che emergono e che vengono sollecitati riguardano i rapporti inerenti tra tecnica e diritto e, precisamente ci si chiede se il diritto possa dominare la tecnica attraverso una forma di regolamentazione oppure se la tecnica, a causa della propria onnipotenza, non sia suscettibile di regolamentazione[1].
Per cercare di fornire una risposta agli interrogativi appena esposti si è deciso di affrontare la questione attraverso la prospettiva del diritto costituzionale e, precisamente, sulla scorta dell'interpretazione delle nuove forme lavorative gestite tramite piattaforme e algoritmi alla luce del principio lavorista contenuto nella Costituzione italiana. Il metodo consiste quindi in una prima esposizione del rapporto che intercorre tra il diritto del lavoro e la rivoluzione tecnologica provvedendo quindi ad analizzare il concreto funzionamento del lavoro gestito da algoritmi per poi approdare alla riflessione di diritto costituzionale. In base a quest'ultima verrà evidenziata la centralità del diritto al lavoro all'interno della Carta costituzionale italiana in quanto esso risulta essere contenuto non solo all'interno dei principi fondamentali ma anche in quella che viene definita come Costituzione economica.
Successivamente si analizzerà il rapporto che intercorre tra il principio lavorista e la *gig economy* chiedendosi quindi se, a seguito dell'evoluzione tecnologica applicata al mondo del lavoro, il principio lavorista risulti essere rispettato oppure se lo stesso possa essere definito come un principio dimenticato e appartenente all'oblio costituzionale.

2. Le coordinate del rapporto tra diritto del lavoro e rivoluzione tecnologica

La quarta rivoluzione industriale, secondo quanto definito dal Governo nel documento riguardante l'industria 4.0, risulta derivare dalla combinazione di undici tecnologie, ossia: robotica, robotica collaborativa, *Internet of things*, *big data*, *cloud computing*, sicurezza informatica, stampa 3D, simulazione, nanotecnologie ed infine materiali intelligenti. Le precedenti rivoluzioni hanno avuto quali elementi caratterizzanti la macchina a vapore (prima rivoluzione tecnologica) avvenuta tra il 1700 e il 1800, l'elemento peculiare della seconda è stato il lavoro all'interno delle fabbriche (fine 1800), la terza,

[1] M. Novella, *Il rider non è un lavoratore subordinato ma è tutelato come se lo fosse*, in *Labour Law and Issues*, 55(1), 2019, 84 ss.

realizzatasi a partire dalla metà del 1900, è stata quella del *computer*.
Nel momento in cui ci si approccia alla quarta rivoluzione ci si rende conto che l'aspetto di novità riguarda l'interazione tra uomo e ogni nuova tecnologia; proprio per questo si tratta di una rivoluzione che possiede un impatto senza alcun precedente in quanto incide sulla prestazione di lavoro, sull'occupazione e di conseguenza sulla nuova definizione di uomo.
Analizzando le conseguenze che questa rivoluzione determina nell'ambito che qui interessa, ossia il diritto del lavoro, esse, sostanzialmente, si traducono in una ri-definizione degli spazi poiché si vuole sostituire lo spazio fisico con quello virtuale dando forma a nuove modalità di esecuzione della prestazione lavorativa, cioè, *crowd work*[2], *work-on-demand via app* [3]e *smart-working*.
Il principale aspetto problematico è dato dall'impatto che queste nuove modalità possono determinare nella stessa concezione di uomo: in altri termini vi è il rischio che l'uomo iniziando ad interagire con la macchina arrivi a rinunciare al contatto con l'altro con l'ulteriore conseguenza di non staccarsi mai dai dispositivi mobili utilizzati nell'esecuzione della prestazione lavorativa.
Queste riflessioni relative a quella che è stata definita la innovazione distruttiva hanno iniziato ad animare il dibattito dottrinario in maniera particolarmente accesa a partire dal cd. Caso Uber[4]. Il fenomeno Uber, infatti, ha posto differenti questioni di carattere generale che, a loro volta, hanno prodotto delle ripercussioni e implicazioni teoriche per i giuristi.
Il primo aspetto da analizzare è strettamente socio-economico poiché è strettamente connesso al ruolo svolto dalla piattaforma digitale nell'organizzazione dei rapporti economici e sociali: il gestore della piattaforma risulta essere il nuovo intermediario fra colui che cerca e colui che offre un determinato servizio.
In secondo luogo l'emersione di questi nuovi intermediari determina la creazione di nuovi mercati[5] che prima possedevano dimensioni ridotte oppure non esistevano e su

[2] È caratterizzato dalla distribuzione lavorativa su piattaforma digitali che permettono a un committente (*crowdsourcer*) di affidare in *out-sourcing* a una folla indeterminata di lavoratori compiti che gli stessi possono sviluppare da remoto posto che gli incarichi possono riguardare sia *micro-tasks* sia *macro-tasks*. G. Valenduc - P. Vendramin, *Le travail dans l'économie digitale: continuités et ruptures*, in *WP ETUI*, 3, 2016, 35 ss.

[3] Il tratto peculiare è quello di concretizzarsi in attività che vengono coordinate in rete ma eseguite in quella che può essere definita come l'economia reale. E. Dagnino, *Una questione di fiducia: la reputazione ai tempi delle piattaforme online tra diritto alla privacy e prospettive di mercato*, in *Diritto delle Relazioni Industriali*, 1, 2017, 247 ss.

[4] Esso risulta essere particolarmente importante per tre elementi: il gruppo Uber risulta essere il più rilevante operatore economico riconducibile alla *sharing economy*, opera in un peculiare terreno di competizione ed infine il suo ingresso nel mercato ha determinato conseguenze giuridiche concernenti la natura dei servizi resi rispetto alle regole già dettate per i vettori tradizionali.
In relazione ai servizi offerti tramite questa modalità si è pronunciata la Corte di giustizia dell'Unione europea la quale, a seguito del rinvio operato da un giudice spagnolo, ha affermato che Uber «crea al contempo un'offerta di servizi di trasporto urbano che rende accessibile segnatamente con strumenti informatici […] e di cui organizza il funzionamento generale» evidenziando altresì che Uber esercita un'influenza determinante sulle condizioni della prestazione di siffatti conducenti». CGUE, C-434/15, *Asociación Profesional Elite Taxi* (2017).

[5] A.J. Wood - M. Graham - V. Lehdonvirta - I. Hiorth, *Good Gig, Bad Gig: Autonomy and Algorithmic Control in the Global Gig Economy*, in *Work, Employement and Society*, 33(1), 2019, 56 ss.

questi nuovi mercati vengono offerti e acquistati i fattori tradizionali della produzione, cioé forza lavoro e beni immobili[6].

La peculiarità di Uber è quella di aver prodotto e successivamente immesso nel mercato un'applicazione *software mobile* (app) su smartphone*;* questa app è in grado di consentire l'incontro fra la domanda e l'offerta di mobilità urbana: in questo modo si realizza una community in cui gli iscritti, ossia i *drivers*, e gli utenti possono accedere ad informazioni di geolocalizzazione, visualizzazione dei tempi di attesa nonché mettersi in contatto tra di loro per definire gli estremi della prestazione di trasporto. Il corrispettivo che l'utente deve al *driver* per l'esecuzione della prestazione è determinato dal gruppo Uber e quantificato grazie ad una elaborazione algoritmica secondo il meccanismo del *surge pricing*, ossia il prezzo della prestazione cresce in maniera proporzionale all'aumentare della domanda[7].

Se il caso Uber rappresenta il punto a partire dal quale la riflessione giuridica ha preso le mosse, attualmente l'attenzione dei giuristi è incentrata sulla progressiva semplificazione digitale che risulta essere ampiamente diffusa nei settori riguardanti le politiche del lavoro e dell'occupazione, della tutela del lavoro e del sistema previdenziale. Queste risultano essere svolte solamente con il mero supporto delle tecnologie informatiche: il modello economico risulta essere centrato sulla *gig economy*[8] cioè su piattaforme digitali[9] nelle quali «l'autonomia negoziale degli utenti è talora surrogata dalla "mano invisibile" degli algoritmi»[10]. Il risultato di questo modello lavorativo è che il *gig worker*

---

[6] V. Zeno-Zencovich, *Uber: modello economico e implicazioni giuridiche*, in *questa Rivista*, 1, 2018, 140 ss.

[7] L. Belviso, *Il caso Uber negli Stati Uniti e in Europa fra mercato, tecnologia e diritto. Obsolescenza regolatoria e ruolo delle Corti*, in *questa Rivista*, 1, 2018, 144 ss.

[8] La *gig economy* è caratterizzata dalla presenza di prestazioni lavorative intermittenti e flessibili nonché dalla offerta di prestazioni *on demand* da parte dei *gig workers*.
Quando ci si approccia al lavoro su piattaforma si fa riferimento a un fenomeno assai variegato comprendente al proprio interno diverse attività come, ad esempio, l'organizzazione di consegne e distribuzioni di beni mediante *riders*. M. Faioli, *Mansioni e macchina intelligente*, Torino, 2018.
«L'economia delle piattaforme nel confezionare la libertà dei *gig workers*, affina e consolida l'idea di un potenziale emancipatorio del lavoro *app driven*: il prestatore è «imprenditore di sé stesso», spinto – gentilmente – verso una efficiente e consensuale forma di autosfruttamento. L'esperienza sinora maturata ci suggerisce una lettura più critica – ma non per questo neo-luddista – circa la trasformazione in atto dell'economia e del lavoro, in questo senso l'invisibilità del lavoro – subordinato «gentilmente» – è una deriva sociale pericolosa che si insinua nell'agenda digitale UE». F. Bano, *Il lavoro invisibile nell'agenda digitale di Europa 2020*, in *Lavoro e diritto*, 3, 2020, 483.
Gli aspetti problematici erano già stati evidenziati nel discorso di Hilary Clinton del 2015, nel quale la stessa sostenne che «*this on-demand, or so-called gig economy is creating exciting economies and unleashing innovation, but it's also raising hard questions about workplace protections and what a good job will look like in the future*».

[9] Inizialmente le piattaforme digitali sono nate per immagazzinare le informazioni immesse dagli utenti e successivamente procedere ad una operazione di rielaborazione delle stesse. Questo procedimento, a sua volta, genera ulteriori dati la cui progressiva accumulazione ha permesso lo sviluppo e l'espansione dell'e-commerce. Uno sviluppo successivo è stato quello della digitalizzazione del mercato di beni e servizi per poi approdare, in ultima battuta, alla conservazione di queste informazioni e dei relativi *feedback* su piattaforme digitali di tipo *cloud*. E. Raimondi, *Il lavoro nelle piattaforme digitali e il problema della qualificazione della fattispecie*, in *Labour & Law Issues*, 5(2), 2019, 59 ss.

[10] G. Arrigo, *Il lavoro al tempo della "subordinazione digitale" (cominciò con un clic e finì con un sms),* in *TCRS*, 1(18), 2019, 72-73.
Per algoritmo si intende «una procedura sistematica di calcolo, più specificamente una sequenza di istruzioni non ambigue che muovono da un problema e ne costruiscono la soluzione in modo univoco (ovvero «deterministico») in un numero infinito di passi». M. Mezza, *Algoritmi di libertà. La potenza del*

è obbligato a sommare un numero assai elevato di prestazioni lavorative al fine di ottenere quella che è definita dalla Carta costituzionale italiana una «retribuzione sufficiente ad assicurare a sé e alla famiglia un'esistenza libera e dignitosa» (art. 36 Cost.). In altri termini «il progresso tecnologico ha facilitato nuove forme di lavoro, caratterizzate da alti livelli di flessibilità, e nuove opportunità di partecipazione al mercato del lavoro, attraverso diverse tipologie lavorative e sfide connesse alle definizioni esistenti di rapporto di lavoro[11]».

È evidente quindi che il sistema delle tutele deve essere adattato a questa nuova tipologia di lavoro prevendendo una applicazione di quella già presenti come: sicurezza del lavoro, assicurazione contro gli infortuni, contribuzione e tutela previdenziale, limite orario e previsione di pause di lavoro. Si ritiene che questi elementi debbano essere adattati e applicati al lavoro su piattaforma dato che lo stesso realizza non solo una potenziale disumanizzazione dei ritmi di lavoro organizzati e diretti dalle macchine ma anche la difficoltà di individuare e gestire i tempi di recupero delle energie psico-fisiche oltre ai riposi[12]. A tal proposito è doveroso richiamare l'attenzione mostrata dal Parlamento europeo circa l'impatto della rivoluzione digitale sul mercato del lavoro nonché sui diritti dei lavoratori: questo si dovrebbe tradurre in una previsione di «regimi di assicurazione sanitaria e di sicurezza sociale» ai quali deve unirsi un controllo effettivo da parte degli Stati membri circa «tutti i termini e condizioni del rapporto di lavoro o del contratto di servizi, prevenendo gli abusi di posizione dominante da parte delle piattaforme[13]».

Questa nuova riflessione risulta essere non solo necessaria ma altresì doverosa poiché le informazioni nella piattaforma digitale vengono elaborate e scambiate ad una velocità talmente elevata da determinare la disintermediazione tra produzione e consumo. L'aspetto centrale di questo meccanismo è l'algoritmo, il quale, a sua volta, diviene funzionale a dissimulare la natura dell'impresa stessa[14]. In altri termini la piattaforma

calcolo tra dominio e conflitto, Roma, 2018, spec. 27.

[11] È tratto dalla presentazione del sito della multinazionale olandese Randstad, considerata la seconda agenzia al mondo nel campo della ricerca, selezione e formazione di risorse umane.

[12] S. Ciucciovino, *Le nuove questioni di regolazione del lavoro nell'industria 4.0 e nella Gig economy: un problem framework per la riflessione,* in *Astril,* working paper n. 36/2018, 3 ss.
È possibile richiamare, a tal proposito, la Carta dei diritti fondamentali del lavoro digitale nel contesto urbano promossa dal Comune di Bologna con l'obiettivo di «migliorare le condizioni di lavoro dei lavoratori e collaboratori digitali», stabilendo «standard minimi di tutela che si applicano a tutti i lavoratori e collaboratori, operanti all'interno del territorio della Città metropolitana di Bologna, indipendentemente dalla qualificazione dei rapporti di lavoro che si servono per l'esercizio della propria attività lavorativa di una o più piattaforme digitali». F. Martelloni, *Individuale e collettivo: quando i diritti dei lavoratori digitali corrono su due ruote*, in *Lab. law iss.,* 4(1), 2018, 21. C. Lazzari, *Gig economy e tutela della salute e sicurezza sul lavoro. Prime considerazioni a partire dal caso Foodora*, in *Rivista del Diritto della Sicurezza Sociale*, 3, 2018, 455 ss.
Volendo operare un confronto comparatistico è possibile richiamare la *Lei* 10.8.2018 del Portogallo la quale contiene delle previsioni in merito al «*regime jurídico da atividade de transporte individual e remunerado de passageiros em veículos descaracterizados a partir de plataforma eletrónica*».

[13] Risoluzione del Parlamento europeo del 19 .1.2017 su un *Pilastro europeo dei diritti sociali* (2016/2095(INI).

[14] In altri termini la piattaforma possiede la funzione di programmare e indirizzare la consegna grazie all'ausilio dell'algoritmo il quale, a sua volta, è capace di interconnettere i tre punti della rete, che, nel caso della consegna di cibo a domicilio sono: i ristoratori associati alla piattaforma, i consumatori e

mostra tutti i servizi che sono a disposizione dei clienti; una volta che il cliente inoltra l'ordine questo viene inoltrato al ristorante, nel caso in cui si tratti di consegna a domicilio del cibo, che inizia a preparare e confezionare il prodotto; una volta preparato viene adibito al trasporto. L'assegnazione di un ordine a un determinato rider avviene grazie a un calcolo algoritmico: dal punto di vista teorico esso dovrebbe garantire la massima efficienza circa i tempi di attesa per il cliente, in realtà l'algoritmo persegue un altro scopo. Dal calcolo algoritmico, infatti, deriva il diritto di ogni fattorino a ottenere i turni di lavoro o a vedersi assegnate maggiori consegne quando lo stesso risulta essere online; oltre a questo, è sempre l'algoritmo a scegliere con quale grado di priorità chiamare un rider rispetto ad un altro sulla scorta di un punteggio derivante dalle precedenti prestazioni e quindi alla classifica del rider. Nell'ipotesi in cui un rider non dovesse accettare un ordine o dovesse accettarlo non entro un breve lasso temporale[15] si apre un meccanismo di asta: lo stesso ordine viene proposto ad altri fattorini sempre sulla scorta del *ranking*.

È evidente che «l'algoritmo quindi non è altro che un gestore del personale digitale automatizzato, che, attraverso il processo di assegnazione dei turni e delle consegne, controlla la flotta di rider che fa lavorare sul territorio in un dato momento e il valore delle loro paghe, scaricando di fatto su di essi tutto il rischio d'impresa, particolarmente alto questo settore di mercato[16]».

Ulteriore evoluzione è il *crowdworker*[17] in rete ossia la «distribuzione di lavoro su piattaforme *online* che consentono ai clienti di affidare l'esecuzione in *outsourcing* di qualsiasi tipo di compito che possa essere svolto da remoto a una folla (appunto "*crowd*") di lavoratori potenzialmente connessi da ogni parte del mondo[18]» diretto a incrementare l'esternalizzazione dell'intera attività economica che, a sua volta, viene divisa e frammentata in piccole commesse avvalendosi della rete in quanto quest'ultima risulta essere «un mezzo formidabile di segmentazione della catena produttiva, prestandosi all'abbattimento dei rischi imprenditoriali, dei costi e delle obbligazioni nei confronti della forza lavoro[19]». Questo nuovo sistema lavorativo possiede quale caratteristica peculiare quella di divenire una gara rivolta a chiunque si renda disponibile (ad eccezione di alcuni requisiti richiesti come la maggiore età, ad esempio); logica conseguenza di questa impostazione è che «il corrispettivo sarà erogato al solo "vincitore", ciò ancor-

l'ampia rete di *riders* gestiti da un'applicazione alla quale risultano essere connessi. R. Voza, *Nuove sfide per il welfare: la tutela del lavoro nella gig economy*, in *Rivista del Diritto della Sicurezza Sociale*, 4, 2018, 662 ss.

15 Nel momento in cui il rider accetta di effettuare la consegna egli riceve tutte le coordinate sul proprio smartphone riguardanti il luogo dove ritirare il pacco e il luogo dove effettuare la consegna dello stesso.

16 A.J. Avelli, *Diritti per i riders*, in *Lavoro Diritti Europa*, 14 gennaio 2021, 2-3.

17 Esso è stato interpretato quale «forma rinnovata e internazionalizzata» del *putting out system* «caratteristico della fase di protoindustrializzazione, nel corso della quale il costruttore [...] distribuisce gli ordini ricevuti, unitamente al materiale necessario per il compi mento dell'opera, ai lavoratori a domicilio, che riportano i prodotti finiti nei tempi ed alle tariffe concordate». E. Signorini, *Il diritto del lavoro nell'economia digitale*, Torino, 2018, 188.

18 A. Felstiner, *Working the Crowd: Employment and Labour Law in the Crowdsourcing Industry*, in *Berkeley Journal of Employment & Labor Law*, 2011, 143.

19 P. Tullini, *Economia digitale e lavoro* non-standard, in *Labour & Law Issues*, 2(2), 2016, 9.

ché tutti i partecipanti abbiano invero svolto l'intera prestazione commissionata[20]».
Dall'analisi condotta fino a questo momento emerge che utilizzare la piattaforma[21] risulta essere altamente interessante per l'impresa poiché essa, così facendo, può ottenere il cd. fattore lavoro necessario per realizzare il servizio attraverso l'utilizzazione di contratti in cui il prestatore si obbliga a essere disponibile a svolgere la prestazione in modo continuativo[22]. A questo si deve aggiungere che ricorrendo bassi costi di transazione il gestore del servizio possiede un'ampia gamma di possibilità per trovare un sostituto, nonché la circostanza in base alla quale il prestatore possiede un interesse a cogliere le occasioni di lavoro che vengono offerte poiché, qualora rinunciasse, sarebbe inattivo e non potrebbe percepire il compenso[23].
È evidente, quindi, come la quarta rivoluzione industriale abbia determinato delle conseguenze importanti in diversi settori. Per quanto interessa ai fini del presente lavoro l'aspetto che viene in rilievo concerne il nuovo assetto che il mondo del lavoro sta assumendo.
La domanda principale è come il sistema della *gig economy* possa essere definito "costituzionalmente conforme", a quali condizioni e con la previsione di quali tutele.
Per perseguire detto obiettivo si inizierà da un'analisi dell'origine del principio lavorista nella Carta costituzionale italiana per poi approdare alla disamina del rapporto diritto e dovere al lavoro e rivoluzione tecnologica.
L'interrogativo che ci si pone è se questo principio costituzionale, insieme ai suoi corollari, sia effettivamente rispettato dalla presenza sul mercato di piattaforma quali Uber e Foodora.

3. Il principio lavorista

La centralità del principio lavorista è data dal combinato disposto di diverse disposizioni costituzionali, ossia, l'art. 1 - «l'Italia è una repubblica democratica fondata sul lavoro[24]», l'art. 3, c. 2, il quale impegna la Repubblica a rimuovere gli ostacoli che si interpongono tra la realizzazione dell'eguaglianza e la piena partecipazione dei lavoratori alla vita economia e sociale del Paese e l'art. 4 Cost. Quest'ultima disposizione contiene il riconoscimento del diritto al lavoro e attribuisce alla Repubblica il compito di promuovere l'effettività di detto diritto provvedendo a stabilire le condizioni che lo rendano effettivo. Il riferimento al lavoro non si rinviene solamente nelle disposizioni di apertura ma anche all'interno del Titolo III ossia all'interno della «Costituzione economica della Repubblica». Proprio per la peculiare posizione del principio lavorista

[20] W. Däubler, -T. Klebe, Crowdwork*: datore di lavoro in fuga?*, in *Dir. lav. rel. ind.*, 2016, 477.

[21] S. Vallas - J.B. Schor, *What Do Platforms Do? Understanding the Gig Economy*, *in Annual Review of Sociology*, 46, 2020, 273 ss.

[22] A. Gandini, *Labour process theory and the gig economy*, in *Human Relations*, 72(6), 2019, 1039 ss.

[23] M. Novella, *Il rider non è un lavoratore subordinato ma è tutelato come se lo fosse*, cit.

[24] Questa formulazione è stata adottata al fine di utilizzare altre formule, quali «Repubblica democratica dei lavoratori», poiché ritenute troppo classiste o troppo simili a quelle fatte proprie dai regimi collettivisti di stampo sovietico. C. Tripodina, *Il diritto ad un'esistenza libera e dignitosa. Sui fondamenti costituzionali del reddito di cittadinanza*. Torino, 2013, spec. 86-89.

è stato osservato in dottrina che questo derivi dalla volontà dei Padri Costituenti di assicurare l'effettivo riscontro e godimento di questo diritto[25].

Il motivo di questa centralità affonda le proprie radici sul valore che detto diritto e dovere ha assunto, in modo progressivo, nelle società nazionali contemporanee: esso rappresenta un bene primario ed essenziale poiché tramite il lavoro il soggetto acquista gli strumenti necessari per collocarsi all'interno della sfera delle relazioni giuridiche, per definire la propria collocazione sociale e partecipare in maniera effettiva e attiva alle dinamiche sociali.

Volendo esporre un breve excursus storico si nota come il diritto al lavoro, già a partire del XVIII secolo, venne configurato come principio fondamentale non nell'accezione di soddisfacimento di esigenze di solidarietà sociale ma in quello dello Stato di polizia e della libertà di impresa privata, il tutto conformemente allo sviluppo dello Stato liberale di diritto[26]. La successiva evoluzione ha visto l'affermazione dei diritti sociali all'interno dei documenti costituzionali del Novecento e, in particolare, all'interno delle Costituzioni adottate in un momento successivo al secondo dopoguerra nei Paesi europei.

Il diritto al lavoro, all'interno della Costituzione italiana, è percepito in maniera talmente intensa al punto da indurre parte della dottrina a definire il lavoro come il «segno distintivo dello sviluppo della personalità dell'uomo[27]» nonché «il più idoneo ad esprimere il pregio della persona» e a valutare la posizione da attribuire ai cittadini nello Stato poiché non rappresenta soltanto uno strumento per il conseguimento di mezzi di sostentamento ma «il tramite necessario per l'affermazione della personalità[28]». In altri termini il valore di ciascun individuo non deve essere una conseguenza di una posizione di privilegio che si è consolidata in maniera progressiva nel tempo[29] ma del merito acquisito dai soggetti attraverso la propria laboriosità ed intelligenza realizzatasi sia attraverso il lavoro sia attraverso lo studio[30].

Solo i meriti ottenuti attraverso lo studio e il lavoro possono essere gli unici criteri idonei a creare delle differenze tra i cittadini senza che possano rilevare posizioni sociali che non trovano riscontro nell'apporto che ciascuno dovrebbe prestare al progresso materiale e spirituale della società. La formula costituzionale relativa al diritto al lavoro non integra «una prerogativa della classe lavoratrice» bensì deve essere inter-

---

[25] C. Mortati, *Il diritto al lavoro secondo la Costituzione della Repubblica (Natura giuridica, efficacia, garanzie)*, dagli *Atti della Commissione parlamentare di inchiesta sulla disoccupazione*, 1953, ora in *Raccolta di scritti*, vol. III, Milano, 1972, 144.

[26] Nonostante ciò il liberismo sia economico che politico era divenuto insufficiente a causa dell'emersione degli squilibri e del senso di insicurezza sociale che si era venuto a creare. In altri termini si era realizzato «mutamento-adattamento, necessitato e tuttavia 'intelligente'» della forma di Stato alle nuove condizioni». L. Ventura, *Lo Stato sociale,* in L. Ventura - P. Nicosia - A. Morelli - R. Caridà, *Stato e sovranità. Profili essenziali*, Torino, 2010, 112.

[27] P. Barile, *Diritti dell'uomo e libertà fondamentali*, Bologna, 1984, 103.

[28] C. Mortati, *Istituzioni di diritto pubblico*, Padova, 1975, 156-157.

[29] M.S Giannini, *Rilevanza costituzionale del lavoro*, in *Riv. giur. del lavoro*, I, 1-2, 1949, 18.

[30] M. Olivetti, *Art. 1*, in A. Bifulco - M. Celotto - M. Olivetti, (a cura di) *Commentario alla Costituzione*, Torino, 2006, 33 ss.

pretata quale «titolo di appartenenza alla comunità nazionale, alla cittadinanza[31]». Di conseguenza il riferimento al lavoro possiede una centralità antropologica ed egualitaria[32], etica ed economica[33]; «si configura come tratto caratterizzante universalmente la condizione umana, non soltanto in quanto attività lavorativa connessa al bisogno e alla necessità, ma anche in quanto motivo di emancipazione sociale, connesso cioè alla realizzazione dell'obiettivo politico sancito dall'art. 3, c. 2, Cost., vale a dire quello della piena partecipazione dei lavoratori all'organizzazione politica, economica e sociale del Paese, tramite la predisposizione di misure che consentano ai lavoratori il superamento degli ostacoli economici e sociali che si frappongono al loro pieno sviluppo; assume una centralità etica poiché l'adempimento del dovere al lavoro esprime la partecipazione del singolo alla società, alla quale rende ciò che riceve in termini di servizi e di diritti, contribuendo a rafforzare il comune legame sociale, ed una centralità economica in uno Stato sociale interventista che non rinnega l'iniziativa economica privata ma, diffidando delle capacità di autoregolamentazione dei fattori del mercato, impegna le istituzioni nel loro complesso a promuovere le condizioni di effettività di tale diritto, nella prospettiva della piena occupazione[34]».

Conseguenza immediata di detta affermazione è che è la cittadinanza[35] il parametro costituzionale di riferimento per il lavoro e i lavoratori, non il lavoro subordinato. In altri termini parte della dottrina sostiene che se la scelta del Costituente è stata quella di porre il lavoro a fondamento della Repubblica si dovrebbe arrivare a sostenere che l'architettura fornita dalla Costituzione economica formale sarebbe preordinata a garantire l'effettività del principio poc'anzi menzionato al punto da considerare il lavoro subordinato quale valore da affermarsi nello svolgimento dell'indirizzo politico-legislativo derivante dalla stessa Carta costituzionale. Sulla scorta di questo iter logico, quindi, parte della dottrina tradizionale giungerebbe a fornire un maggiore importanza al lavoro dipendente al punto da renderlo un parametro idoneo a condizionare e ricondurre a sé l'interpretazione logica e sistematica del dettato costituzionale[36].

La circostanza in base alla quale il diritto al lavoro è stato inserito all'interno dei principi fondamentali è stata interpretata quale prescrizione avente portata generale e, soprattutto, non limitata ai soli rapporti economici: tramite il lavoro, infatti, si realizza una crasi tra il principio personalistico e quello solidarista caratterizzata, a sua volta, dalla previsione di un diritto/dovere all'esercizio di un'attività lavorativa[37].

Il fatto che il lavoro sia stato posto quale fondamento della Carta costituzionale italia-

31 G. Zagrebelsky, *Fondata sul lavoro. La solitudine dell'art. 1*, Torino 2013, 20-21.

32 M. Luciani, *Radici e conseguenze della scelta costituzionale di fondare la Repubblica democratica sul lavoro*, in *Arg. Dir. lav.*, 3, 2010, 634 ss.

33 L. Carlassare, *Priorità costituzionali e controllo sulla destinazione delle risorse*, in *Costituzionalismo.it*, 1, 2013, 4.

34 V. Pupo, *Il principio lavorista*, in *Forum di Quaderni Costituzionali*, 29 novembre 2013, 7.

35 G. Silvestri, *Il lavoro nella Costituzione italiana*, in Aa. Vv., *Il sindacato e la riforma della Repubblica*, Roma, 1997, 76.

36 C. Mortati, *Art. 1.– Principi Fondamentali artt. 1-12*, in G. Branca (a cura di) *Commentario alla Costituzione* in *Commentario alla Costituzione*, Bologna, 1975, 18.

37 T. Martines, *Diritto pubblico*, Milano, 2009, 441. T. Martines, *Diritto costituzionale*, Milano, 2010, 544-545.

na rappresenta la scelta del Costituente di adottare una norma di principio da declinare in modo coerente con le altre disposizioni costituzionali. Conformemente a questa premessa parte della dottrina è arrivata ad affermare che «non è il lavoro nella sua materialità (o la forza che da essa promana) che fonda la Repubblica, ma è la Repubblica, nella sua Carta costituzionale, che sceglie di porre a suo fondamento il lavoro; in questo significato letteralmente più corretto, il lavoro non è il «fondamento fondante» la forza sociale dalla quale la Repubblica prende origine, (e che in qualche modo fondandola la trascende dinamicamente) ma è la sua norma di principio, accanto a quella democratica, dalla quale, pertanto, dovrebbe derivarne, insieme all'assetto fondamentale della costituzione politica democratica, che si articola nella parte relativa all'ordinamento delle Repubblica, un altrettanto fondamentale assetto della sua costituzione economica formale da ricercarsi, in particolare, nella parte relativa ai diritti e doveri dei cittadini attinenti essenzialmente ai rapporti economici[38]».

Alla centralità conferita al principio lavorista si accompagna una «portata universale» dello stesso idonea ad includere al proprio interno «le diverse forme della '*vita activa*' (il lavoro subordinato, il lavoro autonomo, il lavoro imprenditoriale, ecc.)», mediante le quali «si realizza quella saldatura tra realizzazione individuale e riconoscibilità sociale su cui si gioca la capacità di progresso di una comunità[39]». Da questo rimane escluso il non-lavoro, il parassitismo sociale, la rendita improduttiva, la speculazione finanziaria[40]: nella logica costituzionale il lavoro risulta essere, in prima battuta, l'adempimento di un dovere civico da attuare mediante lo svolgimento di un'attività individuale che possa concorrere al progresso sociale. Si tratta di un dovere relazionale che un cittadino possiede nei confronti degli altri consociati, un dovere al quale deve adempiere alla luce delle possibilità che gli si presentano o che può procurarsi con i mezzi di cui dispone, delle sue propensioni personali sempre però all'interno del limite in cui egli può scegliere in modo concreto ed effettivo[41].

Quanto evidenziato fino a questo momento porta a concludere che la Costituzione, in materia di diritto al lavoro, contiene una specie di nucleo duro che continua a possedere una propria utilità la quale si traduce in un divieto assoluto circa la realizzazione del lavoro prestato in condizioni di dipendenza economico-sociale[42]. Questo monito contenuto nella Carta costituzionale risulta essere rivolto al legislatore, il cui compito è quello di predisporre politiche capaci di arginare le naturali tendenze aggressive del capitale, al sindacato che, in sede di contrattazione collettiva provveda ad estendere ai "nuovi" lavoratori protezioni effettive e concrete ed infine alla giurisdizione in sede di interpretazione. La problematica che emerge concerne la tendenza a rivolgersi al potere giudiziario in modo individuale per ottenere giustizia non adottando forme di

[38] G. Di Gaspare, *Il principio lavoristico nella Costituzione della Repubblica*, in T. Treu (a cura di) *La costituzione economica a 60 anni dalla Costituzione, Astrid-Online*, 2 settembre 2009, 4-5.

[39] R. Nania, *Riflessioni sulla "Costituzione economica" in Italia: il "lavoro" come "fondamento", come "diritto", come "dovere"*, in E. Ghera - A. Pace (a cura di), *L'attualità dei principi fondamentali della Costituzione in materia di lavoro*, Napoli, 2009, 68.

[40] G. Di Gaspare, *Il lavoro quale fondamento della Repubblica*, in *Dir. pubbl.,* 2008, 876 ss.

[41] M. Mazziotti, *Diritto al lavoro*, Milano, 1956, 57 ss.

[42] I. Massa Pinto, *Costituzione e lavoro, totem e tabù*, in *Costituzionalismo.it*, 3, 2012; M. Cavino - I. Massa Pinto, *Costituzione e lavoro oggi*, Bologna, 2013, 41 ss.

organizzazione collettiva[43].

Una parte della dottrina ha sintetizzato in maniera eccellente quanto esposto fino a questo momento sostenendo che «bisogna riconoscere che, a differenza di quanto è accaduto ai costituenti, se l'amore del sindacato per la specie, non gli avesse fatto perdere di vista il genere, i rider ribelli di Foodora oggi, come i *pony-express* ieri, avrebbero potuto placare la loro sete di giustizia attraverso la contrattazione collettiva; un metodo assai più affidabile di una leggina arruffona o della statuizione di un giudice che inforca le lenti d'ingrandimento della Pantera Rosa[44]».

4. Il principio lavorista applicato alla *gig economy*: un ossimoro?

L'automazione ha posto, quale problematica principale da un punto di vista storico, una scissione tra le posizioni che forniscono una interpretazione ottimistica del fenomeno e le posizioni che ne danno una lettura pessimistica a seconda della matrice alla quale si aderisce. Nella versione liberale, ossia quella che fornisce un'interpretazione positiva, l'automazione viene vista come uno strumento per diminuire la fatica dell'essere umano poiché diretta ad agevolarne il lavoro[45]; a contrario, secondo l'impostazione marxista, il macchinario risulta essere utilizzato solamente per produrre ciò che lo stesso filosofo definisce quale plusvalore[46]. Aderendo a questa seconda ricostruzione il progresso tecnologico, quindi, rappresenterebbe un mezzo di oppressione del proletariato e, di conseguenza, preordinato ad accrescere il divario tra il datore di lavoro e il lavoratore.

La problematica appena esposta ha subito un'accelerazione negli anni recenti in quanto si è realizzata una esponenziale crescita di disoccupazione determinata dai nuovi progressi tecnici consistenti nella robotica, nell'applicazione dell'intelligenza artificiale ed infine dal graduale procedimento di informatizzazione all'interno di diversi settori delle società e del mondo del lavoro[47]. Precisamente la preoccupazione di parte della dottrina concerne il cambiamento che i nuovi progressi possono determinare, ossia, «nell'era dell'informatizzazione e di questa "nuova automazione", infatti, il problema non sarà più tanto il fatto che le macchine soppiantino l'uomo nello svolgimento del lavoro manuale ma diventerà, piuttosto, sempre più il fatto che le intelligenze artificiali saranno in grado di soppiantare l'uomo anche nello svolgimento di prestazioni intellettuali[48]».

---

[43] I. Massa Pinto, *La libertà dei fattorini di non lavorare e il silenzio sulla Costituzione: note in margine alla sentenza Foodora (Tribunale di Torino, sent. n. 778 del 2018),* in *Rivista AIC-Osservatorio Costituzionale*, 2, 2018, 1 ss.

[44] U. Romagnoli, *In mezzo al guado del diritto del lavoro*, *Nuovi-Lavori.it*, 15 maggio 2018, 4.

[45] J. S. Mill, *Principles of political economy*, (1848), London, 1920, 99.

[46] K. Marx, *Das Kapital*, (1867-1910), trad. it., *Il capitale*, Torino, 2013, libro I, sez. IV, cap. XIII, par. 1, 502-508.

[47] M. Castells, *The rise of the network society, the information age: Economy, society and culture*, Oxford, 1996; U. Beck, *Schöne neue Arbeitswelt,* Berlino, 1999; A. Papa, *Il diritto dell'informazione e della comunicazione nell'era digitale*, Torino, 2018.

[48] G. Cavaggion, *Il diritto al lavoro nella prospettiva dell'automazione e dell'informatizzazione*, in *Federalismi.it,* 5,

A questo si deve aggiungere che la atomizzazione del lavoro imposta dall'economia digitale pone altresì la trasformazione della questione salariale in una reddituale poiché il rischio è quello di non garantire un adeguato corrispettivo economico qualora non sussista un salario minimo legale[49]. All'interno della macro-categoria del lavoro digitale rientra la fattispecie del lavoro realizzato con il supporto della piattaforma digitale; quest'ultimo pone importanti problematiche connesse con il principio lavorista presente nella nostra Carta costituzionale italiana.

L'aspetto innovativo di questa nuova modalità di esecuzione della prestazione lavorativa concerne il mutamento dell'idea che è alla base del «rapporto che lega la persona alla necessità di procurarsi un reddito capace di garantire un'esistenza libera e dignitosa[50]». È necessario ricordare, infatti, quanto sostenuto dalla Corte costituzionale[51], cioè l'affermazione secondo cui al diritto al lavoro si correla la tutela del lavoratore «in tutte le sue forme e applicazioni» (artt. 4 e 35, c. 1, Cost.): questo impone al legislatore ordinario di apprestare specifiche tutele e protezioni al fine di assicurare la realizzazione all'interno dei luoghi di lavoro «altri diritti fondamentali costituzionalmente garantiti» sulla scorta della considerazione in base alla quale il diritto al lavoro è qualificato come diritto fondamentale. Quest'ultimo aspetto, quindi, ammette l'intervento anche della riflessione costituzionalistica applicata al diritto del lavoro.

Il principio lavorista, il quale rappresenta un aspetto unico nel panorama delle Carte europee e che testimonia quindi l'apporto fornito dalla Costituzione italiana alle tradizioni costituzionali degli altri Paesi appartenenti all'Unione Europea[52], obbliga a prestare una particolare attenzione al coinvolgimento della persona umana quale elemento tipico e connotante le relazioni lavorative[53]; questa particolare attenzione deve essere rivolta non solamente al lavoro subordinato ma a tutte le forme a applicazioni del fenomeno lavoro[54].

In altri termini, partendo dal cuore pulsante di quello che è il principio lavorista nella Carta costituzionale italiana, ossia l'art. 4 Cost. è necessario attuare, e non solo promuovere, tramite strumenti aggiornati ed efficienti, «le condizioni che potranno rendere effettivo il diritto al lavoro in una società satura di AI. Solo con questo impegno, da avviare in tempi rapidissimi, la Repubblica potrà, secondo l'imperativo dell'art. 1 e nel solco del principio lavorista, ritrovarsi fondata su un lavoro che non crei nuove e più profonde discriminazioni, ma si riveli vero motore di mobilità e arricchimento sociale

---

2019, 243.

Si pensi solamente alle ricerche relative all'applicazione dell'intelligenza artificiale all'interno delle professioni artistiche: attualmente vi sono degli algoritmi capaci di realizzare dei dipinti che vengono venduti dalle principali case d'asta. G. Cohn, *AI art at Christie's sells for $432,500*, in *The New York Times*, 25 ottobre 2018.

[49] R. Voza, *Nuove sfide per il welfare: la tutela del lavoro nella gig economy,* cit., 684.

[50] R. Sanlorenzo - G. Armone, *Introduzione. Il valore del lavoro*, in *QG*, 4, 2019, 6.

[51] Corte cost., 26 settembre 2018, n. 194.

[52] C. Pinelli, *"Lavoro" e "progresso" nella Costituzione*, in *Giorn. dir. lav. rel. ind.*, 2009, 401.

[53] R. Sanlorenzo - A. Terzi, *Al centro, il giudice. La Corte costituzionale e il* Jobs Act, in *Questione Giustizia*, 2018.

[54] C. Salazar, *Diritti e algoritmi: la Gig Economy e il "caso Foodora" tra giudici e legislatori*, in *ConsultaOnline*, 1, 2019, 1 ss.

e di realizzazione personale[55]».

Il rischio che si pone dinnanzi al massiccio utilizzo delle nuove tecnologie concerne la scomparsa del concetto di persona nell'analisi delle criticità che queste nuove modalità lavorative pongono. A contrario, nel momento in cui si svolge un ragionamento giuridico, il concetto di persona gioca un ruolo nevralgico: si tratta di una nozione, infatti, che racchiude al proprio interno significati quali libertà, intenzionalità, volontà; si tratta di ambiti strettamente connessi alla vita interiore dei singoli per poi, solo in un secondo momento, venire esteriorizzati. Con l'affermazione della rete, anche e soprattutto all'interno del mondo lavorativo, «l'essere umano, divenuto l'occhio fotografico di sé stesso, si proietta in un continuo narcisismo esibizionistico[56]».

Se il lavoro è stato definito da parte della dottrina come uno dei luoghi nei quali l'uomo può sviluppare la propria personalità nel momento in cui la prestazione lavorativa viene svolta attraverso una piattaforma gestita da un algoritmo si assiste ad una totale assenza della soggettività individuale in quanto l'individuo viene considerato quale mero oggetto funzionale[57] il cui unico compito è quello di eseguire l'ordine che gli viene impartito dalla piattaforma e nel minor tempo possibile. In questo modo il concetto di persona risulta essere indebolito poiché si assiste ad una progressiva affermazione della sostituzione del concetto di individuo con quella di flusso informazionale, di combinazione di dati. Si perviene a quest'ultimo risultato a causa del significato stesso di Internet, ossia, dati, algoritmi e, in base a questi, il campo di informazioni e l'aspetto esistenziale degli utenti risulta essere sostituita da una determinata quantità di dati definita tramite algoritmi[58].

Oltre a questo l'innovazione tecnologica produce anche quale effetto quella che è stata definita come «solitudine digitale» ossia la sostituzione del linguaggio umano con l'uso di concetti matematici al punto da far sopravvivere, quale unico aspetto umano, una mera prestazione economica la quale, a sua volta, viene valutata secondo il parametro rappresentato dal «linguaggio numerico dei prezzi[59]» che, attualmente, si fonda sulla trasmissione e conservazione dei dati.

A questo si deve aggiungere anche la problematica reddituale che il lavoro tramite piattaforma pone: ai sensi dell'art. 35 Cost. i lavoratori vantano il diritto ad un equo e paritario trattamento rapportato alle condizioni di lavoro, alla protezione sociale e alla formazione e questo indipendentemente dalla tipologia e della durata del rapporto di lavoro[60].

Di conseguenza risulta essere assai problematico sostenere che il lavoro tipico della *gig economy* possa essere definito conforme al dettato costituzionale dato che «la progres-

---

55 C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *Biolaw Journal – Rivista di BioDiritto*, Special Issue, 2, 2019, 716; v. anche C. Mortati, *Costituzione dello Stato*, II, *La costituzione italiana*, in *Enciclopedia di diritto*, vol. XI, Milano, 1962, 14.

56 L. Avitabile, *Il diritto davanti all'algoritmo*, in *Rivista Italiana per le Scienze Giuridiche*, 8, 2017, 315.

57 M. Castells, *Comunicazione e potere*, Milano, 2017, 533.

58 D. Cardon, *Che cosa sognano gli algoritmi*, Milano, 2016; P. Domingos, *L'algoritmo definitivo*, Torino, 2016; A. Greenfield, *Tecnologie radicali*, Milano, 2017.

59 B. Romano, *Senso e differenza nomologica*, Roma, 1993

60 Si tratta di un principio richiamato anche dal punto n.15 del Pilastro sociale.

siva trasformazione economica approda ad un concetto di scambio totalmente diversificato rispetto alla sua origine: innesta nell'economia l'idea di profitto derivante dal commercio di dati. Nell'ambito della struttura complessa della rete, la dignità umana è omologata ad unità calcolate, identificate dall'algoritmo. Diventata merce anche la dignità, già declassata a categoria intellettuale, scade in uno svuotamento rispetto alla sua struttura originale ed unica, in un'entità depersonalizzata che si adatta progressivamente agli schemi comportamentali dettati dalla rete[61]».

In altri termini se da sempre l'evoluzione del progresso tecnico-scientifico ha suscitato sentimenti di preoccupazione, interrogativi circa la capacità degli esseri umani di gestirlo nel terzo millennio l'accelerazione di questa evoluzione tecnologica pone attualmente la necessità di riflettere «sull'essenza e sui confini dell'umano[62]».

Proprio queste mutazioni impongono al diritto costituzionale la necessità di riflettere sia per l'impatto che queste novità pongono sia per i contenuti che possono derivare da una riflessione costituzionalistica[63].

In tutto questo è compito del diritto costituzionale divenire concreta applicazione della sua essenza ossia svolgere il compito che l'ha connotato da sempre cioè lottare contro quello che è «il monarca assoluto[64]» tramite una attività incessante di regolamentazione[65].

5. Conclusioni

La riflessione svolta in questi paragrafi ha dimostrato come l'utilizzo e l'applicazione dell'informatica e della tecnica al mondo del lavoro, in assenza di una regolamentazio-

[61] L. Avitabile, *Il diritto davanti all'algoritmo*, cit., 322-323.

[62] T. Groppi, *Alle frontiere dello Stato costituzionale: innovazione tecnologica e intelligenza artificiale*, in *ConsultaOnline*, 3, 2020, 675-676.
R. Bifulco, *Futuro e costituzione. Premesse per uno studio sulla responsabilità delle generazioni venture*, in A. Tarantino - R. Corsano (a cura di), *Diritti umani, biopolitica e globalizzazione*, Milano, 2006, 43; A. Simoncini, *Sovranità e potere nell'era digitale*, in T. E. Frosini - O. Pollicino - E. Apa - M. Bassini (a cura di), *Diritti e libertà in Internet*, Firenze, 2017, 19 ss.

[63] Sicuramente la riflessione risulta essere presente in dottrina, basti pensare all'attività di ricerca svolta da diversi costituzionalisti ma, allo stesso tempo, risulta essere in pericolo la stessa forma di Stato costituzionale o Stato democratico pluralista. B. Caravita, *Principi costituzionali e intelligenza artificiale*, in U. Ruffolo (a cura di), *Intelligenza artificiale.Il diritto, i diritti, l'etica,* Milano, 2020, 451-453; T. E. Frosini*, Liberté, Égalité, Internet,* Napoli*,* 2020; C. Casonato, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE*, 3, 2020, 3369 ss.; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal, Rivista di BioDiritto*, 1, 2019, 63 ss.
A tal proposito è stato sostenuto in dottrina che ci si trova dinnanzi ad una nuova forma di potere di sovrano che pone al diritto costituzionale una sfida del tutto nuova poiché esso è chiamato, in primo luogo, a comprendere il fenomeno per poi, successivamente, elaborare nuove forme e strumenti efficaci per gestirlo. A. Simoncini, *Sovranità e potere nell'era digitale,* cit., 20; T. Groppi, *Menopeggio. La democrazia costituzionale nel XXI secolo*, Bologna, 2020.

[64] C. Casonato, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal, Rivista di BioDiritto*, 1, 2019, 178; M. Barberis, *Populismo digitale. Come Internet sta uccidendo la democrazia*, Milano, 2020, spec. 184-186.

[65] A contrario vi è chi sostiene che sia necessario lasciare che Internet si sviluppi come se fosse un diritto spontaneo: T.E. Frosini, *Il costituzionalismo nella società tecnologica*, in *Diritto dell'informatica*, 4, 2020, 483.

ne della stessa, determini un'elusione del dettato costituzionale in materia di diritto del lavoro.

La gestione della prestazione lavorativa da parte di una piattaforma digitale e, quindi, di un algoritmo, determina l'insorgenza di minacce ai diritti fondamentali da parte di queste nuove tecnologie al punto da indurre la riflessione costituzionalistica ad interessarsi del fenomeno sulla scorta dell'affermazione contenuta nell'art. 1 Cost. secondo cui «l'Italia è una Repubblica democratica fondata sul lavoro».

La realizzazione di un mercato del lavoro globale dominato dalla *gig economy* importa una continua ed incessante competizione diretta al ribasso del costo della prestazione lavorativa al punto da indurre i prestatori di lavoro ad accettare la retribuzione più esigua senza possedere nemmeno la garanzia di ottenerla. Vi è il rischio, infatti, che il committente possa "assumere" più di un lavoratore per scegliere, alla fine, colui che riesce a concludere per primo la prestazione richiesta[66].

Il binomio rappresentato dalla sconfinatezza della Rete e la sua potenzialità di creare e riprodurre le dinamiche all'interno del cyberspazio[67] in assenza di una regolamentazione specifica rende possibile una totale deresponsabilizzazione in relazione alla dinamica tra il richiedente e l'esecutore della prestazione.

Per questo motivo è necessario e forse urgente costruire quello che è stato definito un «costituzionalismo tecnologico[68]» al quale affiancare l'attività legislativa chiamata a decidere sull'impiego e sullo sviluppo delle nuove tecnologie in costante dialogo con tecnici e scienziati al fine di individuare il necessario bilanciamento tra i principi fondamentali e le spinte tecnocratiche[69].

Una possibile conciliazione tra il lavoro tramite piattaforme e i principi costituzionali impone di adottare quale strategia quella «del "reddito dignitoso a prescindere", che significa rinviare a politiche pubbliche di contrasto al fenomeno dei *working poors*[70]». Questo significherebbe dare attuazione alla direttiva europea relativa alle condizioni di lavoro trasparenti e prevedibili grazie al richiamo presente nella stessa dei «lavoratori tramite piattaforma digitale[71]».

Al di là delle possibili soluzioni astrattamente applicabili si ritiene che sia necessario in primo luogo riconoscere e in secondo luogo attuare il nocciolo duro dei diritti previsti dalla Costituzione non solamente ai cd. lavoratori digitali ma anche a coloro i quali vengono definiti come lavoratori vulnerabili e, di conseguenza, risulta essere doverosa la concreta applicazione della direttiva (UE) 2019/1152.

---

66 V. Cagnin, GIG-Economy *e la questione qualificatoria dei* gig-workers: *uno sguardo oltre confine*, in A. Perulli (a cura di), *Lavoro autonomo e capitalismo delle piattaforme*, Padova, 2018, 41.

67 Esso è stato definito come «lo spazio telematico che si distende intorno alla Terra come un sopramondo». N. Irti, *Norma e luoghi*, Roma-Bari 2006, 61.

68 C. Salazar, *Diritti e algoritmi: la Gig Economy e il "caso Foodora" tra giudici e legislatori,* cit.*,* 14.

69 P. Costanzo, *Il fattore tecnologico e le trasformazioni del costituzionalismo*, in Aa. Vv., *Annuario 2012. Costituzionalismo e globalizzazione*, a cura dell'AIC, Napoli, 2014, 81.

70 B. Caruso, *Il lavoro digitale tramite piattaforma: profili giuridici e di relazioni industriali. I lavoratori digitali nelle prospettive del Pilastro sociale europeo: tutele rimediali legali, giurisprudenziali e contrattuali*, in *Diritto delle Relazioni Industriali*, 4, 2019, 15.

71 Considerando 8 della direttiva (UE) 2019/1152 del Parlamento europeo e del Consiglio del 20 giugno 2019.

A questo si aggiunge il rispetto necessario ed imprescindibile del principio cardine del rispetto della dignità della persona umana[72] a prescindere dalla tipologia e dalla qualificazione del rapporto di lavoro garantendo un corrispettivo proporzionato alla quantità e qualità di lavoro nonché sufficiente a cui si deve aggiungere la previsione di un sistema di sicurezza sociale nei confronti di colui che ha perso il posto di lavoro[73].
La modalità tramite la quale applicare questo sistema complesso di diritti e tutele ai lavoratori della *gig economy* rappresenta un aspetto cruciale nel momento in cui si pone l'interrogativo circa la possibile estensione delle precedenti e già applicate tutele oppure se sia necessario predisporne di nuove, maggiormente avanzate e fondate su criteri di accesso e distribuzione differenti[74]. Posta la peculiarità e l'eterogeneità delle prestazioni che vengono e che possono essere ascritte al mondo della *gig economy* sarebbe necessario che l'intervento legislativo si concretizzasse in un modello sganciato dalla dicotomia subordinazione/autonomia a favore di un modello «olistico e maggiormente articolato di protezione sociale, organizzata per gradazioni crescenti[75]».
Le protezioni speciali dei lavoratori delle piattaforme oltre a comprendere le tutele già previste dalla normativa in materia di prestazioni occasionali accessorie dovrebbe altresì possedere una disciplina speciale concernente, ad esempio, la fissazione di un massimo margine di guadagno della piattaforma sulla prestazione resa dal lavoratore, un sistema di trasparenza per quanto attiene al sistema di valutazione della prestazione al quale aggiungere il diritto al contraddittorio del lavoratore che avesse ricevuto una valutazione negativa[76], il diritto alla disconnessione[77], nonché specifiche garanzie di procedimento da seguire nell'ipotesi di esclusione del lavoratore della piattaforma.

---

[72] R. Scognamiglio, *voce Lavoro I) Disciplina costituzionale*, in *EGT*, 1990, XVIII, 4.
Si rammenta altresì che l'art. 41, c. 2, Cost. afferma che l'iniziativa economica privata non possa svolgersi in contrasto con l'utilità sociale e in maniera tale da non recare un danno alla sicurezza, alla libertà e alla dignità umana. Questi parametri devono essere interpretati quali limiti esterni e non funzionali all'impresa e necessitanti della mediazione del legislatore.

[73] G. Santoro-Passarelli, *Trasformazioni socio-economiche e nuove frontiere del diritto del lavoro. Civiltà giuridica e trasformazioni sociali nel diritto del lavoro*, in *Diritto delle Relazioni Industriali*, 2, 2019, 417 ss.

[74] V. De Stefano, *Lavoro «su piattaforma» e lavoro non standard in prospettiva internazionale e comparata*, in *Rivista Giuridica del Lavoro e della Previdenza Sociale*, 2017, 251 ss.

[75] S. Ciucciovino, *Analisi e proposte sul diritto del lavoro nel tempo di Industria 4.0. Le nuove questioni di regolamentazione del lavoro nell'industria 4.0 e nella gig economy: un problem framework per la riflessione*, in *Diritto delle Relazioni Industriali*, 4, 2018, 1049.

[76] E. Dagnino, *Il lavoro nella "on-demand economy": esigenze di tutela e prospettive regolatorie* , in *Labour & Law Issues*, 2, 2015, 25-27.

[77] D. Poletti, *Il c.d. diritto alla disconnessione nel contesto dei «diritti digitali»,* in *Responsabilità Civile e Previdenza,* 1, 2017, 8-12; R. Zucaro, *Il diritto alla disconnessione tra interesse collettivo e individuale. Possibili profili di tutela,* in *Labour & Law Issues*, 5(2), 2019, 216 ss.

Note a sentenza

The CJEU's take on unauthorized framing of online content: (only) if technologically precluded, then prohibited

Giulia Priora

Court of Justice of the European Union, 9 March 2021, Case C-392/19, *VG Bild-Kunst v Stiftung Preußischer Kulturbesitz (VG Bild-Kunst)*

Following several decisions on the interpretation of the right of communication to the public in the digital environment, the CJEU clarified that embedding a protected work in a website constitutes a copyright violation if it circumvents effective technological protection measures. The systematic and practical significance of the judgement in Case C-392/19, *VG Bild-Kunst* promises to bring legal certainty into the realm of online uses of creative content and its constant and future evolution.

Table of contents

1. Introduction. – 2. Facts. – 3. Legal context. – 3. Analysis. – 4. Practical significance. – 5. Conclusion.

Keywords

copyright - Court of Justice - communication to the public – linking - framing

1. Introduction

In a recent popular interview, the Duchess of Sussex expressed her idea of privacy by giving an example: exhibiting a picture of someone's own child at the workplace or on social media – she argued – does not authorize co-workers or anyone else to access the whole photo gallery of family pictures.[1] Murmurs of appreciation have spread among privacy lawyers, who are ever busier showcasing the boundaries set by the fundamental protection of personal data, private and family life in the online environment. One may presume that copyright scholars were not equally satisfied with the example. The evolution of the discipline over the past two decades has mostly revolved around online uses of protected materials, thus emphasizing the question: what can Internet users do with the pictures that are made available to them?

[1] For a partial transcript of the interview, see C. Fernandez, *Meghan Markle says her family has a 'basic right to privacy'*, in *Insider*, 9 March 2021.

In broad brush, the dispute at stake in Case C-392/19 *VG Bild-Kunst*[2] places itself within the contours of this fundamental query. The decision issued by the Court of Justice of the European Union (CJEU) represents a milestone in the interpretation of EU copyright rules, which puts some order into the fluid and often problematic notion of communication to the public in the online environment.

2. Facts

The controversy arose between a cultural heritage institution and a collecting society, both based and operating in Germany. The dispute concerns the use of digitized pictures of artworks in the form of thumbnails. The Stiftung Preußischer Kulturbesitz (SPK) is a cultural heritage foundation, which runs the German Digital Library (DDB), a nation-wide project connecting cultural institutions to display and promote their digital collections on a single website. More precisely, the DDB shows thumbnail pictures of the artworks (reaching a maximum size of 800x600 pixels) and direct links to the original websites where the works were first made available online by the respective cultural institutions. VG Bild-Kunst is a collecting society managing copyrights over works of visual art, among which numerous works included in the DDB digital offer.

SPK sought permission from VG Bild-Kunst to use thumbnail pictures of the works included in its managed repertoire on the DDB website. VG Bild-Kunst showed willingness to conclude a license agreement, however under the condition that SPK implemented effective technological protection measures (TPMs) to prevent the framing of the thumbnail pictures by third parties on other websites. The *framing* (or inline linking) technique consists of embedding a work, which is accessible on one website, in another webpage. As a result, Internet users can access it independently from the original site where the content was first made available. This feature marks a fundamental difference between framing and *hyperlinking*, as the latter merely provides clickable links, which redirect the user to the original source of the published content.[3] SPK holds that the deployment of TPMs on the DDB website would not only entail considerable costs, but also potentially be in contrast with the intention of many artists in favor of having their works displayed and framed over the web.[4] In this light, SPK challenged the reasonable nature of the contractual clause advanced by VG Bild-Kunst and sought judicial enforcement of its obligation to grant the license without imposing the implementation of TPMs.

[2] Case C-392/19, *VG Bild-Kunst v Stiftung Preußischer Kulturbesitz (VG Bild-Kunst)* (2021).

[3] A distinction that seemingly inspired Advocate General (AG) Szpunar, who in his Opinion theorized a different legal approach towards "clickable links" and "automatic non-clickable links". See *VG Bild-Kunst,* AG Opinion, § 98.

[4] See DDB, *Test Case German Digital Library vs VG Bild Kunst Press Release*, 10 March 2021.

3. Legal context

The dispute pivots on three mandatory provisions of EU copyright law: Art. 3 InfoSoc Directive, which harmonizes the exclusive right of communication to the public; Art. 6(1) InfoSoc Directive, which enjoins Member States to introduce provisions against the circumvention of effective TPMs implemented by right holders to prevent or restrict access or use of works; and Art. 16 CRM Directive, which introduces the obligation for collecting societies and end-users to conduct licensing negotiations in good faith, based on objective and non-discriminatory criteria.[5]

The claim advanced by SPK was dismissed before the Court of first instance, and then upheld by the Court of Appeal. VG Bild-Kunst brought an appeal before the German Federal Supreme Court, which referred the case to the CJEU arguing that, according to relevant national case law, collecting societies can exceptionally refuse to grant a license if there is an objectively legitimate reason to do so. If the licensed use would enable the perpetuation of a copyright violation by third parties, this would represent a legitimate reason not to proceed with the authorization.

The leading question of the case thus becomes whether the framing of a picture, which is available online and on which the right holder has implemented effective TPMs, in a third-party website constitutes an act of communication to the public ex Art. 3 InfoSoc Directive. Even though reckoning with the fact that an answer in the negative would lead to a de facto exhaustion of the right of communication to the public, and thus should be avoided, the German Supreme Court decided to refer the question to the CJEU considering its existing case law on linking practices and their role in the protection of freedom of expression and information online.[6]

4. Analysis

As highlighted by Synodinou and Rosati,[7] the CJEU has been particularly creative in recollecting prior decisions on the right of communication to the public online. Its consolidated interpretation foresees that the copyright owner's authorization is required for acts that (i) amount to a communication by the user, and (ii) are addressed to a "new" public, that is a fairly large number of people who had not been addressed by the first publication of the work by the right holder.[8] Whereas the Court consist-

[5] These provisions find transposition into the German copyright legal system in Section 19a German Copyright Act, protecting the exclusive right of making available to the public, and Section 34(1) Act on the Management of Copyright and Related Rights by Collecting Societies, which sets an obligation to collecting societies to grant a reasonable license to any user requesting to use a work.

[6] See also *VG Kunst-Bild*, AG Opinion, § 54, where AG Szpunar highlighted how the linking to unauthorized content needs to be permitted to preserve the smooth functioning of the Internet and safeguard users' fundamental rights.

[7] T. Synodinou, *'Framing' the right of communication to the public: the CJEU's decision on the VG Kunst case*, in *Kluwer Copyright Blog*, 15 March 2021; E. Rosati, *CJEU rules that linking can be restricted by contract, though only by using effective technological measures*, in *The IPKat*, 9 March 2021.

[8] See e.g., Case C-466/12, *Nils Svensson and Others v Retriever Sverige AB* (2014) (*Svensson*), § 24; Case

ently holds linking practices to amount to acts of communication,[9] the interpretation of the notion of new public remains more controversial.

The existing case law outlines a spectrum of digital uses of content available online, which the CJEU already reviewed to assert whether the user addresses a different or, rather, the same audience that the right holder wanted to reach in the first place. The spectrum ranges from the act of *posting* a work on another website, which is deemed by the Court a fully-fledged communication to a new public,[10] to the practice of *hyperlinking*, which instead fails to reach a different audience and hence does not require authorization.[11] In *VG Bild-Kunst*, the CJEU's reasoning tackles the practice of *framing*, which represents a middle ground between the two digital uses mentioned above.

The Court argues that the framing in one's own website of someone else's work that is already and lawfully available online is an act of communication, but not to a new public.[12] However, this applies only if the work was made available by the right holder without implementing TPMs, thus addressing from the outset all Internet users.[13] Conversely, the deployment of TPMs by the copyright owner signals his/her manifest intent to restrict access to the work to a certain public.[14] Framing the work in another website by circumventing such restrictions would make it available to a broader Internet audience, thus requires specific authorization.[15]

Even though without particular emphasis on the notion of fair balance of rights and interests, the decision highlights the need to protect both right holders and Internet users. On the one hand, the Court stresses that copyright owners shall be able to decide on each online use of their works and limit access to them by way of contractual restrictions, should they wish so at any point in time.[16] On the other hand, it is

C-348/13, *BestWater International GmbH v Michael Mebes and Stefan Potsch* (2014) (*BestWater*), § 14; Case C-161/17, *Land Nordrhein-Westfalen v Dirk Renckhoff* (2018) (*Renckhoff*), § 19; *VG Bild-Kunst*, § 32. Specific subjective requirements have been, at times, added in the construing of Art. 3 InfoSoc Directive, such as the for-profit commercial purpose of the user, and his/her awareness of the lawful nature of the content used. See Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others* (2016) (*GS Media*), §§ 35-38.

[9] See *VG Kunst-Bild*, AG Opinion, § 51. Interestingly, this view was contested by AG Whatelet vis-à-vis hyperlinking in *GS Media*, AG Opinion, § 60 («I consider that hyperlinks posted on a website which direct to works protected by copyright that are freely accessible on another website cannot be classified as an 'act of communication' (…) since the intervention of the operator of the website which posts the hyperlink (…) is not indispensable to the making available of the photographs in question to users (…)»).

[10] *Renckhoff*, cit., § 35.

[11] *GS Media*, cit., § 42.

[12] *VG Kunst-Bild*, cit., § 36.

[13] Ivi, §§ 37-38 with reference to *Svensson*, cit., *BestWater*, cit., and Case C-301/15, *Marc Soulier and Sara Doke v Premier ministre and Ministre de la Culture et de la Communication* (2016) (*Soulier*), all cases regarding uses of works that were freely available online without TPMs implemented.

[14] *VG Kunst-Bild*, cit., §§ 44-45.

[15] Ivi, §§ 39-40.

[16] According to E. Rosati, *CJEU rules that linking can be restricted by contract, though only by using effective technological measures,* cit., this interpretation has been implicitly part of the Court's interpretation since *Svensson*.

important that end-users can clearly ascertain the intentions of the right holder, thus leading the CJEU to assert that the *only* way right holders can prohibit framing is by way of effective TPMs.[17]

5. Systematic and practical significance of the decision

By clarifying that the framing of pictures that are protected by TPMs amounts to an act of communication to the public, the CJEU's decision in *VG Bild-Kunst* not only entails a considerable practical impact over online uses of creative content, but also adds systematic consistency to the existing case law. In particular, it touches upon three core aspects of EU copyright law: the high level of protection of right holders, legal certainty, and the notion of new public.

5.1. The protection of right holders online

As it glaringly emerged in the *Renckhoff* decision,[18] the main driver of the Court's reasoning is the will to effectively ensure the right holder's control over the work online. In this vein, the CJEU consolidates the centrality of the exclusive right of communication to the public as a key prerogative to retain control over digital works.[19] The interpretation of such right, which is preventive in nature and inexhaustible,[20] shall be broad and align with the pursued objective of protection of right holders.[21]
Interestingly, the CJEU departs from prior judgments in the choice of wording: instead of insisting on the notion of high level of protection of *right holders*, it emphasizes the need to safeguard *authors*, embracing a markedly economic rationale and stressing the need to enable them to get appropriate reward from their works.[22] No reference is made to any broader justifications relating, for instance, to the protection of the author's reputation.[23]

---

[17] *VG Kunst-Bild*, cit., § 46.

[18] *Renckhoff*, cit., §§ 30-35.

[19] See also T. Synodinou, *'Framing' the right of communication to the public: the CJEU's decision on the VG Kunst case,* cit. («by omitting any assessment of the possible cumulative application of the right of reproduction, the CJEU seems to indirectly affirm the all-encompassing character of the right of communication as the dominant legal prerogative of controlling access to digital content»).

[20] Art. 3(3) InfoSoc Directive. See also e.g., *VG Bild-Kunst*, cit., § 21, § 28; *VG Bild-Kunst,* AG Opinion, § 57.

[21] E.g., recitals 4 and 23 InfoSoc Directive; *Renckhoff*, cit., §§ 18, 29; *VG Bild-Kunst*, §§ 26, 50-53.

[22] *VG Bild-Kunst*, cit., § 27 («the principal objective of that [InfoSoc] directive is to establish a high level of protection of authors, allowing them to obtain an appropriate reward for the use of their work, including when a communication to the public takes place»).

[23] See Case C-201/13, *Johan Deckmyn and Vrijheidsfonds VZW v Helena Vandersteen and Others* (2014) (*Deckmyn*), §§ 30-31. See also S. Dusollier, *Realigning Economic Rights with Exploitation of Works: The Control of Authors over the Circulation of Works in the Public Sphere* in B.P. Hugenholtz (ed.), *Copyright Reconstructued: Rethinking Copyright's Economic Rights in a Time of Highly Dynamic Technological and Economic Change,* Alphen aan den Rijn, 2018, 163 ss.

However, the exclusive rights granted by copyright law are not limitless. The Court evokes only once the notion of fair balance to emphasize how the circumvention of TPMs would determine a disequilibrium in favor of end-users.[24] What remains unexplored are the boundaries of copyright protection – i.e., its limited duration, subject matter, and scope – and the potential abuses or misuses of rights by copyright owners. *VG Bild-Kunst* seems to encourage those who want to retain control over their works online to deploy TPMs. Yet, questions related to the risk of capture effect by such measures that may prevent the framing of works belonging to the public domain and fail to effectively protect copyright exceptions and limitations remain unaddressed.[25]

5.2. Legal certainty and TPMs

The prohibition of circumventing TPMs represents the gist of the decision. TPMs represent, on the one side, the right holder's manifest expression to retain control over any communication to the public, and, on the other side, the possibility to showcase his/her authorization to frame the work in other websites. In fact, in light of the *VG Bild-Kunst* decision, the absence of TPMs corresponds to either a presumption of the right holder's consent to authorize the framing of the work or, at least, a lawful basis for third parties to do so.[26]

This prompts the question: why TPMs? The factual background of the case leads the CJEU to assess that private contractual clauses, mostly hidden from Internet users, could not be effective in restricting access and use of a work online. According to the Court, *only* TPMs can guarantee legal certainty in the digital environment and the smooth functioning of the Internet. This has three main implications.

First, the implementation of effective TPMs as a technical pre-condition to copyright protection could be considered to amount to a formality, thus being incompatible with Art. 5(2) Berne Convention.[27] Second, the CJEU seems to suggest that any implicit or tacit intention by the copyright holder to prohibit framing is to be deemed insufficient. However, drawing the conclusion that only TPMs can effectively showcase the right holder's intent, the CJEU overlooks other forms of explicit contractual restrictions, such as written indications by the right holder clearly displayed on the work (e.g., "all rights reserved", "confidential do not use or disseminate without author's

[24] *VG Bild-Kunst*, cit., § 54.

[25] On the point see also P. Mézei-B.J. Jütte, *CJEU clarifies that framing infringes copyright it TPMs are circumvented*, forthcoming in *JIPLP* («It will be especially interesting to see how potential preventive framing-blockers will interact with copyright exceptions, which Article 6(4) InfoSoc Directive already anticipates»); E. Rosati, *CJEU rules that linking can be restricted by contract, though only by using effective technological measures,* cit. («Article 4 of the DSM Directive allows rightholders to reserve the doing of text and data mining activities in relation to their content. The *VG Bild-Kunst* judgment may serve to clarify further, beyond the language of that directive, how such reservation is to be done»).

[26] See T. Synodinou, *'Framing' the right of communication to the public: the CJEU's decision on the VG Kunst case,* cit. («It is noteworthy that this approach appears to implicitly confirm a trend towards the recognition of the absence of technological restrictions on access to online content as a basis for lawful access»).

[27] See also E. Rosati, *CJEU rules that linking can be restricted by contract, though only by using effective technological measures,* cit.

consent") or explicit references to licensing terms (e.g., Creative Commons licenses). Third and last, not to underestimate is the strong reliance on a purely technological element (the TPMs), which is de facto considered a normative component in the digital copyright scenario, namely a feature that regulates Internet users' behaviors. This approach has to do with a peculiar understanding of EU copyright rules that is on the rise in the recent CJEU case law, which accounts for legal as well as technological rules governing the Internet, giving shape to a composite idea of legality.[28]

5.3. The partitioning of the Internet public

The *VG Bild-Kunst* decision has the great virtue of settling the controversial interpretation of the notion of "new public" vis-à-vis acts of communication online. Avoiding excessive technicisms, the CJEU rejects the differentiation suggested by AG Szpunar between clickable and unclickable links,[29] preferring an all-encompassing approach for all linking practices.

The Court clarifies that, as long as a work is lawfully and freely available online, the presumption is that the right holder meant to reach all Internet users.[30] However, the presence of a "new" public – and hence the need to seek specific authorization – emerges along with one of the following conditions: (i) the lack of authorization to first publication,[31] (ii) the implementation of TPMs,[32] or (iii) the "disconnection" between the page where the work is originally hosted (e.g., via posting).[33]

Despite the attempt to give a comprehensive and consistent interpretation of Art. 3 InfoSoc Directive, on a practical note the take of the Court results quite neatly differentiated between hyperlinking, framing, and posting practices. Worth noting is the fact that in the eyes of the CJEU the framing of works circumventing TPMs more closely resembles posting,[34] while, if TPMs are absent, it seems to correspond to an act of hyperlinking.[35] This confirms that the right holder's power to effectively retain control

[28] See G. Priora, *Dall'armonizzazione all'interlegalità: la tutela dell'utente finale nella disciplina europea del diritto d'autore*, in E. Chiti-A. Di Martino-G. Palombella (eds.), *L'età dell'interlegalità,* forthcoming.

[29] *VG Bild-Kunst*, AG Opinion, § 98.

[30] By doing so, it appeases diverging interpretations based on the view that the online publication of a work addresses only in theory all Internet users, but in practice – due to the vastness of the Internet – reaches a specific segment of audience. See e.g., *VG Bild-Kunst*, AG Opinion, §§ 56, 84.

[31] *GS Media*, cit., § 41.

[32] *VG Bild-Kunst*, cit., § 43.

[33] *Renckhoff*, cit., § 30.

[34] *VG Bild-Kust*, cit., § 47 drawing an analogy with *Renckhoff*, cit. § 35 («In such circumstances (…) the public which was taken into consideration by the copyright holder when he or she authorised the communication of his or her work on the website on which that work was initially published consists solely of the users of that site, and not the users of the website on which the work has been subsequently framed without the authorisation of the copyright holder, nor other internet users»).

[35] Fully rolling out its reasoning, one could have expected the Court to draw an analogy also with *GS Media*, asserting that the public addressed by the right holder who did not implement TPMs and the user framing his/her work was the same audience. See *GS Media*, cit., § 42 («as soon as and as long as that work is freely available on the website to which the hyperlink allows access, it must be considered

over the work is the most decisive element in the reasoning.

5. Conclusion

The CJEU's interpretation in *VG Bild-Kunst* shows several points of strengths and a valuable potential in providing consistency in the Court's interpretation of the right of communication to the public online. Protecting TPMs and the right holder's intention when sharing a work is not only a sound exegesis of EU copyright law, but also a conscious outcome in today's everyday life. Suffice to think of the materials we make available on a daily basis to work colleagues, students, and friends, using TPMs to allocate different privileges of access and use. However, among the aspects that remain unaddressed, the most impelling question seems to be the effective protection of copyright exceptions and limitations in view of a growing TPM-based model of digital cultural consumption.

The case is now pending before the German Federal Supreme Court, who will decide in the merits. Bound by the CJEU's interpretation, one may expect the national Court to embrace a broad understanding of Art. 3 InfoSoc Directive and deem the request for the implementation of TPMs by VG Bild-Kunst to be legitimate. However, it cannot be excluded that the German judges will take the opportunity to give additional insights on aspects that were left uncovered, such as the potential clashes of intention to implement TPMs between individual authors and the collecting society,[36] the relevance of the notion of fair balance of rights in the teleological balancing exercise between copyright protection and access to culture, the qualification of the publication of thumbnail pictures as an act of communication to the public,[37] or even the opportunity to seek a license agreement between SPK and VG Bild-Kunst if the pictures DDB wishes to display were made available in the first place with the consent of the right holders and without effective TPMs.

that, where the copyright holders of that work have consented to such a communication, they have included all internet users as the public»).

[36] See the claimant's remarks on its press release, stating that «DDB and its digital offer are expressly welcomed by a large number of authors. A distinction will therefore have to be drawn between the individual rights holder who wants his works to be made available to the public "with reservations" on the one hand, and a CMO that demands the blanket implementation of technical measures for all the authors and artists it represents on the other hand. For, according to DDB's perception, the opinion among authors is not so unanimous»: DDB, *Test Case German Digital Library vs VG Bild Kunst Press Release,* cit.

[37] Even though none of the parties seems to have included this legal question in the proceedings. On the point, the CJEU asserts that the alteration of size or quality should not affect the assessment as long as the work is perceptible (*VG Bild-Kunst*, cit., § 25); however, German copyright law explicitly relies on the small-scale size of works to carve out room for copyright exceptions and limitations. See Section 60a(2) German Copyright Act.

La responsabilità del gestore del sito per i contenuti pubblicati da soggetti terzi

Silvia Vimercati

Corte di Cassazione, sez. V penale, 12 gennaio 2021, n. 7220

Il gestore di un sito Internet non risponde del reato di omesso controllo di cui all'art. 57 c.p., ma, qualora sussistano elementi che denotino una compartecipazione dello stesso alla condotta offensiva posta in essere da un soggetto terzo, può rispondere a titolo di concorso nel reato di diffamazione aggravata.

Sommario

1. Il principio. – 2. La vicenda. – 3. La motivazione della Cassazione. – 4. Il concorso nel reato di diffamazione del gestore del sito.

Keywords

responsabilità – Internet – diffamazione – concorso - blogger.

1. Il principio

La Corte di Cassazione è tornata a occuparsi della responsabilità dei gestori di siti Internet per gli scritti pubblicati da soggetti terzi, affrontando l'interrogativo, ancora aperto, circa la possibilità e le condizioni in presenza delle quali possano rispondere penalmente dei contributi creati dagli utenti e ospitati nella pagina da loro diretta.
Con la sentenza che si annota, la quinta sezione penale della Corte di Cassazione, in linea con alcuni propri precedenti giurisprudenziali, ha confermato che i titolari di siti web, da una parte, non possono essere chiamati a rispondere del reato di cui all'art. 57 c.p., ma, dall'altra, a certe condizioni possono rispondere a titolo di concorso in diffamazione aggravata con l'utente che ha diffuso il contributo offensivo, se ne condividono il contenuto e non provvedono tempestivamente alla sua cancellazione.

2. La vicenda

Dato conto del principio di diritto espresso dalla Corte, pare opportuno soffermarsi sul caso concreto che ha originato la decisione.
Per quanto si riesce a comprendere dalla sintesi dei fatti offerta in motivazione, un

utente pubblicava sul sito Internet di cui era titolare l'imputata un articolo offensivo nei confronti di un agente di polizia. Più precisamente, lo apostrofava come "criminale in divisa" e "mela marcia", nonostante fosse stato assolto nel procedimento penale celebrato nei suoi confronti. La titolare del sito – a quanto pare – non solo non si sarebbe attivata per rimuovere il contenuto diffamatorio, ma avrebbe partecipato alla raccolta delle informazioni per la redazione dello scritto e ne avrebbe condiviso il contenuto.
La Corte d'appello, confermando la decisione di prime cure, condannava il gestore del sito per concorso nel reato di diffamazione aggravata a mezzo Internet.
La tesi della ricorrente, che chiedeva l'annullamento della sentenza, si basava su due argomenti. Da una parte, rilevava come la Corte avrebbe modificato l'originaria imputazione per averla ritenuta responsabile non per la pubblicazione, ma per la mancata rimozione e così ipotizzando una responsabilità ai sensi dell'art. 40 c.p.; e, dall'altra, avrebbe fondato la propria decisione su precedenti della giurisprudenza di legittimità in cui si attribuisce al titolare del sito la responsabilità di quanto pubblicato da terzi solo quando vi sia prova dell'effettivo concorso nella pubblicazione, quando viceversa nel dibattimento del caso in esame sarebbe emersa l'inesistenza di un effettivo controllo da parte della stessa sui contenuti inseriti dagli utenti.
La Corte di Cassazione rigettava il ricorso e decideva come anticipato.

3. La motivazione della Cassazione.

Ripercorriamo ora il percorso motivazionale che ha condotto la Corte ad attribuire una responsabilità a titolo di concorso in capo al gestore del sito per un contributo immesso da un terzo.
Per giungere a tale approdo, la Cassazione anzitutto richiama alcuni suoi precedenti in materia.
In primo luogo, menziona una prima decisione del 2018[1] che escludeva la configurabilità a carico del titolare di un sito della responsabilità per omesso controllo di cui all'art. 57 c.p. in quanto «tale norma è applicabile alle sole testate giornalistiche telematiche e non anche ai diversi mezzi informatici di manifestazione del pensiero (forum, blog, newsletter, newsgroup, mailing list, facebook)».
La seconda pronuncia citata del 2019[2], oltre a confermare l'inapplicabilità della responsabilità per *culpa in vigilando ex* art. 57 c.p., stabiliva che il gestore di un blog può rispondere a titolo di concorso per il contenuto offensivo pubblicato da un terzo se, venutone a conoscenza, ometta di rimuoverlo tempestivamente: così facendo, infatti,

[1] Cass. pen., sez. V, 19 febbraio 2018, n. 16751. In tale pronuncia, la Corte richiamava la celebre sentenza delle Sezioni Unite n. 31022 del 2015 secondo cui solo le testate giornalistiche telematiche, in quanto ritenute riconducibili alla nozione di stampa, soggiacciono alla disciplina costituzionale e ordinaria prevista per quest'ultima; tuttavia, l'interpretazione evolutiva di stampa coincidente con l'informazione giornalistica professionale non riguarda siti informativi non registrati. Da qui, secondo la Corte, il gestore di un sito non può essere equiparato alla figura del direttore di un periodico né può essere chiamato a rispondere per l'omesso controllo in base all'art. 57 c.p.

[2] Cass. pen., sez. V, 20 marzo 2019, n. 12546.

ne condivide il contenuto e permette l'ulteriore diffusione delle affermazioni lesive della reputazione altrui.
Da qui, applicando al caso di specie tali principi di diritto, la Cassazione giunge a ritenere che i giudici di merito abbiano correttamente valutato gli elementi dai quali hanno dedotto il concorso dell'imputata nella condotta diffamatoria, e in particolare: la sua partecipazione alla raccolta delle informazioni necessarie alla redazione dello scritto, l'adesione al collettivo politico che lo aveva concepito e, infine, la circostanza che, nel corso del dibattimento, l'imputata ne avesse rivendicato il contenuto, affermando di condividerlo interamente.
Per tali ragioni, la Corte riteneva non fondate le doglianze dell'imputata relativa all'applicazione dell'ipotesi di cui all'art. 40 c.p., ritenendo viceversa che i giudici del merito avessero attribuito la responsabilità penale non a titolo di omesso controllo ma individuando correttamente i presupposti del concorso di persone nel reato.

4. Il concorso nel reato di diffamazione del gestore del sito

Pare opportuno affrontare ora alcuni aspetti della decisione che risultano di qualche interesse circa i confini della responsabilità dei gestori di siti web e le regole in tema di concorso di persone nel reato.
La Cassazione, come anticipato, conferma l'impostazione dei giudici di merito in base alla quale al titolare di un sito Internet può essere ascritto il reato di diffamazione in concorso con l'autore del contenuto, ma non quello di omesso controllo.
Anzitutto, la decisione in commento si pone in continuità con l'indirizzo ormai cristallizzato che esclude l'applicabilità del delitto di cui all'art. 57 c.p. che, come noto, punisce a titolo colposo il direttore del periodico che non abbia vigilato sulla pubblicazione e impedito la commissione di reati. In questo senso, a ben vedere, avevano avuto modo di esprimersi già da tempo le sezioni semplici della Corte di Cassazione[3], fino a che tale orientamento ha trovato l'avallo anche delle Sezioni Unite. Nel 2015, infatti, la Corte aveva stabilito che solo le testate giornalistiche telematiche, in quanto ritenute riconducibili alla nozione di "stampa", soggiacciono alla disciplina costituzionale e ordinaria prevista per quest'ultima; diversamente, l'interpretazione evolutiva di "stampa" coincidente con l'informazione giornalistica professionale non può riguardare gli altri e diversi strumenti informativi di manifestazione del pensiero presenti in rete, che restano dunque esclusi dall'estensione della disciplina prevista per tale strumento[4].
Da qui l'impossibilità di equiparare il gestore di un sito alla figura del direttore di un periodico e assumere che possa essere chiamato a rispondere per l'omesso controllo in base a tale fattispecie incriminatrice.
Esclusa l'applicabilità del reato di omesso controllo, chi gestisce un sito web può es-

[3] Cfr. *ex pluribus*, Cass. pen., sez. III, 11 dicembre 2008 (dep. 10 marzo 2009), n. 10535; Cass. pen., sez. V, 16 luglio 2010 (dep. 1° ottobre 2010), n. 35511.

[4] Cass. pen., sez. un., 29 gennaio 2015 (dep. 17 luglio 2015), n. 31022.

sere chiamato a rispondere penalmente dei contenuti pubblicati da soggetti terzi solo in quanto concorrente nel reato, e cioè sulla base delle regole generali di cui all'art. 110 c.p.

In altri termini, quando un utente commette un delitto doloso pubblicando un contributo su un sito Internet, al suo gestore tale illecito può essere rimproverato con una sola forma: direttamente, appunto per concorso, quando sussistono elementi che consentono di ritenere che quest'ultimo abbia posto in essere un contributo morale o materiale alla realizzazione del fatto; non può invece essergli attribuita una responsabilità per colpa *ex* art. 57 c.p. per il mero omesso controllo rispetto a uno scritto per il quale non ha contribuito alla redazione né ne ha condiviso il contenuto.

Come è intuibile, tutto dipende dalla corretta individuazione degli elementi che permettono di ritenere integrato il concorso nel reato.

Sul punto, come anticipato, la Cassazione afferma di applicare un principio di diritto espresso in un proprio precedente del 2019 secondo cui il gestore del sito risponde in concorso con l'autore qualora, venuto a conoscenza di scritti diffamatori, non abbia provveduto alla loro tempestiva cancellazione; e ciò perché l'omessa rimozione equivale alla consapevole condivisione del contenuto offensivo e ne consente l'ulteriore diffusione.

Una simile tesi non pare del tutto convincente perché rischia di non essere perfettamente in linea con le regole in materia di concorso di persone nel reato; una considerazione critica che, invece, come si dirà a breve, non può essere rivolta alla decisione in commento che, a ben vedere, pare in realtà non avallare tale principio di diritto e porsi in discontinuità rispetto al precedente che pure la stessa richiama.

Vediamo perché. Cercando di applicare in modo corretto le regole del concorso al caso concreto, al gestore di un sito dovrebbe essere contestata la diffamazione per uno scritto pubblicato da un terzo sulla pagina da lui curata qualora ponga in essere un contributo morale o materiale alla realizzazione del fatto, ossia l'offesa, precedentemente o in corrispondenza della diffusione dello scritto. In concreto, volendo esemplificare, nel caso in cui ispiri, istighi o rafforzi il proposito criminoso dell'autore, oppure svolga un monitoraggio degli scritti immessi da terzi e ne autorizzi la pubblicazione.

La decisione del 2019, tuttavia, sembra far derivare la conferma della condanna dalla circostanza che il blogger, pur venuto a conoscenza del testo lesivo della reputazione altrui, non si sia prontamente attivato per cancellarlo. In breve, dunque, la condotta concorsuale coinciderebbe con il mantenimento online di un contributo diffamatorio; si tratta, dunque, di una mera inerzia che, pur potendo protrarre gli effetti offensivi, interviene in un momento successivo a un'attività illecita già integralmente compiuta.

Diversamente, la decisione in commento ha il pregio di distinguersi proprio per il buon governo delle regole classiche in tema di concorso di persone nel reato. La Corte, infatti, individua una serie di circostanze che imponevano di concludere per la compartecipazione dell'amministratrice del sito all'attività diffamatoria in un momento antecedente alla pubblicazione dello scritto: nello specifico, aver collaborato alla raccolta delle informazioni necessarie per la redazione dello scritto diffamatorio, aver partecipato al collettivo politico che ne aveva elaborato l'idea e, infine, aver rivendicato il contenuto anche in sede di dibattimento.

In breve, dunque, a differenza del proprio precedente richiamato, la Corte ha individuato correttamente gli elementi che consentivano di affermare che la titolare del sito aveva dato un contributo sia morale sia materiale alla realizzazione del fatto tipico e, da qui, di ritenerla responsabile a titolo di concorso.

Per tale ragione, sembra che la Cassazione abbia fatto riferimento a un precedente – quello del 2019 – che, pur essendo relativo alla medesima materia del caso in esame (ossia, la responsabilità del gestore di un sito per contributi redatti da un soggetto terzo), non ha in concreto orientato la sua decisione.

Non si vuol certo negare che il ricorso al precedente giudiziario nella giustificazione della pronuncia sia una pratica che assume sempre un maggior peso nell'esperienza giuridica del nostro ordinamento e che presidia la certezza del diritto. In merito alla rilevanza del vincolo che deriva dal precedente, è stato opportunamente osservato che «è sopra ogni altra cosa un vincolo di sistema: discende dal fatto stesso che ciascuna decisione non sta a sé, ma si inserisce in un flusso giurisprudenziale che contribuisce a modellare l'ordinamento giuridico e, per ciò stesso, non può prescindere da un minimo di coerenza sistematica»[5]. Tuttavia, pur tenendo conto dell'importanza e del valore persuasivo del precedente, nella decisione in commento gli elementi di differenziazione tra il caso concreto e quello del precedente del 2019 richiamato superavano i profili di similitudine, anche e soprattutto sotto il profilo della *ratio decidendi*; sicché pare non fosse necessario né tenerne conto né richiamarlo, essendo sufficiente – come peraltro ha poi correttamente fatto la Corte – applicare le regole generali classiche del concorso di persone nel reato.

In conclusione, il gestore di un sito, oltre ad essere responsabile dei contributi di cui risulta essere l'autore, può rispondere a titolo di concorso qualora si riesca a dimostrare che ha offerto un contributo morale o materiale alla commissione dell'illecito e dunque con una condotta che precede o coincide con la pubblicazione del messaggio lesivo. Resta, invece, più problematico e ancora aperto il tema della responsabilità per la mancata cancellazione di un contenuto offensivo di cui il titolare del sito sia venuto a conoscenza, ma alla cui creazione sia rimasto estraneo. In questo caso, la protrazione degli effetti diffamatori dovuti al mantenimento in rete di un contributo illecito, ossia un comportamento omissivo che interviene successivamente ad un fatto illecito già integralmente compiuto, a parere di chi scrive, non pare poter integrare una partecipazione penalmente rilevante a titolo di concorso.

[5] R. Rordorf, Stare decisis*: osservazioni sul valore del precedente giudiziario nell'ordinamento italiano*, in *Il Foro Italiano*, 129, 280-281, 2006.

Esposto a un ordine professionale: quali confini per il diritto di critica

Laura Ninni

Corte di Cassazione, sez. V. penale, 11 febbraio 2021, n. 9803

In tema di diffamazione mediante esposto inviato ad un organo di disciplina, sussiste il diritto di critica laddove l'agente abbia assolto l'onere di deduzione di fatti nella convinzione, anche erronea, del rilievo dei medesimi, al fine di ottenere un controllo sulla violazione delle regole deontologiche in relazione all'operato del professionista.

Sommario

1. La vicenda – 2. La comunicazione "con più persone" - 3. Diritto di critica ed esposto all'Ordine professionale - 3.1 Il limite della verità - 3.2 Il limite della continenza espressiva - 4. In conclusione

Keywords

diffamazione - diritto di critica - libertà di espressione - ordine professionale - verità

1. La vicenda

Un cliente, con esposto diretto al Consiglio dell'Ordine degli avvocati, contesta l'operato del proprio legale, il quale avrebbe tenuto condotte in violazione delle regole deontologiche, in particolare fornendo «informazioni eticamente non corrette non nell'interesse del cliente, ma nell'interesse dell'amico avvocato medico con cui condivide laute parcelle».

Il Giudice di pace condanna il cliente per il delitto di diffamazione di cui all'art. 595 c.p. per le affermazioni contenute nella segnalazione all'Ordine.

L'imputato ricorrente deduce, tra l'altro, carenza di motivazione in relazione all'esclusione della causa di giustificazione dell'esercizio del diritto di critica: il giudice di prime cure avrebbe omesso di argomentare in punto di veridicità e continenza espositiva delle espressioni diffamatorie.

Nell'accogliere il ricorso dell'imputato, la Cassazione, con la sentenza in commento, si pronuncia su alcune questioni relative alla configurabilità del delitto di diffamazione ai danni di un avvocato nel caso di esposto al Consiglio dell'Ordine, con particolare riguardo ai limiti al diritto di critica.

2. La comunicazione "con più persone"

Prima di occuparsi del "buon uso" dei principi stabiliti dalla giurisprudenza in tema di

diffamazione e diritto di critica, la Corte ritiene opportuno fugare ogni dubbio in relazione a un profilo che non costituisce motivo di doglianza da parte del ricorrente, ossia il requisito oggettivo del delitto di diffamazione: la comunicazione "con più persone"[1].
Come noto, la condotta che integra il delitto di cui all'art. 595 c.p. – recare offesa all'altrui reputazione – deve realizzarsi attraverso una comunicazione rivolta a più persone, circostanza che avviene qualora due o più persone abbiano notizia dell'offesa, contemporaneamente o anche in momenti successivi[2].
La Cassazione coglie dunque l'occasione per ribadire un principio già consolidato in giurisprudenza: la comunicazione "con più persone" può ritenersi sussistente *in re ipsa*, quando, per la *natura* della comunicazione, la stessa sia "ontologicamente" destinata ad essere diffusa tra più persone[3].
D'altro canto, il principio era già stato affermato proprio in tema di diffamazione realizzata mediante segnalazioni indirizzate ad organi di disciplina[4]. La condotta di comunicazione con più persone è integrata non solo nei casi in cui sia direttamente riscontrabile la volontà, da parte dell'agente, di divulgare a più persone le proprie dichiarazioni, ma anche nel caso in cui, per il *carattere* della comunicazione, questa sia "ontologicamente" destinata alla divulgazione a più parti: proprio come accade allorché taluno operi un esposto all'Ordine, circostanza *di per sé* propulsiva di un procedimento disciplinare e, dunque, costitutiva di una comunicazione che viene naturalmente portata a conoscenza di terzi.

3. Diritto di critica ed esposto all'Ordine professionale

Esaurita la questione, non particolarmente problematica come s'è visto, del requisito

[1] Il primo comma dell'art. 595 c.p. prevede infatti che «Chiunque, fuori dei casi indicati nell'articolo precedente, *comunicando con più persone,* offende l'altrui reputazione, è punito […]».

[2] Così, tra le molte, Cass. pen., sez. V, 4 novembre 2010, n. 7408, *CED* 249599.

[3] Il principio è stato più volte affermato in giurisprudenza e in un'ampia casistica. Si pensi ad esempio a Cass. pen., sez. V, 6 luglio 2015, n. 3963, *CED 265815*, che ha ritenuto integrato il delitto di diffamazione in un caso di espressione offensiva contenuta in un registro per sua natura destinato ad essere normalmente visionato da più persone, come quello dello delle iscrizioni nel registro cronologico utilizzato negli uffici giudiziari per annotare le somme riscosse dai dipendenti per i diritti di trasferta; o ancora, in precedenza, nel caso di frasi offensive contenute in un telegramma (Cass. pen., sez. V, 13 aprile 2007, n. 19559, in *Riv. pen.*, 2008, 3, 318), o inviate a mezzo telefax (Cass. pen., sez. V, 24 aprile 2003, n. 30819, in *Riv. pen.*, 2005, 357), dovendosi considerare tra le "più persone" anche i soggetti che vengano a conoscenza dei contenuti offensivi per la mansione che stanno svolgendo, come ad esempio l'impiegato del telegrafo. Sono dunque le caratteristiche *intrinseche* di tali mezzi che li rendono idonei alla diffusione del contenuto della comunicazione a "più persone".

[4] In questo senso, oltre ai precedenti richiamati dalla Cassazione nella sentenza *de qua* (Cass. pen., sez. V, 29 aprile 2014, n. 26560, *CED 260229*, relativa ad un invio di missiva all'Ordine dei medici e Cass. pen. sez. V, 6 aprile 2011, n. 23222, *CED 250458* ancora in tema di missiva all'Ordine degli avvocati), si segnalano anche Cass. pen., sez. V, 26 settembre 2014, n. 47103, in *DeJure*; Cass. pen., sez. V, 7 novembre 2007, *CED 238909*. Contraria a questo indirizzo, invece, ed in modo isolato, Cass. pen., sez. V, 23 gennaio 2009, n. 19396, *CED 243606*, secondo cui *non* sussiste il requisito della comunicazione con più persone in caso di lettera al Presidente dell'Ordine degli avvocati contenente espressioni offensive e segnalazione di comportamenti deontologicamente scorretti tenuti dal difensore, laddove la successiva comunicazione sia avvenuta per esclusiva iniziativa del destinatario.

della comunicazione con più persone in caso di esposto all'Ordine, la Corte si occupa del primo (e assorbente rispetto agli altri proposti) motivo di doglianza: l'(*in*)*sussistenza della causa di giustificazione del diritto di critica*.

È bene tra l'altro precisare come, in un iniziale passaggio della sentenza in commento, la Cassazione afferma la possibilità di rilevare *ex officio*, oltre alla predetta causa di giustificazione, alternativamente la speciale *causa di non punibilità* di cui all'art. 598 c.p.[5], ossia il diverso istituto[6] che rende non punibili le condotte diffamatorie contenute in scritti e discorsi diretti all'autorità giudiziaria o a quella amministrativa. Nel prosieguo della pronuncia, ad ogni modo, la Corte sembra fare esclusivo riferimento alla causa di giustificazione di cui all'art. 51 c.p., senza soffermarsi sulla configurabilità della speciale causa di non punibilità, la cui applicabilità, in sede di esposti agli ordini professionali, non è del tutto pacifica in giurisprudenza.

In tema di applicabilità dell'esimente di cui all'art. 598 c.p. in sede di esposti a ordini professionali si registrano infatti due indirizzi giurisprudenziali. Secondo un primo, minoritario orientamento, l'esimente in parola è applicabile in questo contesto, poiché l'autore della segnalazione deve essere considerato "parte" del procedimento disciplinare, in quanto titolare di un interesse tutelato[7]. Un secondo orientamento, più fedele alla lettera della legge, ritiene invece l'esimente *non* applicabile alle offese veicolate in sede di segnalazioni all'ordine. Secondo quest'ultimo indirizzo, infatti, l'autore dell'esposto non è tecnicamente "parte" dell'instaurando procedimento disciplinare, trattandosi di un soggetto che si limita a *sollecitare* l'esercizio di una potestà pubblicistica, senza divenire contraddittore[8].

Tornando alla pronuncia in esame, la causa di giustificazione dell'esercizio del diritto di critica, espressione del principio costituzionale di libertà di manifestazione del pensiero, viene come noto frequentemente in rilievo nell'ambito della tutela penale della reputazione[9]. La possibilità di ravvisare la causa di giustificazione dell'esercizio del diritto di critica, e dunque di considerare il fatto di diffamazione lecito all'interno dell'ordinamento, si delinea in presenza dei noti "limiti" elaborati dalla giurisprudenza sul tema: la verità del fatto narrato, la correttezza espressiva, la pertinenza in relazione

[5] Il cui primo comma recita «Non sono punibili le offese contenute negli scritti presentati o nei discorsi pronunciati dalle parti o dai loro patrocinatori nei procedimenti dinanzi all'Autorità giudiziaria, ovvero dinanzi a un'Autorità amministrativa, quando le offese concernono l'oggetto della causa o del ricorso amministrativo».

[6] Come ricordato da Cass. pen., sez. V, 6 luglio 2018, n. 39486, *CED 273888* «in tema di diffamazione, la causa di non punibilità prevista dall'art. 598 c.p., e la scriminante di cui all'art. 51 c.p., *operano su piani diversi*; la prima non esclude l'antigiuridicità del fatto ma solo l'applicazione della pena e ricomprende anche condotte di offesa non necessarie, purché inserite nel contesto difensivo; la seconda si ricollega, invece, all'esercizio del diritto di difesa richiede il requisito della necessarietà ed il rispetto dei limiti di proporzionalità e strumentalità» (corsivi aggiunti). Dello stesso tenore, in precedenza, anche Cass. pen., sez. V, 7 marzo 2017, n. 14542, *CED 269734*.

[7] Così ad esempio Cass. pen., sez. V, 25 settembre 2008, n. 44148, *CED 241806*.

[8] Per questo secondo orientamento, che appare maggioritario, cfr. ad esempio Cass. pen., sez. V, 6 luglio 2018, n. 39486, cit., e Cass. pen., sez. V, 16 ottobre 2002, n. 40725, in *Riv. pen*., 2003, 909.

[9] Come altrettanto noto, il fondamento normativo del "diritto di critica" si rinviene, a livello penale, nell'art. 51 c.p., a livello costituzionale nell'art. 21 (per tutti, in tal senso, G. Vassalli, *Libertà di stampa e tutela penale dell'onore*, in *Arch. pen*., 1967, 34) e infine a livello convenzionale nell'art. 10 C.E.D.U.

all'interesse per l'opinione pubblica[10] .
Nella sentenza in commento, la Corte afferma che, in caso di dichiarazioni offensive contenute in un esposto ad un ordine professionale, è necessario verificare la possibilità di ravvisare la causa di giustificazione di cui all'art. 51 c.p.[11], ricorrendo la scriminante del diritto di critica «quando i fatti esposti siano veri o quanto meno l'accusatore sia fermamente e incolpevolmente, ancorché erroneamente, convinto della loro veridicità» (§ 1.2). Nel peculiare ambito della diffamazione commessa a mezzo di esposto all'Ordine, il diritto di critica «si concretizza in un giudizio valutativo che postula l'esistenza del fatto assunto ad oggetto o spunto della prospettazione critica ed una forma espositiva non ingiustificatamente sovrabbondante rispetto alle censure espresse» (§ 1.3).
Ebbene, secondo la Corte di Cassazione, il Giudice di pace nella sentenza impugnata non avrebbe reso una motivazione rappresentativa della corretta applicazione di tali principi.

3.1 Il limite della verità

I rilievi sull'operato del giudice di prime cure sono svolti dalla Corte principalmente in tema di giudizio di verità delle dichiarazioni rese dall'imputato.
Nel censurare la sentenza impugnata, la Corte da un lato afferma che il Giudice di pace avrebbe impropriamente valutato l'(in)fondatezza delle accuse rivolte all'avvocato sulla base degli esiti del successivo procedimento disciplinare, instaurato a seguito dell'esposto, quindi con una valutazione *ex post*, così sovrapponendo «alla delibazione della soggettiva prospettazione il successivo esito del procedimento» (§ 2.1); dall'altro, il giudice avrebbe totalmente omesso «la disamina delle coordinate di fatto relative ai rapporti tra le parti, ampiamente circostanziate dalla difesa […] in correlazione a ciascuna delle espressioni offensive censurate» (§ 2.1).
Il primo tema censurato dalla Cassazione attiene dunque alla *prospettiva temporale* con cui il giudice valuta il requisito della verità delle affermazioni offensive.
Il giudice, afferma la Corte, deve determinare la veridicità delle dichiarazioni con un procedimento logico *ex ante* e in concreto, "ritagliato" sul soggetto dichiarante e sulle conoscenze di questi al momento in cui manifesta il proprio pensiero. In altre parole, il giudizio deve essere effettuato *dal punto di vista del soggetto agente* in relazione alla consapevolezza circa la verità dei fatti dichiarati e *al momento delle affermazioni offensive*. Il giudizio non può dunque essere "appiattito" su una verità "processuale" come quella scaturente all'esito del procedimento disciplinare, né essere tantomeno riferito ad una realtà che è "vera" solamente in un momento successivo, quale, per esempio, quello della valutazione disciplinare avvenuta a seguito dell'esposto.
Diversamente ragionando, come nel caso in esame, si perverrebbe ad escludere «del tutto apoditticamente e con valutazione postuma, il requisito della verità dei fatti – e

[10] Per tutte v. Cass. pen., sez. V, 14 dicembre 1999, n. 2144, in *Foro it.,* 2001, II, 179.

[11] Di cui si riporta, per comodità del lettore, il primo comma: «L'esercizio di un diritto o l'adempimento di un dovere imposto da una norma giuridica o da un ordine legittimo della pubblica Autorità, esclude la punibilità».

dunque del fondamento di veridicità delle segnalate irregolarità – come postulato in tema di elaborazione critica»[12].

La necessità che la critica appaia *"vera"* al momento del fatto e non *ex post*, è questione peraltro già affrontata dalla giurisprudenza di legittimità[13], anche nell'ambito della stessa casistica della diffamazione a mezzo esposto all'Ordine professionale[14].

Il secondo tema affrontato dalla Corte in materia di veridicità delle affermazioni è quello della necessità che il giudice operi un *vaglio sulle circostanze di fatto* relative ai rapporti tra le parti, ossia sulle «specifiche circostanze del concreto contesto» (§ 2.2).

Nella sentenza impugnata sarebbe infatti mancata qualsiasi «disamina delle coordinate di fatto relative ai rapporti tra le parti […] in correlazione a ciascuna delle espressioni offensive censurate, sì da ancorare la valutazione dell'antigiuridicità del fatto a specifiche circostanze, rispetto alle quali il giudizio di veridicità, come quello di pertinenza e continenza espositiva, deve essere svolto» (§ 2.1). Il Giudice di pace, in altri termini, avrebbe mancato di operare qualsiasi valutazione in relazione alle «specifiche circostanze del concreto contesto, così escludendo, del tutto apoditticamente e con valutazione postuma, il requisito della verità dei fatti» (§ 2.2).

Né, d'altro canto, il giudice avrebbe proceduto ad una simile verifica in termini di putatività[15] «dell'esercizio del diritto di critica, applicandosi la relativa esimente nei confronti di chi abbia la ragionevole e giustificabile convinzione della veridicità dei fatti denunciati, lesivi dell'altrui reputazione, anche se di essa non sussista certezza processuale» (§ 2.2).

Viceversa, dalla sentenza in commento emerge come il ricorrente avesse puntualmente circostanziato i rapporti intercorsi con il legale, in particolare dettagliando come quest'ultimo avesse, tra l'altro, richiesto una consulenza, senza specificare la necessità di una remunerazione diretta del professionista. L'imputato, dunque, per quanto ci è dato sapere, aveva correttamente allegato le specifiche circostanze concrete a fondamento della critica all'operato del proprio legale.

Nella pronuncia in commento la Corte ricostruisce dunque condivisibilmente l'*iter* logico-argomentativo che il giudice deve seguire per affermare il requisito della verità dei fatti esposti dall'agente: il giudizio deve essere operato *ex ante*, riportandosi al momento delle dichiarazioni offensive, per la valutazione delle quali sono necessari riscontri fattuali che fungano da base per le opinioni espresse dall'agente.

---

[12] § 2.2 della sentenza in commento. La Corte richiama sul punto il precedente conforme Cass. pen., sez. V, 17 novembre 2017, n. 8721, *CED 272432*.

[13] Ad esempio, Cass. pen. Sez. feriale, 29 agosto 2017, n. 43139, in *DeJure*, richiamando l'arresto della CEDU, *Zakharov c. Russia,* ric. 14881/2003, in riferimento alla denunciata violazione dell'art. 10 della Convenzione, aveva affermato come la contestazione offensiva, per essere scriminata ai sensi dell'art. 51 c.p., debba apparire vera *al momento del fatto* e non *ex post*, dopo l'accertamento giudiziario.

[14] Ad esempio, Cass. pen., sez. V, 20 luglio 2016, n. 42576, in *DeJure*, aveva annullato la sentenza che aveva condannato, per il delitto di diffamazione, la controparte di un avvocato che aveva inviato un esposto al Consiglio dell'Ordine per manifestare dubbi sulla correttezza del collega, nonostante l'Ordine degli avvocati competente sulla questione avesse poi accertato l'infondatezza delle contestazioni mosse.

[15] Il quarto comma dell'art. 59 c.p. dispone infatti che: «Se l'agente ritiene per errore che esistano delle circostanze di esclusione della pena queste sono valutate sempre a favore di lui».

3.2 Il limite della continenza espressiva

Il secondo limite al diritto di critica oggetto di censure da parte della Corte è quello relativo alla "continenza" delle espressioni utilizzate, ossia alla circostanza che la critica sia operata con una forma espositiva proporzionata, «'corretta' in quanto non ingiustificatamente sovrabbondante al fine del concetto da esprimere»[16].

Anche in tema di continenza espressiva la Cassazione censura l'operato del giudice di prime cure, che non avrebbe fatto buon governo del principio secondo cui «il requisito della continenza postula una forma espositiva corretta della critica rivolta – e cioè strettamente funzionale alla finalità di disapprovazione e che non trasmodi nella gratuita ed immotivata aggressione dell'altrui reputazione»[17].

È principio ormai noto che «l'esercizio del diritto di critica trova un limite immanente nel rispetto della dignità altrui, non potendo lo stesso costituire mera occasione per gratuiti attacchi alla persona ed arbitrarie aggressioni al suo patrimonio morale»[18]. La Corte si riporta qui al consolidato orientamento secondo cui il requisito della continenza «non può ritenersi superato per il solo fatto dell'utilizzo di termini che, pur avendo accezioni indubitabilmente offensive, hanno però anche significati di mero giudizio critico negativo di cui deve tenersi conto anche alla luce del complessivo contesto in cui il termine viene utilizzato […] rispetto al quale assume rilevanza il profilo soggettivo del dichiarante»[19].

Ebbene, la Corte nella sentenza in commento appare pienamente consapevole del fatto che, in tema di esposti all'Ordine, massima è la frizione tra il diritto alla libera manifestazione del pensiero e la tutela della dignità altrui.

Considerando il mezzo e soprattutto le *finalità* con cui le affermazioni offensive sono portate a conoscenza di terzi, l'esposto ad un ordine professionale mira infatti *di per sé*, com'è ovvio, a rendere noto gli organi competenti una *manifestazione d'opinione critica* sull'operato del professionista, di cui si chiede una verifica in ordine ad eventuali infrazioni.

La Cassazione dunque ricorda che in questo, come in altri frangenti, le espressioni

---

[16] Così, da ultimo, Cass. pen., sez. V, 18 gennaio 2021, n. 8898, in *DeJure*.

[17] §. 2.3. La Corte richiama a tal proposito il precedente Cass. pen., sez. V, 18 aprile 2019, n. 21445, *CED 275554*. In precedenza, si veda inoltre, nello stesso senso, Cass. pen., sez. V, 6 luglio 2018, n. 39486, *CED 273888*, che ha escluso la possibilità di ravvisare la causa di giustificazione dell'esercizio del diritto di critica in un caso di esposto al Consiglio dell'Ordine degli avvocati mediante una «missiva gratuitamente denigratoria», contenente «espressioni gravemente e indubitabilmente offensive, oltretutto generiche, insuscettibili di verificazione e non riconducibili all'attribuzione di fatti determinati e concreti, da sottoporre a puntuale indagine deontologica, anche se espressi con asprezza e improprietà da un soggetto digiuno delle terminologie tecniche di un Ordine professionale». Alla stessa conclusione era giunta anche Cass. pen., sez. V, 29 gennaio 2019, n. 14644, in *Leggi d'Italia*, che ha ritenuto non censurabile la valutazione del giudice di seconde cure che aveva ritenuto lesivi della dignità morale di un avvocato, definito – sebbene nel diverso contesto del pezzo giornalistico – "rapinatore" e "gaglioffo" da parte del proprio cliente. La Corte in quell'occasione ha infatti ritenuto che tali epiteti fossero di per sé infamanti non rispettando il limite della continenza ed esorbitassero dunque dal diritto di critica.

[18] Cass. pen., sez. V, 29 gennaio 2019, n. 14644, cit.; in precedenza *ex plurimis* Cass. pen., sez. V, 28 ottobre 2010, n. 4938, *CED* 249239.

[19] § 2.3. Anche in questo caso la Corte richiama precedenti conformi, tra cui Cass. pen., sez. V, 19 febbraio 2020, n. 17243, *CED* 279133.

utilizzate devono essere lette nell'ambito della loro «concreta articolazione e nella complessiva portata significativa» (§. 2.3) delle stesse.
Nel caso di specie, le dichiarazioni offensive non possono allora che essere lette nell'ottica della finalità nell'ambito della quale sono state enucleate: quella di far emergere le criticità dell'operato del professionista, di cui si chiede un giudizio in termini di violazione delle regole deontologiche. La causa di giustificazione in esame deve dunque ritenersi sussistente laddove il soggetto abbia «assolto l'onere di deduzione di fatti nella convinzione, anche erronea, del rilievo dei medesimi ai fini richiesti».
Il requisito della continenza deve essere pertanto valutato tenendo conto «del complessivo contesto dialettico in cui si realizza la condotta e verificare se i toni utilizzati dall'agente, pur aspri e forti, non siano gravemente infamanti e gratuiti, ma siano invece, comunque pertinenti al tema in discussione (…) ed alla sede dell'esternazione, che tollera limiti più ampi alla tutela della reputazione» (§. 1.3).
Ebbene, il giudice di prime cure, oltre a non aver opportunamente indicato quali espressioni fossero da ritenere non continenti, non ha, secondo la Corte, fatto buon governo dei principi sopra richiamati in tema di continenza espressiva, avendo ritenuto superato il requisito della continenza «per il solo fatto dell'utilizzo di termini […] indubitabilmente offensiv[i]» (§ 2.3), senza un'opportuna verifica del *contesto dialettico* nell'ambito del quale gli stessi erano stati utilizzati.

4. In conclusione

La Corte, nella sentenza in commento, sembra fare buon uso dei principi elaborati dalla giurisprudenza in tema di limiti al diritto di critica.
La decisione appare equilibrata e tutelativa del diritto dei cittadini di sollecitare, liberamente, un controllo sulle violazioni da parte del professionista, a patto che la segnalazione sia puntuale, documentata e veritiera, nel senso sopra precisato. Su tali circostanze non può che pronunciarsi il giudice nel caso concreto, operando il consueto bilanciamento tra interessi in gioco.
Sembra infine condivisibile il passaggio di una più risalente pronuncia che, in un caso simile, aveva già affermato come «una risposta diversa si tradurrebbe in un inconcepibile divieto, per gli interessati, di chiedere il controllo sul livello deontologico, nei confronti di soggetti, la cui attività di liberi professionisti o di lavoratori dipendenti, può profondamente incidere sui propri diritti personali e patrimoniali»[20].

[20] Cass. pen., sez. V, 5 luglio 2010, n. 33994, in *Giur. it.*, 2011, 2, 401 che prosegue chiosando «L'interrogativo sulla correttezza professionale di questi soggetti non può tradursi automaticamente, sempre e comunque, in una reazione punitiva dello Stato. La negativa evoluzione del costume, che porta a equiparare controllo/responsabilità, non può giustificare il divieto per i cittadini di chiedere nella sede istituzionale, senza anticipazioni di giudizio e senza devianti comunicazioni, l'esame di chi ha operato e opera nella loro sfera giuridica. Lo *status* di esaminandi, perenni, senza fine è razionalmente giustificato dai poteri che l'ordinamento conferisce ad alcune categorie di consociati».

Consenso, intelligenza artificiale e privacy

Federica Paolucci

Corte di Cassazione, sez. I civile, 25 maggio 2021, n. 14381

In tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati.

Sommario

1. Introduzione. – 2. La vicenda. – 3. Il requisito del consenso validamente prestato: tra tradizione e innovazione giuridica. – 4. Riflessioni conclusive

Keywords

consenso - intelligenza artificiale - protezione dei dati personali – privacy – Cassazione

1. Introduzione

Il provvedimento in commento vede la I sezione civile della Corte di Cassazione pronunciarsi con l'ordinanza n.14381/2021 sulla validità del consenso reso dall'utente che non è venuto preventivamente a conoscenza dello schema esecutivo di un algoritmo. Nei fatti di causa del ricorso *de qua* proposto dal Garante per la Protezione dei Dati Personali è altresì rilevante che tale sistema automatizzato veniva impiegato da parte resistente per l'elaborazione di profili reputazionali degli utenti.

Nell'annullare, dunque, la sentenza del Tribunale di Roma, la Corte elabora un importante principio di diritto che non si sofferma solamente sulle criticità legate all'impiego di strumenti algoritmici per la definizione di un rating di persone fisiche e giuridiche. La Corte si focalizza, in particolare, sul requisito della consapevolezza nella concessione del consenso: gli ermellini hanno esaminato l'opacità di cui il presupposto di liceità del trattamento è ammantato nel momento in cui ci si avvale di un algoritmo per la valutazione di dati personali. Molteplici sono le problematiche etiche e di diritto che vengono in rilievo in questa vicenda. Un primo insieme di osservazioni afferisce al tema del consenso, alla sua validità quando raccolto per sottoporre i dati personali dell'interessato a un *ranking* reputazionale tramite un sistema automatizzato e ai neces-

sari *quid pluris* per la formazione di un consenso reso consapevolmente.
In secondo luogo, occorre invece guardare alla conoscibilità dello schema esecutivo dell'algoritmo e la sua comunicabilità agli interessati: un tema che è persino oggetto della Direttiva (UE) 2019/2161 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori[1].
Prima di passare, dunque, all'esame dei fatti di causa occorre sottolineare che se da un lato queste problematiche si inseriscono nel solco di una serie di novelle normative dell'Unione Europea, dall'altro la pronuncia della Cassazione ha offerto uno sguardo al passato. La causa ha, difatti, avuto inizio nel 2016, periodo in cui il Regolamento (UE) 2016/679, noto come General Data Protection Regulation[2], ancora non era entrato in vigore. Come osservano alcuni commentatori[3], la Cassazione ha ivi messo nero su bianco un principio centrale delle nuove norme europee in materia di protezione dei dati personali e di *governance* dell'intelligenza artificiale pur applicando la disciplina previgente.

2. La vicenda

Con provvedimento n. 488 del 24 novembre 2016[4], l'Autorità garante per la protezione di dati personali aveva considerato la piattaforma illecita a causa della forte incidenza del servizio sulla dignità dei soggetti interessati. Dalle documentazioni al tempo offerte in comunicazione all'Autorità da parte dell'Associazione Mevaluate Onlus, titolare del trattamento[5], si evince che il peculiare modello di business in oggetto è costituito da una piattaforma web (e correlato *database*) e viene descritto come "Infrastruttura Immateriale Mevaluate per la Qualificazione Reputazionale" gestita da Mevaluate Holding Ltd., Mevaluate Italia s.r.l. e Associazione Mevaluate Onlus[6]. Tale piattaforma consta di un sistema di raccolta, verifica, ed elaborazione di dati personali e una successiva fase di assegnazione di «indicatori alfanumerici asseritamente in grado di misurare l'affidabilità reputazionale dei soggetti censiti (persone fisiche e giuridiche)»[7].
Per ovvie ragioni, l'Autorità si è soffermata sugli aspetti che riguardano esclusivamente gli individui e ha riscontrato delle criticità con riferimento all'erogazione di un siffatto servizio che ha delle ripercussioni sulla rappresentazione economica di una pletora di soggetti, siano essi clienti, dipendenti, o candidati a vario titolo per una qualche posi-

[1] Di qui in avanti, Direttiva Omnibus.

[2] Di qui in avanti, GDPR.

[3] G. Scorza, *L'algoritmo deve essere trasparente, la Cassazione rilancia il GDPR*, in *Agenda Digitale*, 26 maggio 2021.

[4] Registro dei provvedimenti n. 488 del 24 novembre 2016, Autorità garante per la protezione dei dati personali.

[5] Si veda punto 1.8 del provvedimento n. 488/2016 dell'Autorità.

[6] Si veda punto 2.1 del citato provvedimento.

[7] Cfr nota n. 6.

zione. Come osserva il Garante, dal momento in cui tali effetti si ripercuotono pesantemente non solo nella vita professionale, bensì (e soprattutto) nella vita privata degli interessati, «occorre, pertanto, estrema cautela nell'affrontare tematiche così delicate, anche in considerazione del fatto che la "reputazione" che si vorrebbe qui misurare, in quanto strettamente correlata alla considerazione delle persone e alla loro stessa "proiezione" sociale, risulta intimamente connessa con la loro dignità, elemento cardine della disciplina di protezione dei dati personali»[8].

L'Autorità, alla luce di queste considerazioni, aveva disposto, *ex* art. 154, c. 1, lett. *d*) del d.lgs. 196/2003[9], il divieto di qualunque operazione di trattamento dei dati personali (presente e futura) effettuata dall'Associazione nell'ambito, precedentemente individuato, della "Infrastruttura Immateriale Mevaluate per la Qualificazione Professionale".

L'Associazione adiva il Tribunale di Roma chiedendo l'annullamento del provvedimento. Con parziale accoglimento del ricorso, il giudice di merito accoglieva l'istanza di parte ricorrente facendo salva la portata del provvedimento solamente per un particolare ambito del servizio: il c.d. "Profilo Contro", ovverosia soggetti terzi non associati a Mevaluate Onlus. A prescindere dalle osservazioni in punto di diritto, ciò che, secondo la valutazione della Corte di Cassazione sconcerta è la motivazione addotta dal giudice di merito. Quest'ultima è stata basata sull'autonomia privata di organizzare sistemi di accreditamento di soggetti, mancando di valutare la *condicio sine qua non* del servizio stesso: la validità del consenso e la conseguente liceità del trattamento. Il Tribunale di merito soffermandosi sulla valutazione del modello di business di questa "Pizia contemporanea", ha mancato di centrare il punto provocando un cortocircuito logico-giuridico che la Cassazione ha risolto con l'ordinanza in commento. Il problema, difatti, è da rinvenirsi nella scarsa trasparenza dell'algoritmo impiegato. Tale aspetto non riguarda semplicemente «il momento valutativo del procedimento»[10] e, dunque, la bontà del servizio offerto, ma la liceità stessa di un servizio che sfrutta una base giuridica viziata. Ricorrendo, *mutatis mutandis*, a una metafora cara ai giudici d'oltreoceano, il punto in discussione non è da ricondursi al *free marketplace of ideas*[11] e il fatto che il mercato stesso farebbe prevalere i migliori servizi a scapito di quelli deficitari. La sostanza del discorso è costituita «dalla validità - per l'appunto - del consenso che si assume prestato al momento dell'adesione»[12]. Nel dettare, dunque il principio di diritto precedentemente richiamato, la Supreme Corte cassa la sentenza del Tribunale di Roma ed osserva che non può desumersi il consenso dalla semplice adesione dell'utente ad una piattaforma: tale modalità non costituisce accettazione di un sistema automatizzato per la valutazione di dati personali laddove l'utente non sia venuto a conoscenza dello

[8] Punto 2.2 del provvedimento in esame.

[9] Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, pubblicato nella *Gazzetta Ufficiale* n. 174 del 29 luglio 2003.

[10] Sentenza del Tribunale di Roma, così come citata Corte di Cassazione, sez. I civile, ordinanza n. 14381/21, depositata il 25 maggio). Cit. al punto VII, 7.

[11] Teoria che anche quando applicata nel suo campo di indagine tradizionale, la libertà di parola, necessita di ripensamenti e aggiustamenti, come osserva O. Pollicino, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in *questa Rivista,* 1, 2018, 31 ss.

[12] Ivi, nt. 8.

schema esecutivo dell'algoritmo.

3. Il requisito del consenso validamente prestato: tra tradizione e innovazione giuridica

Quando si parla di consenso per gli addetti ai lavori è automatico pensare, da tre anni a questa parte, al GDPR. Dovendo, tuttavia, guardare alla normativa previgente, ovverosia, sul piano comunitario, la direttiva 95/46/CE[13], possiamo notare come il Regolamento non abbia stravolto la concezione di consenso. Difatti, l'art. 6 inserisce, come è logico, il consenso tra i presupposti di liceità del trattamento[14] e nel far ciò ricalca quanto era già previsto, sul piano nazionale, dal d.lgs. 196/2003[15]: il Codice Privacy. Sebbene, dunque, non sia l'unica base giuridica, il consenso è tradizionalmente[16] considerato il principale perno dell'intera disciplina della protezione dei dati personali[17]. Ai fini della liceità del trattamento, esso deve essere comunicato ma, secondo le previsioni del d.lgs. 196/2003, soprattutto, deve essere validamente prestato[18]. Nel definire tale criterio, l'art. 23 dispone che il trattamento di dati personali è ammesso solo nei seguenti casi:

- il consenso dell'interessato deve essere espresso;
- questo può riguardare l'intero trattamento o operazioni singole;
- è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 13[19];
- il consenso deve rispettare la forma scritta *ad substantiam* quando trattasi di dati sensibili.

La Corte nell'ordinanza in commento osserva, inoltre, che il consenso può dirsi validamente prestato solo quando il trattamento viene "chiaramente individuato": «ben

[13] Il riferimento è alla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[14] Come osserva R. Panetta, *Consenso o non consenso? Ecco cosa cambia con il GDPR*, in *Corriere Comunicazioni*, 16 aprile 2018, il GDPR ricalca taluni aspetti già presenti nel Codice, quali la necessità che il consenso sia libero, specifico, informato e manifesto. È opportuno sottolineare, anche alla luce della vicenda in esame, che il consenso non è né l'unica né la principale base giuridica del trattamento, dovendo di contro considerare l'ossequio ad obblighi di legge o in adempimento ad un contratto quali i sistemi maggiormente in applicazione tra soggetti pubblici o privati.

[15] Si veda nota n.9.

[16] Si veda M. C. Meneghetti, *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in *questa Rivista,* 1, 2021, 266 ss

[17] Si richiamano in tal senso gli studi di Stefano Rodotà, il quale considerava il consenso la massima espressione del controllo da parte dell'individuo sulle proprie informazioni. Un principio che, del resto, ha tradizionalmente ispirato gli stessi padri della privacy, Warren e Brandeis. Si veda, pertanto con riferimento ai concetti richiamati S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Bari, 2004; S. D. Warren-L. Brandeis, *The Right to Privacy*, in *Harvard Law Review* 4(5), 1890, 193 ss.

[18] Requisito da desumere anche dalla giurisprudenza della Corte richiamata anche nell'ordinanza in esame. *Ex multis,* Cass. civ., sez. I, 11 maggio 2018, n. 17278; Cass. civ., sez. I civ., 22 marzo 2018, n. 16358.

[19] Articolo che si riferisce all'informativa.

definito nei suoi elementi essenziali»[20]. Nel caso in esame il titolare del trattamento poneva alla base della raccolta del consenso una semplice adesione volontaria ai «valori della community»[21]: dunque, l'adesione dell'utente alla piattaforma. In che modalità il titolare del trattamento può sincerarsi del fatto che la scelta è stata effettuata in maniera ponderata, informata, libera, consapevole? Il Gruppo di lavoro Articolo 29 risponde a questa domanda dicendo che il consenso è libero quando «l'interessato [ha effettuato] una scelta effettiva e il controllo sui propri dati»[22]. E il controllo sui propri dati passa (soprattutto) attraverso la consapevolezza delle finalità per le quali sia stato validamente prestato. Il problema che viene ivi in rilievo è che dall'adesione dell'utente ad una piattaforma non può desumersi l'accettazione di ulteriori finalità del trattamento quali la determinazione automatizzata del suo profilo reputazionale[23]. Posto che secondo la disciplina del GDPR tale attività sarebbe critica tanto per i dati oggetto del trattamento, quali, ad esempio, *ex* art. 10[24] afferenti a condanne penali (in quanto l'Associazione sottoporrebbe ad analisi algoritmica anche i casellari giudiziali), quanto per i rimedi, *ex* art. 22.1 del GDPR, la Corte, sebbene non applichi le richiamate norme, si allinea sostanzialmente ad esse. Difatti, gli ermellini, stabilendo il nuovo principio di diritto, hanno posto la conoscibilità dello «schema esecutivo dell'algoritmo»[25] da parte dell'utente come elemento per rendere il consenso validamente prestato. Pertanto, consenso, trasparenza e *accountability* si riconfermano i nodi focali dell'intera disciplina della protezione dei dati personali.

4. Riflessioni conclusive

Nell'ordinanza in commento la Corte si è, da un lato, pronunciata sulla validità del consenso e, dall'altro, sulla liceità del trattamento. Un terzo ordine di domande riguarda, invece, un problema che è rimasto a latere della vicenda giurisprudenziale. Sebbene i giudici tanto di merito quanto di Cassazione, nel rispetto del principio della domanda, non si siano soffermati sul punto, la vicenda in esame fa sorgere diversi quesiti circa la necessità di operare un design chirurgico di tali sistemi algoritmico-reputazionali che siano affidabili, etici e rispettosi dei diritti degli interessati. In secondo luogo, occorre chiedersi: la generalità dei consociati è in grado di comprendere, anche se menzionati

[20] Si veda punto VI, 6, dell'ordinanza.

[21] Si veda punto 1.5 del provvedimento del Garante.

[22] Gruppo di lavoro Articolo 29, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679.

[23] «Le informazioni e i documenti caricati dagli aderenti, infatti, verrebbero raccolti, verificati e resi disponibili agli altri utenti della piattaforma, unitamente ai relativi profili reputazionali, solo a seguito della preventiva raccolta del consenso da parte degli interessati, che "coprirebbe" anche le successive operazioni di trattamento effettuate da terzi (visualizzazione, estrazione e riutilizzo dei dati e dei documenti); il medesimo consenso, inoltre, verrebbe acquisito per giustificare eventuali operazioni di trattamento collegate a presunte "irregolarità" documentali segnalate da altri, nonché per pubblicare atti e documenti attinenti a controversie giudiziarie pendenti o future», citazione dal provvedimento del Garante, punto 1.5.

[24] Cfr punto 1.3 del provvedimento del Garante.

[25] Punto VI, 6, dell'ordinanza.

nell'informativa, gli elementi essenziali che caratterizzano lo schema esecutivo dell'algoritmo?

Con riferimento al primo aspetto e senza l'intenzione di sviscerare le questioni etiche prima che giuridiche dell'impiego di tali strumenti, come ribadisce la bozza di Regolamento dell'intelligenza artificiale recentemente pubblicata, devono essere definiti dei limiti nell'implementazione di strumenti automatici che si sostituiscono al giudizio umano e che hanno delle conseguenze legali e sociali nella vita degli individui. Tuttavia, come osserva il noto saggista Frank Pasquale[26], esistono sempre più meccanismi in grado di contraffare l'esperienza umana e non è logico attendere la consacrazione creazione di un limite al momento della formazione del consenso. Ciò non solo per mancanza di competenze da parte degli stessi utenti, come si vedrà in seguito, ma anche perché è da ripensare il legame tra limiti giuridico-etici e tecnologia, affidando a quest'ultima, e sin dalla sua programmazione, la interiorizzazione dei primi. Tale necessità si manifesta dal momento in cui la trasparenza dell'algoritmo non può essere considerata una panacea, come sostengono anche taluni commentatori[27]. Una criticità questa che appare impellente sia con riferimento alla vicenda in esame sia alla luce della disciplina dell'art. 22 del GDPR ove la vaghezza della norma non protegge adeguatamente gli interessi degli individui. Difatti, come osservano Simoncini e Suweis[28], il punto cruciale è che, pur ammettendo di essere di fronte ad un algoritmo conoscibile e comprensibile e sempre che questo non rappresenti la motivazione esclusiva della decisione, l'algoritmo può essere di per sé discriminatorio e, quindi, incostituzionale.

Per quanto concerne il secondo aspetto, come si accennava all'inizio, l'Unione Europea si sta già muovendo nella direzione di rendere gli utenti-consumatori consapevoli del funzionamento dell'algoritmo. Una scelta normativa che si può rintracciare tanto nella Direttiva Omnibus, lato persone fisiche, quanto nel c.d. Regolamento P2B, lato persone giuridiche[29]. Tali previsioni normative si scontrano però con una triste realtà dei fatti: secondo i risultati del Rapporto Annuale 2020 dell'Istituto Nazionale di Statistica (ISTAT), in termini di *digital divide* l'Italia è ancora in una posizione di svantaggio rispetto agli altri paesi avanzati[30]. In una società, dunque, scarsamente provvista di competenze tecnologiche e caratterizzata dal fenomeno "accetta e continua"[31], il consenso non risulta essere più una base giuridica affidabile. Le prossime sfide per il diritto (e non solo) dovranno essere, dunque, trainate dalla attualizzazione delle norme alle novità tecnologiche, tenendo necessariamente conto della realizzazione di nuovi rimedi e sistemi per rendere effettivo il requisito (imprescindibile) della trasparenza: il rischio è, altrimenti, di imporre rigidi meccanismi di *compliance* alle persone giuridiche

[26] F. Pasquale, *New Laws of Robotics,* Cambridge MA, 2020.

[27] L. Edwards-M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For,* in *Duke Law & Technology Review*, 16, 2017, 18 ss.

[28] A. Simoncini-S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto,* 1, 2019, 87 ss.

[29] Regolamento (UE) 2019/1150 ("Regolamento P2B").

[30] Si veda il *Rapporto annuale 2020. La situazione del Paese, Istat,* 3 luglio 2020.

[31] G. Scorza, *Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché*, in *Agenda Digitale,* 23 aprile 2021.

e dimenticarsi di educare al contempo le persone fisiche per renderle fattivamente in controllo dei propri dati personali.

Il diritto di accesso ai dati personali contenuti nello smartphone di una persona deceduta e conservati in cloud

Valerio Natale

Trib. Milano, sez. I civile, ord. 10 febbraio 2021

Partendo da una recente pronuncia cautelare del Tribunale di Milano, con cui è stato concesso ai genitori di un giovane prematuramente scomparso l'accesso ai dati dello smartphone del figlio conservati in iCloud, si esamina la disciplina sul trattamento dei dati personali delle persone decedute e, in particolare, le condizioni previste dalla legge per l'esercizio dei diritti sui relativi dati personali. Inoltre, il contributo illustra la difficile applicazione di detta normativa nell'ambito dei servizi della società dell'informazione nonché una serie di precedenti del Garante Privacy da cui si evince una particolare esigenza di tutela alla riservatezza dei terzi che hanno interagito col defunto, elemento del tutto disatteso dall'ordinanza in commento.

Starting from a recent urgency decision issued by the Court of Milan, which has granted the parents of a deceased young man the access to the smartphone data of their son that was stored in the iCloud, this article analyzes the provisions on the processing of personal data relating to a deceased person and, in particular, the conditions provided for by the law for the exercise of the privacy rights in relation to the deceased person's data. In addition, this article also highlights the difficult application of this specific legislation in the sector of information society services, as well as a number of previous decisions held by the Italian Data Protection Authority, from which arises a particular need of protection to the privacy of third parties that have interacted with the deceased person – an issue that has conversely been disregarded by the decision that is herein commented.

Sommario

1. Il caso. – 2. Le questioni. – 2.1 La normativa applicabile ai dati personali delle persone decedute: l'art. 2-*terdecies* del Codice Privacy. – 2.2. Segue: la difficile applicazione della normativa ai servizi della società dell'informazione. – 3. I precedenti del Garante Privacy e la tutela posta alla riservatezza dei terzi. – 4. Conclusioni.

Keywords

dati personali – diritto di accesso ai dati personali - persone decedute – Apple – eredità digitale

1. Il caso

L'ordinanza in commento affronta la difficile questione dell'accesso ai dati personali di una persona deceduta e, nello specifico, di quelli contenuti in un dispositivo come lo smartphone.

Nel dicembre 2020 il giovane A. veniva coinvolto in un grave incidente stradale e perdeva la vita di lì a poco. I genitori venivano a conoscenza del fatto che sullo smartphone del figlio, un Apple iPhone X andato distrutto nell'incidente, era attivo il servizio di sincronizzazione automatica denominato iCloud. Quest'ultimo, come il nome suggerisce, è un servizio che consente di salvare sui server di Apple, in via continuativa e automatica, tutti i contenuti digitali presenti nello smartphone, così che essi possano essere recuperati tramite altri dispositivi registrati dallo stesso utente o tramite accesso con credenziali al portale iCloud. Essendo sprovvisti delle credenziali, i genitori di A. chiedevano all'assistenza clienti Apple di poter ottenere l'accesso ai dati contenuti nell'account iCloud del figlio. Dopo il sostanziale rifiuto opposto dall'assistenza clienti in virtù dell'assenza di un provvedimento giurisdizionale a garanzia della liceità del trasferimento, questi promuovevano ricorso *ex* artt. 669-*bis* e 700 c.p.c. avverso la Apple Italia S.r.l. chiedendo in via cautelare l'emissione di un ordine volto ad ottenere l'accesso dei dati personali contenuti nell'account.

Nel ricorso, in particolare, i ricorrenti dichiaravano di voler accedere all'account iCloud per recuperare le fotografie e i video registrati dal figlio per «poter cercare di colmare – almeno in parte – quel senso di vuoto e l'immenso dolore che si accompagna alla prematura perdita di un proprio caro». Inoltre, i ricorrenti dichiaravano di voler accedere alle eventuali ricette del figlio, chef di professione, possibilmente conservate nel dispositivo e dunque nell'account iCloud, al fine di realizzare un libro di ricette commemorativo. In punto di diritto, i ricorrenti motivavano la richiesta ai sensi dell'art. 2-*terdecies* del Codice della protezione dei dati personali (di seguito, il «Codice Privacy»), il quale stabilisce le condizioni che consentono l'esercizio dei diritti che sarebbero spettati all'interessato. Tra le condizioni-presupposto stabilite dalla norma in questione, che operano alternativamente, i ricorrenti ritenevano di poter esercitare il diritto di accesso in virtù dell'esistenza di «ragioni familiari meritevoli di protezione» (su cui si dirà *infra*). Quanto al requisito del *periculum in mora*, invece, i ricorrenti giustificavano l'esigenza di un giudizio cautelare rappresentando che i dati contenuti nell'account iCloud sarebbero andati irrimediabilmente persi dopo un certo periodo di inattività dello stesso, come previsto dai termini e condizioni del servizio.

Apple Italia S.r.l., ritualmente citata, non si costituiva in giudizio e veniva dichiarata contumace.

Il Giudice, ritenuti preliminarmente sussistenti gli estremi per il giudizio cautelare, accoglieva il ricorso e condannava Apple Italia S.r.l. a fornire assistenza ai ricorrenti nel recupero dei dati contenuti nell'account iCloud del defunto.

2. Le questioni

Il caso in esame ha sollevato dinanzi il Tribunale di Milano un tema che, alla luce dei vari interessi in gioco, risulta di difficile interpretazione e applicazione pratica, anche stante l'assenza di precedenti simili nella giurisprudenza nostrana. Ciononostante, pure se in ambiti diversi, il tema dell'accesso ai dati di una persona deceduta è stato oggetto di un discreto numero di decisioni del Garante per la protezione dei dati personali (di seguito, il «Garante Privacy»), delle quali non vi è traccia alcuna nell'ordinanza commentata. Probabilmente complice la contumacia di Apple, infatti, l'ordinanza meneghina omette di considerare aspetti cruciali e meritevoli di approfondimento quali, su tutti, il principio di proporzionalità e di tutela della riservatezza dei terzi che col defunto hanno interagito per il tramite di un dispositivo personalissimo come lo smartphone. Ci arriveremo nel proseguo, dopo aver però fornito un inquadramento sistematico della disciplina.

2.1. La normativa applicabile ai dati personali delle persone decedute: l'art. 2-*terdecies* del Codice Privacy

L'ordinanza affronta preliminarmente il tema dell'individuazione della normativa applicabile al trattamento dei dati personali delle persone decedute. Essa richiama, in particolare, il considerando 27 del Regolamento (UE) 2016/679 (di seguito, il «GDPR»), il quale esclude espressamente dall'ambito di applicazione del Regolamento i trattamenti di dati di persone decedute, lasciando la disciplina di tale peculiare aspetto interamente alla legislazione degli Stati membri.[1] L'impostazione del GDPR ha infatti recepito le indicazioni fornite in passato dal Gruppo di lavoro per la protezione dei dati personali dell'Unione Europea[2] rispetto all'ambito di applicazione della abrogata direttiva 95/46/CE[3], che nulla aveva disposto sul punto.[4] In particolare, con un parere del 2007 sul concetto di dati personali, il Gruppo di lavoro aveva avuto modo di precisare come le informazioni relative alle persone decedute non potessero considerarsi, in linea di principio, dati personali soggetti alle norme della direttiva 95/46/CE [oggi del GDPR]

[1] Tra le più esaustive riflessioni sull'ambito di applicazione del GDPR si veda C. Colapietro-A. Iannuzzi, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano-C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, 85 ss.

[2] Trattasi del gruppo di lavoro (anche noto come Article 29 Working Party) previsto dall'art. 29 della direttiva 95/46/CE, ovvero un organismo consultivo e indipendente composto da un rappresentante della o delle autorità di controllo designate da ciascuno Stato membro e da un rappresentante della o delle autorità create per le istituzioni e gli organismi comunitari, nonché da un rappresentante della Commissione UE.

[3] Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, abrogata a decorrere dal 25 maggio 2018 per effetto dell'art. 94 del GDPR.

[4] In verità, dagli atti del Consiglio dell'Unione europea emerge una posizione congiunta di Consiglio e Commissione volta a lasciare libertà agli Stati membri in relazione alle disposizioni applicabili alle persone decedute (verbale del Consiglio dell'Unione europea del 8 febbraio 1995, documento 4730/95).

poiché, per il diritto civile, i defunti non sono più persone fisiche. Tuttavia, lo stesso parere non aveva escluso che i dati personali dei defunti potessero in alcuni casi beneficiare indirettamente di una protezione, lasciando appunto agli Stati membri la facoltà di disciplinare tale aspetto sussistendo un interesse particolare in tal senso e dando dunque vita a una sorte di «persistenza» dei diritti privacy dopo la morte.[5]

Ebbene, il nostro legislatore aveva già da tempo affrontato la questione con la l. 675/1996, che aveva individuato le condizioni necessarie a giustificare l'esercizio, da parte di terzi, dei diritti del defunto. Molto succintamente, essa prevedeva all'art. 13, c. 3, che i diritti in materia di protezione dei dati personali spettanti in genere alle persone fisiche ma riferiti ai dati personali concernenti persone decedute potessero essere esercitati «da chiunque vi avesse interesse».

Successivamente, il Codice Privacy del 2003, all'art. 9, c. 3, aveva precisato che l'esercizio dei diritti relativi ai dati del defunto potesse essere esperito da chi avesse un «interesse proprio [cioè autonomo da quello del defunto, ndr], o agis[sse] a tutela dell'interessato o per ragioni familiari meritevoli di protezione».

Infine, l'art. 2-*terdecies* del Codice Privacy oggi vigente, introdotto dal d.lgs. 101/2018 nel contesto del generale riordinamento della normativa interna a seguito dell'entrata in vigore del GDPR, ha confermato e ampliato quanto previsto dal Codice Privacy del 2003, disponendo che «I diritti di cui agli articoli da 15 a 22 del [GDPR] riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi [1] ha un interesse proprio, o [2] agisce a tutela dell'interessato, in qualità di suo mandatario, o [3] per ragioni familiari meritevoli di protezione».[6]

La disposizione introduce inoltre alcune novità. Tra queste vi sono due limitazioni all'esercizio dei diritti che sarebbero spettati al defunto. Infatti, non è possibile esercitare detti diritti: (a) nel caso in cui vi sia una limitazione di legge all'accesso alle informazioni (si pensi all'ipotesi di alcune normative specifiche, come quella sul *whistleblowing*)[7] e (b) nel caso in cui l'interessato abbia in vita espressamente vietato l'esercizio dei diritti da parte di terzi, ma limitatamente ai soli servizi della società dell'informazione (come è peraltro il caso di iCloud). L'eventuale divieto deve esprimersi con dichiarazione al Titolare del trattamento, dimostrando una volontà specifica, libera e informata. A

[5] Parere 4/2007 sul concetto di dati personali adottato il 20 giugno 2017 (documento 01248/07/IT WP 136). Il parere richiama altresì la sentenza della CGUE, C-101/2001, *Lindqvist*, secondo cui le «possibilità [di manovra riservate agli Stati Membri in relazione ad aspetti non coperti dalla direttiva 95/46/CE] devono essere usate nel modo previsto dalla direttiva 95/46 ed in conformità del suo obiettivo, che consiste nel mantenere un equilibrio tra la libera circolazione dei dati personali e la tutela della vita privata» (§ 97).

[6] Il lettore più attento non mancherà di notare l'aggiunta, alla seconda ipotesi, rispetto al testo previgente, dell'inciso «in qualità di suo mandatario», su cui si tornerà più avanti. Per un approfondimento sulla fase attuativa del GDPR negli Stati membri si veda C. Colapietro, *I principi ispiratori del Regolamento UE2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, *Federalismi.it*, 22, 2018.

[7] L'art. 23 del GDPR consente al diritto dell'Unione e degli Stati membri di limitare, mediante misure legislative, la portata degli obblighi e dei diritti degli interessati. Nel nostro ordinamento l'art. 2-*undecies* del Codice Privacy si preoccupa di individuare un elenco di ipotesi per le quali i diritti di cui agli artt. da 15 a 22 non possono essere esercitati. In taluni di questi casi, comunque, l'ordinamento consente un esercizio mediato dei diritti per il tramite del Garante, il quale poi provvede a informare l'interessato rispetto all'esito (cfr. artt. 58 e 160 del Codice Privacy).

parziale deroga di tale divieto, il c. 5 dell'art. 2-*terdecies* prevede che questo non possa produrre effetti pregiudizievoli per l'esercizio dei diritti patrimoniali di terzi derivanti dalla morte dell'interessato o per la difesa in giudizio dei propri interessi. Trattasi di una previsione chiaramente finalizzata ad assicurare la facile ricostruzione del patrimonio del defunto e evitare che il divieto posto da quest'ultimo possa bloccare qualsivoglia azione da parte degli aventi diritto. Si pensi, ad esempio, al legittimario pretermesso che in virtù del generale divieto all'accesso disposto dal *de cuius* si ritroverebbe impossibilitato ad esperire le azioni previste a sua tutela, non avendo egli modo di ricostruire il patrimonio effettivamente esistente (ad esempio, l'ammontare della giacenza su di un portafoglio elettronico o i documenti contabili salvati in un archivio in cloud). Infine, si noti come con l'art. 2-*terdecies* il legislatore non abbia voluto attribuire alcun valore all'eventuale qualifica giuridica del soggetto che intende esercitare i diritti del defunto (quale, ad esempio, potrebbe essere stata l'indicazione dell'erede, del congiunto, dell'unito civilmente, etc.), lasciando invece al caso concreto la valutazione sull'effettiva esistenza di un rapporto meritevole di tutela. Una impostazione figlia del progresso e del riconoscimento di una dimensione naturalistica degli affetti dell'individuo.[8]

2.2. Segue: la difficile applicazione della normativa ai servizi della società dell'informazione

La normativa in questione si scontra con una difficile applicazione pratica nell'ambito dei servizi della società dell'informazione (come per l'appunto il servizio di sincronizzazione iCloud di Apple, ma anche altri servizi, ad esempio di posta elettronica come Gmail o Yahoo! o di social network come Facebook e Instagram). In tutti questi casi, infatti, non possono ignorarsi talune peculiarità, come: (1) la difficoltà, per i fornitori, di strutturare un'unica soluzione capace di declinare le diverse scelte normative adottate nel mondo; (2) l'esistenza di un rapporto contrattuale tra utente e fornitore e l'atteggiarsi di tale rapporto in relazione alla normativa interna (talvolta inderogabile); e, soprattutto, (3) l'impatto che l'esercizio del diritto di accesso può avere sulle aspettative di riservatezza dei terzi che hanno interagito col defunto tramite quello stesso servizio (si pensi, ad esempio, all'impatto sui terzi nei casi di accesso alla cartella «posta ricevuta» di un account di posta elettronica, ai messaggi ricevuti su WhatsApp o persino in App per incontri come Tinder o Grindr).

Partendo dalla prima delle questioni richiamate, negli anni recenti si è via via sempre più diffusa, nel mercato dei servizi della società dell'informazione, l'abitudine di concedere agli utenti la facoltà di indicare un cd. «contatto erede». Si tratta, in sostanza, di un terzo utente cui può essere riconosciuto dopo il proprio decesso l'accesso a tutti i, o parte dei, dati contenuti nell'account. Viceversa, si è anche diffusa la pratica di

[8] Tale condivisibile impostazione segue l'impianto originario già contenuto nella l. 675/1996; si veda sul punto in dottrina G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione: commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, Milano, 1997, 321 e Garante Privacy, 17 luglio 2009 (doc. web. 1656642) con cui è stato riconosciuto al convivente di una donna deceduta, in assenza di un rapporto coniugale, l'accesso alla sua cartella clinica, il cui diritto di accesso era stato precedentemente rifiutato dalla struttura sanitaria in quanto non ritenuto un di lei «prossimo congiunto».

consentire all'utente di impostare la cancellazione automatica di tutti i, o parte dei, dati conservati nell'account al momento del decesso (notificato da un terzo o presunto per decorrenza di un determinato periodo di inattività).[9] È proprio con riferimento all'insorgenza dell'opzione di selezione di un cd. "contatto erede" che deve probabilmente assumere significato l'inciso, aggiunto dal d.lgs. 101/2018 all'art. 2-*terdecies*, che specifica che per soggetto che «agisce a tutela dell'interessato [defunto]» deve intendersi un soggetto che agisce «in qualità di suo mandatario». Come ha sostenuto la dottrina, infatti, il legislatore ha così voluto recepire la forte spinta all'autonomia privata intrapresa dalle *big tech*, dopo averla ritenuta compatibile con i principi nostrani del diritto delle successioni e, nello specifico, con il generale divieto di patti successori. Questi strumenti, infatti, non si porrebbero in contrasto col divieto di patti successori in quanto essi consentono di regolare rapporti che afferiscono alla mera sfera della personalità, e non alla sfera patrimoniale, circostanza che sì invece avrebbe sollevato dubbi di compatibilità con i principi del del nostro ordinamento.[10] Infine, la mancata apposizione di requisiti di forma per l'espressione di detto mandato costituirebbe ulteriore conferma della volontà di riconoscere l'utilità e la legittimità di tali strumenti, semplificando le modalità di svolgimento dell'autonomia privata.

Dubbi, invece, emergono in relazione al requisito di forma scritta previsto dal c. 2 dell'art. 2-*terdecies* per l'espressione della volontà dell'interessato di vietare a terzi l'esercizio dei diritti sui propri dati dopo la morte. Se da un lato, infatti, l'assenza di requisiti di forma per l'indicazione del cd. «contatto erede» sembrerebbe voler dimostrare un'apertura del legislatore in termini di progresso, d'altro lato il requisito della forma scritta per l'espressione del divieto sembrerebbe voler ostacolare qualsiasi semplificazione. Ad ogni modo, nonostante il dato letterale della disposizione, è opinione di chi scrive che, ispirandosi al pensiero dalla giurisprudenza più progressista sull'interpretazione da attribuire, nel contesto online, al requisito di forma scritta per la sottoscrizione delle clausole vessatorie di cui all'art. 1341 c.c., può ritenersi che la forma scritta per l'espressione del divieto di cui all'art. 2-*terdecies* possa ritenersi soddisfatto laddove l'espressione avvenga mediante la tecnica del "*point & click*" (cioè, con l'apposizione di una mera spunta su di un'opzione di divieto preimpostata dal fornitore del servizio all'interno

[9] Prendendo in esame lo strumento «Gestione account inattivo» di Google, ad esempio, l'utente può indicare un periodo di tempo oltre il quale Google deve considerare inattivo l'account (al momento, da 3 a 18 mesi di inattività). Oltre tale periodo, nel corso del quale Google prova a contattare il titolare dell'account tramite SMS e email ad un altro indirizzo indicato dallo stesso, è possibile disporre l'eliminazione automatica dell'account e di tutti i dati oppure autorizzare in via automatica l'accesso a massimo 10 persone di fiducia, da indicare tramite indirizzo email, i quali potranno accedere, secondo l'opzione selezionata, a tutti i dati o soltanto parte di essi, individuabili per servizio (ad es. soltanto Gmail, o Drive, o Calendar, etc.). La scelta tra l'eliminazione e la designazione di uno o più contatti autorizzati, infine, può anche sovrapporsi, posto che se l'utente decide di consentire a un terzo di scaricare i propri contenuti dell'account inattivo e al contempo dispone la cancellazione automatica dei dati, tale terzo avrà tre mesi di tempo per farlo prima che l'account venga eliminato definitivamente. La dottrina non ha mancato di passare in rassegna le varie soluzioni adottate e, per una ricostruzione anche cronologica delle soluzioni succedutesi, si rimanda alle opere di G. Resta, *La morte digitale,* in *Il diritto dell'informazione e dell'informatica*, 2014, 896 ss. e A. Magnani, *L'eredità digitale*, in *Notariato*, 5, 2014, 519 ss.

[10] Si veda in particolare G. Resta, *Chi controlla la nostra identità digitale dopo la morte?*, in *Giustiziacivile.com*, 9 ottobre 2003, 5, secondo la cui ricostruzione la dottrina prevalente avrebbe ben accolto tale autonomia negoziale ritenendola non in conflitto con il generale divieto di patti successori e riconducendo la libertà di scelta concessa dalle piattaforme agli interessati nella fattispecie del mandato *post mortem exequendum*.

dell'area riservata dell'account) o altra tecnica analoga, secondo il grado di evoluzione della tecnica informatica.[11]

Muovendo invece al secondo degli aspetti segnalati, ovvero le questioni attinenti al rapporto contrattuale tra fornitore e utente e al suo atteggiarsi rispetto alla normativa interna, val la pena evidenziare come l'art. 2-*terdecies* non faccia menzione alcuna al contratto con l'utente. Eppure, l'esistenza di tale rapporto contrattuale è stato più volte posto al centro dell'attenzione dalla giurisprudenza straniera che si è trovata ad affrontare casi simili a quello in commento.[12] Altrettanta rilevanza al tema del rapporto contrattuale esistente tra utente e fornitore del servizio è stata riservata da parte della dottrina nostrana, la quale ha peraltro mosso critiche per il fatto che molto spesso trattasi di contratti standardizzati e per mera adesione.[13] In sostanza, secondo tale giurisprudenza e dottrina il mandato conferito dal defunto a un terzo al di fuori dell'ambito della piattaforma (ad esempio, in un testamento) non potrebbe che esplicarsi nei limiti posti dalle condizioni contrattuali precedentemente sottoscritte tra defunto e fornitore del servizio. Un simile mandato, dunque, troverebbe un ostacolo insormontabile nelle clausole di intrasferibilità che sono spesso previste nei termini e condizioni di detti servizi, vanificando dunque l'esperibilità del mandato.[14] È peraltro questo il caso anche del servizio iCloud, secondo i cui termini «Se non diversamente previsto dalla legge, accettate che il Vostro Account non è trasferibile e che qualsiasi diritto verso il Vostro ID Apple o Contenuto nell'Account si estingue con la Vostra morte […]».[15] L'incipit

[11] Sul punto, è particolarmente esaustiva la motivazione offerta dalla sentenza del Trib. Napoli, 13 marzo 2018, n. 2508 che ha ritenuto soddisfatto il requisito di accettazione per iscritto delle clausole vessatorie mediante "point & click": «[…] gli strumenti tecnologici impiegati per la stipula del contratto telematico ontologicamente non si prestano ad assecondare le previsioni dell'art. 1341 c.c. in tema di specifica sottoscrizione delle clausole vessatorie presupponendo tale norma l'esistenza di un modulo a stampa sottoposto alla firma del contraente che, in ambito telematico, viene sostituita dalla compilazione online di un formulario […] e dalla presa visione e accettazione con la tecnica del point & click delle condizioni contrattuali a cui rimanda con un link (c.d. collegamento ipertestuale) e dalla definitiva conferma della propria volontà negoziale attraverso la medesima tecnica». È spesso richiamata nella dottrina anche un precedente apparentemente conforme risalente al 2002 del G.d.P. Pantanna (cit. in G. Cassano-P. Cimino, *Contratto via Internet e tutela della parte debole*, in *I Contratti*, 10, 2002, 869 ss.). In contrasto con le precedenti pronunce dei giudici di Napoli e Pantanna, invece, si veda Trib. Catanzaro, ord. 30 aprile 2012, secondo cui «con riguardo alle clausole vessatorie on line, l'opinione dottrinale prevalente – alla quale il Tribunale aderisce – ritiene che non sia sufficiente la sottoscrizione del testo contrattuale, ma sia necessaria la specifica sottoscrizione delle singole clausole, che deve essere assolta con la firma digitale. Dunque, nei contratti telematici a forma libera il contratto si perfeziona mediante il tasto negoziale virtuale, ma le clausole vessatorie saranno efficaci e vincolanti solo se specificamente approvate con la firma digitale[!]». Una lettura, quest'ultima, che applicata alla manifestazione di divieto di cui all'art. 2-*terdecies*, finirebbe per azzerarne l'uso concreto e dunque la funzione di tutela per l'interessato.

[12] Per un approfondimento della giurisprudenza straniera si veda I. Maspes, *Successione digitale, trasmissione dell'account e condizioni generali di contratto predisposte dagli internet services providers* in *I Contratti,* Milano, 2020, 5, 583 e ss.

[13] Tra le innumerevoli pubblicazione che affrontano il tema, si vedano G. Resta, *La morte digitale*, cit., 907 ss., F. Padovini, *Rapporto contrattuale e successione per causa di morte*, 1990, 35 ss.; S. Deplano, *La successione a causa di morte nel patrimonio digitale*, in C. Perlingieri -L. Ruggeri (a cura di), *Internet e diritto civile*,, Napoli, 2015, 427 ss., nonché A. Zoppini, *Le «nuove» proprietà nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni),* in *Riv. dir. civ.*, 1, 2000, 185 ss.

[14] G. Finocchiaro, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, 469.

[15] Termini e condizioni del servizio iCloud, Sezione IV, paragrafo «D. Nessun diritto di successione»,

della clausola, pensata per essere applicata in più giurisdizioni, lascia volutamente impregiudicata la normativa inderogabile eventualmente applicabile nel Paese del contraente, come deve ritenersi sia il caso della disciplina italiana contenuta nell'art. 2-*terdecies* del Codice Privacy. Infatti, si ritiene di poter aderire alla tesi della migliore dottrina, secondo cui la scelta del legislatore italiano sia stata quella di rimarcare il massimo potere di controllo e autodeterminazione dell'interessato sui propri dati; conseguentemente, l'intervento del terzo mandatario designato dovrebbe essere assicurato, dopo la morte del mandate, al di là di qualsivoglia contrasto con le condizioni poste dal fornitore del servizio.[16] In tale ottica, dunque, in presenza di un mandato chiaro e documentato (ad es., una nomina a esecutore testamentario in relazione alla gestione di taluni dati personali), il fornitore del servizio non potrebbe opporre alcunché, e dovrebbe piuttosto aderire alla volontà del defunto, proprio rivitalizzando quell'autonomia privata che i fornitori stessi hanno, per primi, valorizzato.

Rimane da affrontare la terza questione sopra richiamata, ovvero l'impatto che l'esercizio dei diritti in luogo del defunto – e, specialmente, del diritto di accesso – può avere sulle aspettative di riservatezza tanto del defunto che dei terzi che con questo hanno interagito. Come si vedrà nel paragrafo che segue, il diritto alla riservatezza del defunto e dei terzi è stato oggetto di analisi in alcune interessanti decisioni del Garante Privacy, che hanno cercato di individuare un bilanciamento tra il diritto alla riservatezza e il diritto del terzo istante a esercitare i diritti previsti dalla normativa sui dati del defunto, con risultati che sembrano del tutto in controtendenza rispetto all'ordinanza in commento.

3. I precedenti del Garante Privacy e la tutela posta alla riservatezza dei terzi

Come si è detto, la l. 675/1996 già consentiva di esercitare i diritti sui dati personali di persone decedute, possibilità poi mantenuta (ed ampliata) dal Codice Privacy. Ciò ha consentito di sedimentare nel tempo un discreto numero di decisioni dinanzi il Garante Privacy, che vale la pena analizzare.

Le decisioni del Garante Privacy possono dividersi in due principali categorie: da un lato le decisioni sulle richieste presentate sulla base di un interesse proprio dell'istante, per lo più finalizzate all'accesso ai dati per interessi di natura patrimoniale); dall'altro lato le (più rare) decisioni sulle richieste presentate per «ragioni familiari meritevoli di protezione», per lo più finalizzate alla cancellazione o alla rettifica. Ad ogni modo, come si vedrà, tutte le decisioni passate in rassegna affrontano il tema della tutela dei terzi.

In una prima nota del 22 maggio 2000 il Garante Privacy ha reso noto di aver rigettato un ricorso presentato nei confronti di una banca con cui il figlio di una signora defunta aveva chiesto di accedere all'identità di una persona che aveva prelevato alcune somme

disponibile all'indirizzo *apple.com*.

[16] G. Finocchiaro, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., 470.

da un deposito al portatore intestato alla signora. In particolare, il Garante Privacy, nel respingere il ricorso, motivava che l'interesse proprio del richiedente non potesse che intendersi limitato alle sole informazioni concernenti la posizione della *de cuius* (quali, ad esempio, quelle sull'esistenza di un conto e del relativo saldo), non potendo però estendersi sino a consentire l'accesso ai dati personali di terzi, seppure indirettamente beneficiari delle somme connesse al rapporto intestato alla signora.[17] Dello stesso indirizzo sono la decisione del 27 ottobre 2000 con cui il Garante ha dichiarato inammissibile una richiesta volta a conoscere il nominativo del terzo possessore di un titolo al portatore menzionato nella documentazione del defunto[18], nonché la decisione del 22 settembre 2003 con cui, accogliendo la richiesta di un erede ad accedere ai dati del defunto in relazione ad alcune polizze assicurative, il Garante ha escluso la possibilità di accedere agli estremi identificativi dei terzi beneficiari della polizza stipulata dal *de cuius*.[19] In un altro caso del 2014 concernente la richiesta di accesso alla cartella clinica di un soggetto deceduto in ambito ospedaliero, inoltre, il Garante si è riservato di verificare con un autonomo procedimento l´eventuale illiceità della comunicazione fatta dall'ospedale all'istante ad esito della richiesta, posto che la cartella clinica consegnata conteneva anche dati di terzi non strettamente connessi alla vicenda della defunta.[20] Ancora, nel 2017, decidendo su un ricorso di una signora intentata ad accedere alla cartella clinica della madre deceduta in una casa di cura, nonché all'elenco delle visite alla madre avvenute nel giorno in cui la *de cuius* aveva revocato precedenti disposizioni testamentarie in suo favore, il Garante, pur riconoscendo il diritto della ricorrente ad accedere alla cartella clinica e all'indicazione delle eventuali visite alla madre, ha ritenuto il ricorso inammissibile in ordine alla richiesta di ottenere altresì le generalità dei visitatori. Conseguentemente, la casa di cura ha potuto fornire all'istante esclusivamente conferma o meno delle visite effettuate alla madre in tale giorno, inclusiva degli orari di ingresso ed uscita, ma non anche alle generalità dei visitatori, proprio in virtù del fatto che la legge consente l'accesso ai soli dati del *de cuius*, e non di terzi.[21]

Fuori dall'ambito patrimoniale, invece, e in assenza di decisioni più aderenti al caso in commento, si ritiene estremamente significativa la dichiarazione che fece nel 2006 Mauro Paissan, membro del collegio del Garante, in relazione alla notizia, riportata su diversi giornali, di una donna che aveva chiesto al fornitore del servizio email Yahoo! l'accesso alla casella email del padre defunto.[22] Le dichiarazioni dell'allora membro del Collegio al Corriere della Sera sembrano essere in linea con la forte tutela alla riservatezza dimostrata nelle decisioni passate in rassegna. Egli, infatti, dichiarò: «Non si può consegnare a nessuno, nemmeno agli eredi, una casella di posta elettronica, perché

[17] Garante Privacy, 22 maggio 2000 (doc. web. 1163550)

[18] Il provvedimento, non immediatamente disponibile sul sito del Garante, è richiamato in Garante Privacy, 3 aprile 2002 (doc. web. 1065256).

[19] Garante Privacy, 22 settembre 2003 (doc. web. 1053716 sul sito www.garanteprivacy.it).

[20] Garante Privacy, 6 febbraio 2014 (doc. web. 3039504).

[21] Garante Privacy, 15 giugno 2017 (doc. web. 6697731). Per una panoramica della normativa specifica in materia di trattamento di dati personali in ambito sanitario si veda C. Colapietro-F. Laviola, *I trattamenti di dati personali in ambito sanitario*, in *Dirittifondamentali.it*, 2, 2019, 1 ss.

[22] Per tutti, si veda A. Lisi, *L'insostenibile riservatezza di un'email*, in *punto-informatico.it*, 30 gennaio 2007.

può contenere dati personali non soltanto del defunto ma di tutti i suoi interlocutori. L'accesso va proibito nel modo più assoluto».[23] L'insieme delle decisioni sopra richiamate fanno emergere chiaramente come l'approccio al tema della privacy sia nel tempo mutato, uscendo da una logica unidirezionale focalizzata sul rapporto tra Titolare del trattamento e singolo interessato, emergendo piuttosto la necessità ricorrere a una nozione di ambito più ampio, che comprenda anche quelli che sono stati definiti «i flussi dall'esterno verso l'interno».[24]

Venendo alle decisioni su ricorsi fondati sull'esercizio dei diritti per «ragioni familiari meritevoli di protezione», invece, va innanzitutto chiarito che queste rappresentano un numero estremamente esiguo e si caratterizzano per un esame particolarmente scrupoloso.[25] Queste, infatti, sembrano aver trovato accoglimento esclusivamente in quei casi in cui fosse effettivamente possibile individuare la coesistenza di un duplice interesse, tanto dell'istante quanto del defunto. Conseguentemente, l'immagine che se ne trae è di una tutela normativa offerta non tanto ai superstiti in sé quanto piuttosto alla più ampia formazione sociale di cui era parte il defunto – la famiglia, appunto – quale centro di interessi collettivo e autonomo.

In un provvedimento del 11 ottobre 2006, ad esempio, il Garante è stato chiamato a decidere su alcuni articoli contenenti i dati personali relativi ad un minore che si era tolto la vita «nonché [i dati personali relativi] al padre dello stesso […] e, più in generale, al contesto familiare e sociale nel quale viveva il minore». Il padre ricorreva dunque al Garante per vedere tutelato l'onore e la riservatezza della famiglia quale centro di interessi autonomo, inclusivo sia degli interessi del minore defunto sia di quelli dei familiari superstiti. In particolare, il ricorrente chiedeva di vietare la diffusione di talune informazioni familiari nonché quanto lasciato scritto dal minore nell'ultimo tema svolto in classe prima del tragico evento, che era stato ripreso in stralci nei medesimi articoli. Il Garante, conclusa l'istruttoria, accoglieva il ricorso riconoscendo l'esistenza di un interesse familiare sotteso alla richiesta, vietando la diffusione ulteriore del quotidiano contenente le informazioni familiari e ordinando all'editore di allegare copia della decisione a tutti gli esemplari del quotidiano conservati in magazzino, a futuro monito.[26]

Infine, in un ultimo caso connesso alla pubblicazione su un giornale locale di informazioni relative alla morte di un uomo per overdose, il Garante ha riconosciuto le ragioni familiari addotte dai ricorrenti, i quali avevano sostenuto vi fosse stata una lesione del diritto alla solidarietà e all'onore familiare, oltre che un'offesa alla memoria del defunto.[27] Anche qui, in sostanza, un interesse duplice, tanto degli istanti quanto del defunto.

---

[23] *Corriere della Sera*, 26 settembre 2006, 31.

[24] C. Colapietro-A. Iannuzzi, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano-C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017. Sul tema, non può non rimandarsi anche alle primissime riflessioni sul tema di S. Rodotà, *La «privacy» tra individuo e collettività*, in *Pol. Dir.*, 1974, 552 ss.

[25] Alla data del 1° aprile 2021 risultano sul sito del Garante n. 106 provvedimenti nella categoria "persone defunte".

[26] Garante Privacy, 11 ottobre 2006, non più disponibile sul sito del Garante ma reperibile a questo link.

[27] Il caso, non più disponibile in rete, è riportato in G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, 247. Sul tema, si vedano anche le interessanti riflessioni di F. Laviola, *Il diritto all'oblio in Italia dalle origini alla «codificazione»* in *Studi parlamentari e di politica costituzionale*,

4. Conclusioni

Alla luce delle considerazioni svolte, l'ordinanza in commento non convince per una serie di motivi.

Preliminarmente, il Tribunale di Milano omette del tutto l'accertamento del ruolo della contumace Apple Italia S.r.l. rispetto al servizio iCloud. Pur volendo disapplicare i termini di servizio nella parte in cui richiamano istituti giuridici inesistenti nel nostro ordinamento, infatti, i termini contrattuali avrebbero potuto (e dovuto) assumere rilevanza ai fini dell'individuazione del soggetto legittimato passivo. Il contratto di servizi iCloud non menziona mai la Apple Italia S.r.l., bensì indica chiaramente la Apple Distribution International Ltd. (con sede in Irlanda) quale controparte contrattuale – e dunque Titolare del trattamento – per gli utenti italiani. La questione rimane irrisolta, posto che la motivazione si occupa del tema soltanto en passant, assumendo la Apple Italia S.r.l. legittimata passiva semplicemente perché «appartenente al gruppo Apple (tramite cui opera la Apple Distribution International LTD)». La motivazione manca dunque, in fatto e in diritto, di fornire prova di una connessione tra le tue persone giuridiche capace di generare una responsabilità dell'una per l'altra, o comunque di provare un rapporto tra la società italiana e quella irlandese in relazione alla gestione del servizio iCloud che risulti sufficiente a qualificare la legittimazione passiva della Apple Italia S.r.l.[28] Preme rilevare, inoltre, come tale elemento rappresentasse un interesse degli stessi ricorrenti, ai quali l'ordinanza offre ora un titolo presumibilmente incapace di produrre effetti nei confronti della Apple Distribution International LTD, titolare dei rapporti connessi ad iCloud.

Quanto al merito, l'ordinanza premette una descrizione della normativa esistente, richiamando ampi stralci dell'art. 2-*terdecies* del Codice Privacy ed evidenziando come l'espressione del divieto di esercizio dei diritti da parte di terzi dopo la propria morte, esperibile nei confronti dei fornitori di servizi online, risulti in qualche modo di ispirazione comune al principio di autodeterminazione previsto dalla recente l. 219/2017 in materia di disposizioni anticipate di trattamento. Accertata dunque l'assenza in atti di una qualsivoglia espressione di divieto esercitata dal defunto nei confronti dei dati con-

2018, spec. 85, secondo cui le richieste di cancellazione *post mortem* possono di fatto qualificarsi quali forme di esercizio di un diritto all'oblio ultra-attivo rispetto alla durata della vita del soggetto interessato.

[28] Ad avviso di chi scrive trattasi di un grave vizio di motivazione, posto che non esiste nell'ordinamento italiano alcuna disposizione secondo cui le persone giuridiche costituite in Italia e afferenti a un gruppo societario straniero possano essere ritenute responsabili per le attività svolte in via esclusiva da altre persone giuridiche del medesimo gruppo costituite e aventi sede in altri ordinamenti. Peraltro, dalla visura camerale della Apple Italia S.r.l. risulta che questa si occupi prevalentemente di attività di supporto alla vendita e che essa non è sede secondaria della Apple Distribution International Ltd., circostanza che avrebbe trovato menzione nella visura ai sensi dell'art. 2197, c. 2 e 3, c.c.). A scanso di equivoci, preme sottolineare che non avrebbe neppure potuto assumere alcun valore una eventuale partecipazione sociale della Apple Distribution International Ltd. nella Apple Italia S.r.l., posto che «l'art. 2497 cod. civ., che disciplina la responsabilità delle società e degli enti che esercitano attività di direzione e coordinamento di altre società, consente ai soci e ai creditori sociali di agire direttamente contro la società o l'ente che esercita l'attività di direzione e coordinamento ove non siano stati soddisfatti dalla società controllata, ma non viceversa, ossia che le società partecipate o controllate possano essere chiamate a rispondere civilmente per attività poste in essere dalla partecipante o dalla controllante» (Trib. Torino, ord. 16 febbraio 2021, in un caso che vedeva erroneamente chiamata in giudizio la Google Italy S.r.l. per fatti concernenti un'altra società del gruppo).

tenuti in iCloud, la motivazione passa alla disamina delle «ragioni familiari meritevoli di protezione» addotte dai ricorrenti, quale requisito di cui all'art. 2-*terdecies* del Codice Privacy. A tal proposito, l'ordinanza omette sia l'accertamento di quell'interesse duplice (tanto dei ricorrenti tanto del defunto) che ha caratterizzato le decisioni passate del Garante, sia l'accertamento della sussistenza di una base giuridica idonea a consentire l'accesso dei ricorrenti ai dati personali di terzi che hanno interagito col defunto tramite lo smartphone – anch'essi conservati nell'iCloud. Assume dunque valore assoluto, agli occhi del giudice meneghino, il solo interesse dei ricorrenti – umanamente più che comprensibile – al ricordo e alla commemorazione, con totale disinteressamento per le legittime aspettative di riservatezza dei terzi, le cui foto, i cui messaggi, le cui voci e confidenze sono verosimilmente conservate nel medesimo account iCloud e potrebbero essere violate. Il risultato che ne esce è una ordinanza che, oltre a non tenere conto dei principi di proporzionalità, manca di assoluta coerenza con le commentate decisioni Garante e con la sensibilità che oggi accompagna l'utilizzo accorto dello smartphone, quale contenitore delle nostre vite.[29]

Al di là della critica in punto di diritto, che all'ordinanza è esclusivamente rivolta, resta ovviamente sottratto a qualsiasi giudizio il dramma umano vissuto dai ricorrenti, a cui nessun giudice potrà dare cura.

[29] In ossequio al principio di proporzionalità, l'ordinanza in commento avrebbe eventualmente potuto garantire l'accesso limitatamente ai dati di talune applicazioni, circostanziando temporalmente i dati oggetto di tutela, sulla base delle precise richieste formulate dai ricorrenti.

Responsabilità del social network per chiusura immotivata dell'account con distruzione dei dati ivi presenti. Sul rapporto giuridico utente/piattaforma: tra protezione e commercializzazione dei dati personali

Lorenzo Albertini

Trib. Bologna, 10 marzo 2021

Nel rapporto Facebook/utente, il secondo offre al primo, con atto negoziale dispositivo, l'autorizzazione a utilizzare i propri dati personali a fini commerciali: sicché, nonostante l'affermata gratuità del servizio, sussiste per entrambi i contraenti il requisito della patrimonialità della prestazione oggetto dell'obbligazione (art. 1174 c.c.). A prescindere dall'utilizzo che Facebook ne fa (se li cede e trasmette a terzi oppure se se ne serve soltanto per offrire ai terzi i presupposti di una informazione pubblicitaria mirata), non può revocarsi in dubbio che i dati personali dell'utente abbiano un manifesto valore economico e siano inquadrabili come controprestazione nel rapporto utente-gestore. Ne consegue il carattere evidentemente oneroso del rapporto negoziale, posto che il contratto è fondato su un evidente sinallagma, per cui alla prestazione del servizio da parte del gestore corrisponde il suo interesse ad utilizzare i contenuti, le reti di relazioni e i dati personali dell'utente, a fini di raccolta pubblicitaria.

Sommario

1. I fatti. Giurisdizione e legge applicabile. – 2. La qualità di consumatore. – 3. Il tipo di rapporto giuridico. – 4. Il consenso al trattamento dei dati. – 5. La disponibilità del diritto sui propri dati personali – 6. Il recesso e altre conseguenze della contrattualità. – 7. La distruzione dei documenti (cancellazione dei dati). – 8. Risarcimento del danno. – 9. La domanda (rigettata) di adempimento contrattuale.

Keywords

contratto di social networking – data montetization – deplatforming – dati personali – social network

1. I fatti. Giurisdizione e legge applicabile

In una recente ed interessante ordinanza *ex* art. 702-*ter* c.p.c. il Tribunale di Bologna ha

deciso una fattispecie del tutto particolare inerente al rapporto tra piattaforma e utente. La stessa ha dunque costituito l'occasione per le riflessioni contenute nel presente scritto.

Un utente Facebook (poi: Fb) gestiva su tale piattaforma da dieci anni un profilo a nome proprio, collegandovi due pagine relative a libri, riviste, storie e altri cimeli militari. Fb improvvisamente gli chiuse l'account il 2 gennaio 2020, senza spiegazione. A dire del ricorrente, la ragione consistette in una ritorsione per avere egli, quale avvocato e per conto di un cliente, venti giorni prima diffidato Fb stessa a riaprire l'account del cliente: Fb gliela avrebbe allora fatta pagare, chiudendo pure a lui l'account. A quel punto il ricorrente citò Fb in giudizio, chiedendone la condanna al ripristino del profilo e delle pagine collegate nonché una penale per ogni giorno di ritardo, oltre al risarcimento dei danni.

Il colosso di Menlo Park si costituisce, eccependo (a parte la carenza di legittimazione passiva: Facebook Italia anziché Ireland), da un lato, l'impossibilità di individuare il profilo e le pagine indicati, visto che non era stata indicata la u.r.l.; dall'altro, di aver sì reperito un account legato ad una certa casella email, ma che il relativo materiale era stato distrutto in via definitiva, in modo da non poter dedurre nulla sulle ragioni di tale rimozione.

Il giudice affronta dapprima la questione della giurisdizione, strumentale alla quale c'è la questione del se si trattasse di rapporto giuridico con un consumatore (come accennato, l'utente-attore nella propria vita lavorativa faceva l'avvocato). La strumentalità deriva dal fatto che l'eventuale proroga di giurisdizione (patto sulla giurisdizione) è nulla, laddove riduca la tutela offerta ai consumatori, inderogabile. Ed in effetti le clausole generali, proposte/imposte da Facebook, prevedono una proroga di giurisdizione a favore del giudice irlandese. Verosimilmente (ma non lo dice espressamente) il giudice, una volta accolta la qualificazione di consumatore, avrà applicato l'art. 18, c. 1, del Regolamento (UE) 1215/2012, che permette al consumatore la scelta del proprio foro. La clausola di proroga, pur non espressamente prevista nell'elenco dell'art. 33 Codice del consumo[1], parrebbe in effetti vietata.

2. La qualità di consumatore

Il giudice esclude che dal materiale, verosimilmente messo on-line, si possa ravvisare un uso c.d. promiscuo[2]. Con ciò lascia intendere che, se invece questo fosse stato ravvisato, non avrebbe potuto considerarlo consumatore: con le conseguenze in punto di giurisdizione.

Il giudice dà quindi per scontata la conseguenza, secondo cui, nel caso di uso promiscuo, non possa applicarsi la disciplina consumeristica. Dato il tenore letterale del regolamento cit., come anche del nostro art. 3, lett. *a)*, Codice del consumo, la conclusione

[1] La lett. *t)* menziona le deroghe alla competenza dell'autorità giudiziaria, mentre la lettera u) quelle alla competenza territoriale.

[2] Lo desume dal fatto che le allegazioni attoree di uso privato non sono state contestate (p. 2/3).

è probabilmente giusta; tuttavia, non dà atto dell'esistenza di opinioni diverse[3]. L'uso promiscuo, dunque, non è tutelato dalla normativa consumeristica (probabilmente: a meno che la componente professionale sia marginale[4]: solo che è difficile dire quando ciò ricorra e comunque andrebbe interpretato restrittivamente).
Una volta allegata e provata la qualità di consumatore, per il giudice spettava a controparte provare la qualità professionale (p. 3).
È pure esatta la considerazione, secondo cui il solo gestire un profilo Fb vantaggioso per la sua immagine pubblica, non significa che quel sito o quella pagina o quella account vadano automaticamente ritenuti strumento dell'attività professionale. Il punto è importante, poiché riguarda una situazione fattuale probabilmente diffusa ed inoltre obiettivamente non chiara.

3. Il tipo di rapporto giuridico

Il giudice passa poi esaminare il merito e cioè il tipo di rapporto tra le parti. Egli ravvisa un contratto (§ 4), ciò che - alla luce della definizione di cui il 1321 c.c. - è corretto. Sarebbe interessante indagare le condizioni predisposte da Facebook per vedere se parlano di contratto: probabilmente no, visto che secondo il giudice (riferendosi alle condizioni generali, come parrebbe dal virgolettato) parlerebbe di "iscrizione" a servizi on-line per entrare in contatto con gli altri utenti del mondo. Il servizio fornito da Fb, dice il giudice, è "a titolo gratuito", anche se subito dopo aggiunge che Fb trae «comunque vantaggio economico dalle inserzioni pubblicitarie, anche mediante l'utilizzo di dati personali degli utenti che consentono di offrire ai terzi spazi pubblicitari calibrati sugli specifici interessi dei loro destinatari».
Nel cit. passaggio l'affermazione di gratuità non è esatta. Non solo non si tratta di prestazione liberale, ma nemmeno di prestazione gratuita: infatti la cessione del diritto sui propri dati è necessaria per accedere al servizio e quindi ne rappresenta il corrispettivo chiesto da Fb. Di solito si parla di atto "gratuito" non solo quando non è accompagnato da controimpegno, nemmeno a titolo di condizione[5], ma anche – in contrapposizione a "liberale" - quando si tratta di atto interessato, sotto il profilo economico o meno[6]. Qui invece l'impegno di Facebook, da una parte, e la cessione di diritti da

[3] Vedasi: A. Barenghi, *Diritto dei consumatori*, Milano, 2020, 44; G. Chinè, sub *art. 3*, in V. Cuffaro (a cura di), *Codice del Consumo*, 2019, Milano, § 2.4, 28-29.

[4] Così CGUE, C-464/01, *Gruber c. Bay Wa AG* (2005), in tema di giurisdizione *ex* Convenzione di Bruxelles del 27 settembre 1968, che pone l'accento sulla necessità di valutare le circostanze oggettivamente emerse e presenti nel fascicolo del giudice nazionale (§ 50 e poi terza conclusione).

[5] A. Gianola, *Atto gratuito, atto liberale. Ai limiti della donazione*, Milano, 2002, 33.

[6] A. Gianola, ivi, 33 e 147 ss., amplia il concetto di "gratuito" all'atto privo di corrispettivo, al cui interno distingue quello interessato da quello disinteressato; v. Id., *Atti gratuiti, atti liberali non donativi*, in S. Martuccelli- V. Pescatore (a cura di), *Diritto civile*, *Dizionari del dir. priv.* prom. da Irti, Milano, 2011, 123 ss, § 2. Analogamente P. Gallo, *Trattato del contratto. 1) La formazione*, Torino, 2010, 210-211; nella stessa opera v. pure il tomo *2) Il contenuto. Gli effetti*, 1009-1013 (promesse gratuite interessate, tipiche o atipiche). Altri riservano il concetto di "gratuito" solo all'atto privo di corrispettivo ma interessato, includendo l'area della prestazione disinteressata in quella della liberalità (F. Gazzoni, *Manuale di diritto privato.*, Napoli, 2006, 833-835), come si dice nel testo. È solo questione di intendersi, anche se il forgiare

parte dell'utente sui propri dati (lasciamo da parte l'esatta qualificazione di questo atto dispositivo)[7], dall'altra, stanno in reciproco rapporto sinallagmatico: per cui, trattandosi di prestazioni a contenuto patrimoniale, il rapporto generato è inquadrabile appunto come contratto.

Anzi è stato osservato che non solo i dati, ma anche il tempo e l'attenzione possono considerarsi corrispettivo del servizio reso da Fb. Così ha infatti osservato l'Autorità per la Concorrenza tedesca nella nota e ponderosa decisione del 2019: «*The user remains a customer, even if the service is available for free. In this respect, time or attention and the data the users enter replace the fee and can be seen as a compensation for the service. This applies in particular to ad-funded services, which offer their users' time, attention and data to advertisers in return for revenues. Ultimately, advertising markets are "markets for time" which consider the users' time and attention to be a product*»[8]. La dottrina ha esplorato le conseguenze del valore che il mercato attribuisce all'attenzione dell'utente, proponendo rimedi contro l'abuso del potere di mercato, ravvisabile nelle pratiche manipolative (così spesso adoperate dalle piattaforme)[9].

In breve, visto che proposta e accettazione combaciano e sono reciprocamente connesse, anche il requisito dell'accordo è soddisfatto[10]: ricorre infatti il c.d. sinallagma genetico. Non c'è bisogno di precisare che questo tipo di scambio è verosimilmente alla base di tutti i servizi digitali fruibili senza corrispettivo monetario[11]. Prassi imprenditoriali, la cui conoscenza dovrebbe rientrare nella formazione dei giuristi di oggi per una corretta trattazione delle pratiche loro affidate: il grosso dei traffici giuridici, infatti, avviene con queste modalità.

In ogni caso, quando il consenso è espresso (anche tramite click o accettazione "per

concetti in proprio rischia di confondere il dibattito.

[7] Si tratta naturalmente non solo di cessione dei propri dati, ma di cessione degli stessi con diritto di usarli nei termini pattuiti. La precisazione, fatta nell'ordinamento tedesco (v. G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, 151-152), parrebbe scontata: l'interpretazione del contratto secondo i canoni consueti porta con sicurezza a tale esito, non rivestendo alcun interesse per la piattaforma la pura memorizzazione senza il diritto di usarli a fini di advertising.

[8] Bundeskartellamt 06.02.2019, B6-22/16, § 246. Ma si tratta di giudizio diffuso, probabilmente preso dalla teoria economica: v. F. Lancieri-P.M. Sakowski, *Competition in Digital Markets: A Review of Expert Reports,* in *Stanford Journal of Law, Business & Finance,* 26(1), 2021, per i quali «*consumers pay for many digital servicesby bartering data and attention in exchange for services and ads. Indeed, not only does this combination of data and attention have a market price, but the high profit margins of digital platforms indicate that this value is not zero*» (p.to 88).

[9] Attento esame in G. Day-A. Stemler, *Are Dark Patterns Anticompetitive?,* in *Alabama Law Review*, forthcoming, letto in *ssrn.com*: «*We argue that online manipulation coerces users into spending attention, data, and money—all things of great value in the digital economy*», 24 (attento esame prima dei profili socio-psicologici - privacy e manipolazione -, e poi di quelli antitrust - parte III e IV -). "*Dark patterns*" sono le modalità di progettazione della piattaforma e del suo software, volti a sollecitare determinati comportamento degli utenti: basate sull'economia comportamentale e in particolare sulla dualità Sistema 1-Sistema 2, proposta da Daniel Kahneman (e Amos Tversky) (ivi, 14).

[10] R. Sacco–G. De Nova, *Il contratto*, Torino, 2016, 211 ss.

[11] Esiste poi un florido mercato secondario dei dati, settore poco conosciuto. Si v. inoltre il sistema di aste automatiche per le inserzioni pubblicitarie, realizzato da Google, ed esaminato da D. Srinivasan, *Why Google Dominates Advertising: Markets Competition Policy Should Lean on the Principles of Financial Market Regulation*, in *Stan. Tech. L. Rev.,* 24, 2020, 55 ss.: l'A. ne esamina i profili concorrenziali, inclusi asimmetrie informative e conflitti di interesse (parte III, 86 ss. e parte IV per suggerimenti *de iure condendo* sull'esempio della regolamentazione finanziaria).

spunta" di casella), non dovrebbero esserci dubbi sulla qualifica contrattuale del rapporto emergente[12].

Il giudice si esprime in termini di "autorizzazione" circa l'utilizzo dei dati. Si tratta di concetto civilistico con un significato preciso. La sua utilità -se non addirittura legittimità- di uso, tuttavia, è assai dubbia, per cui sarebbe probabilmente più lineare limitarsi a parlare di "consenso". Proprio in tema di *data protection* è stata proposta la tesi dello sdoppiamento dell'atto del consenso latamente inteso: uno scriminante l'ingresso nella propria sfera e l'altro permettente la circolazione dei dati relativi[13]. Si tratta però di una distinzione di scarsa aderenza alla prassi e dunque di scarsa utilità, dato che allora potrebbe venir replicata per qualsiasi attività altrui sui propri beni materiali (ad esempio: riparazione di un impianto idraulico in casa): non supererebbe la prova del rasoio di Occam, per cui è preferibile lasciarla da parte[14].

Il fatto che tale rapporto sia inquadrabile come contratto[15] produce conseguenze giuridiche: oltre a sottoporlo alla sua disciplina comune, ad es. permette di sottoporlo a quella consumeristica *ex* artt. 33 ss. Codice del consumo. Potrebbe invece non apparire necessaria, a prima vista, la qualifica contrattuale per sottoporlo a quello delle pratiche commerciali sleali *ex* art. 18 ss. Codice del consumo: qui, infatti, il campo d'applicazione parrebbe a prima vista più esteso, concernendo le "pratiche commerciali tra professioni e consumatori". Tuttavia, affinché "venga falsato il comportamento economico"

[12] Ampio esame delle modalità procedimentali in A. Quarta, *Mercati senza scambi. La metamorfosi del contratto nel capitalismo della sorveglianza*, Napoli, 2020, cap. III, *passim*, spec. §§ 11-12. Il problema si pone per la modalità consistente nella mera navigazione nel sito, che per l'a. non può costituire comportamento concludente nel senso di accettazione tacita, mancando l'inequivocabilità dell'atto alla luce della prassi sociale (292 ss.). L'affermazione, però, suscita perplessità, se riferita al caso in cui le condizioni del servizio sono state fatte presenti all'utente (anche per l'intensissima prassi sociale già formatasi).

[13] Citazioni in C. Angiolini, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020, 123, nt. 33-34.

[14] La rigetta pure C. Angiolini, ivi, 123-124. L'A. qualifica i dati personali come beni giuridici (difficilmente contestabile) e giustamente include le previsioni dell'informativa *ex* art. 13 GDPR nel contenuto del contratto (197-198). Ed infatti il concetto di bene ricomprende sia le *res* che le creazioni intellettuali, che - più ampiamente - quelle *ex lege,* quando ad esempio la legge permetta la regolazione per contratto dei nuovi *digital assets* (N. Banta Lynner, *Property Interests in Digital Assets: The Rise of Digital Feudalism*, in *Cardozo L. Rev.,* 38, 2017, 1099 ss.; *feudalism*, perché i diritti sono attribuiti agli utenti solo nella misura e per il tempo in cui la piattaforma lo concede: sub III, 1149 ss.). Il diritto sui dati, poi, parrebbe "similproprietario", se si concorda che il cuore del "terribile diritto" è lo *ius excludenti alios* (v. C. Salvi, *Neoproprietarismo e teorie giuridiche della proprietà*, in *Eur. dir. priv.*, 4, 2020, 1169 ss., *passim* (spec.1171 e 1177); confermano, in linea di principio, A. Quarta-G. Smorto, *Diritto privato dei mercati digitali*, Milano, 2020, 262 (sull'applicabilità dell'istituto possessorio; per gli A. il diritto di escludere è il "primo diritto" –*rectius*: facoltà- del proprietario: ivi, 265). *Contra* G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., 93-94, soprattutto per il fatto che il bilanciamento, peculiare degli atti dispositivi sui propri dati, sarebbe assente nella proprietà. Il che però non è: non bisogna confondere il momento statico con quello dinamico. Anche la tutela del proprietario di *res*, quando ne dispone, deve conciliarsi con quella di altri diritti confliggenti; come, al contrario e considerando il momento statico, la tutela dei propri dati è assoluta (e non gravata dai limiti propri della relazionalità), fino a che il titolare non li inserisce nel circuito mercantile. Pure non utile è addurre la revocabilità del consenso e gli altri diritti posti dal GDPR *ex* art. 15 ss: da un lato, riguardano la fase dinamica e non statica; dall'altro, stante la indiscutibile differenza tra gli interessi sottostanti (sulla propria persona e sulle res), la disciplina non può essere uguale. Ciò non impedisce però di ravvisare possibilità di estensione analogica delle regole dominicali presupponenti lo *ius excludendi alios*, ove non siano incisi i profili più personali.

[15] In tale senso v. ampiamente S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, cap. II, 49 ss. (per le cui conclusioni spec. 105).

del consumatore, è difficile ipotizzare una modalità diversa dalla stipula di un contratto (di acquisto, solitamente).

A questo proposito non è chiara la posizione del Consiglio di Stato, che pur conferma il rigetto della tesi di Fb disposto dal giudice di primo grado. Ravvisa infatti bensì una pratica commerciale ingannevole, ma esclude che ricorra una commercializzazione dei dati[16]. È ambiguo il riferimento ad una "messa a disposizione" dei dati che non integra una loro "commercializzazione": infatti il titolo, in base a cui la prima avviene, è quello di uno scambio, e cioè appunto quello di una commercializzazione dei dati.

In breve, il rapporto giuridico negoziale è da qualificare come contratto a titolo oneroso: il servizio digitale è erogato a fronte di un diritto sull'uso dei dati prodotti dall'attività online dell'utente[17]. Il punto è ormai pacifico e quasi tutta la dottrina lo riconosce[18]. Profilo, tra l'altro, che rende incerta (o almeno potrebbe modificare) l'applicazione del concetto tradizionale di mercato[19], in cui diversi beni venivano paragonati tramite il loro prezzo monetario, che fungeva da c.d. unità di conto: il diritto ceduto sui propri dati personali, infatti, è dubbio possa svolgere la stessa funzione. Anche se la risposta potrebbe essere positiva, dato che nel trattamento massivo dei big data scompaiono le individualità: potrebbe allora darsi che dal punto di vista della piattaforma i dati di un singolo individuo arrivassero ad avere un valore standardizzato, potendo anche alla fine fungere da unità di conto, al pari del denaro[20]. Ma si potrebbe ribattere in senso opposto che il valore di (*rectius* le utilità ritraibili da) un profilo individuale dipende molto dalla capacità di sfruttamento del suo acquirente: per cui verrebbe meno la possibilità di svolere tale tradizionale funzione.

Ora, poi, la cosa è divenuta non controvertibile alla luce della direttiva (UE) 2019/770, che regola l'inadempimento del fornitore di contenuti e servizi digitali e i rimedi del consumatore (si v. l'art. 3, che ne delimita l'ambito applicativo)[21]. Sono prestazioni che

---

16 Cons. Stato, sez. VI, 29 marzo 2021 n. 2631, 25-26.

17 Si badi, diritto sull'uso dei dati prodotti dall'attività, non diritto ad una determinata attività dell'utente: equivoca sul punto G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., 58-60. Secondo questo a., il rilascio di informazioni personali va equiparato ad un'attività, addirittura richiamando (anche se cautamente, per vero) il rapporto di lavoro subordinato. Al contrario, nel nostro contratto viene dedotto il diritto sulle tracce digitali lasciate dall'attività online, non il diritto sull'attività, la quale resta del tutto libera nell'*an*, nel *quomodo* e nel *quando*.

18 Vedi per citazioni il mio saggio *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione generale sul loro ruolo di gatekeepers della comunicazione)*, in, *MediaLaws - Law and media working paper series*, 15 ottobre 2020, nt. 96 (ove cenno ad una dottrina contraria), cui aggiungi C. Angiolini, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, cit., 189-190 (proprio circa Facebook) e A.Quarta-G. Smorto, *Diritto privato dei mercati digitali*, cit., spec. 211 e 217 (il cui cap. 3 illustra in modo chiaro la caratteristiche degli odierni mercati digitali). In senso contrario alla contrattualità, aderisce alla tesi di Camardi l'articolato lavoro di G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit. (spec. 156 ss., 174-175 e 182 per la revoca).

19 Al netto della scarsissima concorrenzialità dei mercati dominati dai colossi tecnologici.

20 «*Money addresses the commensurability problem by creating a common unit of exchange that can be applied in a variety of contexts*» (R. Hollander Blumoff-M.T. Bodie, *The Market as Negotiation*, in *Notre Dame L. Rev.*, 96, 2021, 1257 ss., spec. 1261.

21 Conf., direi, G. d'Ippolito, *Commercializzzione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inf.* 2020, 666 ss. La storia della redazione non vi è di ostacolo, come vorrebbe A. Addante, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *Giust. civ.*, 4, 2020, 898 ss.

non si possono considerare in modo reciprocamente isolato o comunque tali da evitare la qualificazione di contratto (o negozio bilaterale). La prova sta appunto nell'equiparazione *quoad poenam* o meglio *quoad remedium* disposta dalla direttiva citata, a dispetto del considerando 24 per cui «tali dati non possono dunque essere considerati una merce». All'opposto, si è detto che l'eurolegislatore della direttiva (UE) 2019/770 confermerebbe le difficoltà nel qualificare come contrattuale la fornitura di dati contro servizio digitale: lo proverebbe il diverso *wording*, dovuto all'intento di lasciare impregiudicata la riconducibilità dell'operazione al tipo "contratto" (alla luce dei casi di non applicazione della direttiva indicati nel considerando 25), visto che tale qualifica non sarebbe scontata nei vari ordinamenti[22]. L'opinione non pare da condividere. Al contrario, il considerando 25 esclude la direttiva proprio nei casi in cui i dati non costituiscono il corrispettivo. Quando invece costituiscono corrispettivo, è il considerando 24 ad occuparsene, per affermare inequivocabilmente la contrattualità.

4. Il consenso al trattamento dei dati

In quest'ottica di scambio esplicito tra servizio digitale contro diritto sui dati personali, va menzionata la questione del se il consenso sia libero, quando è prestato per un servizio, alla cui esecuzione non è strettamente necessario. Vediamo se la risposta potrebbe essere positiva, nonostante l'opinione di gran lunga prevalente sia nel senso opposto[23]. È sicuro che il consenso al trattamento dei propri dati a fini promozionali non è tecnicamente necessario per l'esecuzione della prestazione dei servizi di posta elettronica o di motore di ricerca. Solo che (potrebbe osservarsi) la valutazione sarebbe ragionevole farla non in relazione al funzionamento della prestazione promessa, ma dell'operazione economica complessiva, in cui la prima è inserita: ebbene, tale operazione prevede esattamente lo scambio tra prestazione digitale e cessione del diritto sui dati. Quindi se questo è il regolamento negoziale (offerto, accettato e quindi) concordato, in fase esecutiva il consenso sui dati diventa necessario: tanto che la piattaforma in caso contrario può non prestare il servizio a suo carico (oppure, astrattamente ed ex ante, potrebbe anche prestarlo ma a fronte di corrispettivo monetario: il che però cambierebbe radicalmente il tipo di business). In altre parole, affermare che in tale caso il consenso non è libero, potrebbe sembrare inesatto: dire che non è necessitato dall'attuazione della controprestazione, implica considerare questa ultima isolatamente, prescindendo dall'operazione in cui è inserita. Il tenore dell'art. 7, par. 4, del GDPR è ambiguo e non aiuta a chiarire, nonostante prendano invece posizione contraria a quanto qui ipotizzato le linee guida dell'European Data Protection Board[24].

[22] G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., 174-175.

[23] Si v. la cit. nota 96 del mio saggio *Sulla responsabilità civile degli internet service provider per i materiali caricati dagli utenti (con qualche considerazione generale sul loro ruolo di gatekeepers della comunicazione)*, cit. sopra (e qui ad es. la decisione del Bundeskartellamt tedesco del 6 febbraio 2019, caso B6-22/16). Nel senso della maggioranza e quindi in senso opposto alla tesi cautamente avanzata nel testo v. pure A. Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale*, cit., 58 ss.

[24] Linee guida 05/2020 sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 4 maggio 2020, sub § 3.1 e p.ti 13-15.

Inoltre, secondo il considerando 42, «il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio». Qui, però, da un lato, parrebbe libero, poiché nessuno costringe l'utente ad aprirsi un account Fb; dall'altro, non può ravvisarsi pregiudizio, visto che il servizio offerto non è in regime di monopolio né è servizio pubblico, per cui manca un obbligo a contrarre. Nemmeno si tratta di prestazione chiesta, assieme ad un'altra parallela (quasi fosse un *tying* concorrenzialmente abusivo) o solo apparentemente necessaria, ma in realtà evitabile dall'utente e/o evitabile solo con eccessivo sforzo[25]: si tratta invece un'offerta commerciale costruita con corrispettivo non monetario.

Così ragionando, dunque, è poco comprensibile (almeno al sottoscritto) la posizione di chi ravvisa un *tying contract* nell'accordo sulla cessione dei dati (a fini di profilazione) rispetto a quello sulla fornitura del servizio digitale[26]: quasi fosse un accordo imposto dalla parte forte, distinto da quello principale chiesto dall'utente, secondo la nota figura di abuso di posizione dominante in antitrust, chiamata appunto *tying* (art. 102, par. 2, lett. *d*) TFUE; art. 3, lett. *d*), l. 287/1990). Si tratta invece di un unico accordo, servizio digitale contro dati: mancando la pluralità di operazioni da legare, non può ravvisarsi pratica di *tying*.

In breve, dunque, potrebbe sostenersi che la tutela dell'utente contro lo strapotere delle piattaforme, senz'altro doverosa, non potesse percorrere questa via (almeno per ora)[27]. Su questa linea si può ricordare la sent. 17278/2018 della Cassazione, secondo cui «il condizionamento non possa sempre e comunque essere dato per scontato e debba invece essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato, il che non può certo dirsi accada nell'ipotesi di offerta di un generico servizio informativo del tipo di quello in discorso, giacche´ all'evidenza si tratta di informazioni agevolmente acquisibili per altra via, eventualmente attraverso siti a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio».

Ciò a meno di ravvisare la ratio della disposizione nell'intento di «porre un correttivo ad un problema attuale di concentrazione di potere in capo ad alcuni soggetti… rispetto ad un potenziale controllo su una massa enorme di informazioni, che li pone in una condizione simile a quella occupata dalle organizzazioni statali»[28]. È lecito però pensare che, se a questo avesse mirato, il legislatore UE si sarebbe espresso diversamente, ma, se così fosse, la tesi qui ipotizzata perderebbe persuasività.

Il vero problema su questo tema pare allora soprattutto risiedere, da un lato, nella non diffusa consapevolezza dell'esistenza di un *do ut des* e dei suoi termini, occultati da

[25] Questi i profili censurati da CGUE, C-61/19, *Orange România SA c. ANSPDCP* (2021) (v. sintesi finale in § 52).

[26] Così invece C. Basunti, *La (perduta) centralità del consenso - nello specchio delle condizioni di liceità - del trattamento dei dati personali*, in *Contr. impr.*, 2, 2020, § 4, 882 ss. (condivisibili invece le riflessioni sulla commerciabilità al § 5).

[27] Conf., nell'interpretazione della libertà del consenso alla luce dell'art. 7, par. 4, GDPR, G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., 98 ss.

[28] F. Caggia, *Il consenso al trattamemto dei dati personali nel diritto europeo,*in *Riv. dir. comm.,* 2019, 425.

complicate clausole di accettazione, che rendono di fatto oltremodo difficile comprendere l'esatto trattamento approvando[29], anche per l'enorme asimmetria informativa tra le parti, cui il GDPR pone limitato rimedio. Dall'altro lato, nella scarsa (spesso: quasi nulla) fungibilità del servizio volta per volta considerato[30]: senza di questo, l'utente si troverebbe spesso tagliato fuori dalle relazioni sociali (soprattutto i più giovani, naturalmente), come ammesso dal BGH tedesco nella decisione cautelare relativa al procedimento antitrust a carico di Fb[31]. Anche questo aspetto incide sul concetto di consenso "libero ed informato". Il timore ragionevole e significativo, di perdere o di non acquisire relazioni sociali significative, può costituire assenza di *free choice*, come ricorda il Consiglio di Europa: «*No undue influence or pressure (which can be of an economic or other nature) whether direct or indirect, may be exercised on the data subject and consent should not be regarded as freely given where the data subject has no genuine or free choice or is unable to refuse or withdraw consent without prejudice*»[32].

Ne segue che il c.d *privacy paradox* (la gente dice di tenere alla privacy ma poi cede spensieratamente i propri dati alle piattaforme e a vari venditori), da molti affermato, in realtà non è poi così paradossale: è invece agevolmente spiegabile, soprattutto con le difficoltà cognitive e l'insignificante potere di mercato che gravano sull'utente.

5. La disponibilità del diritto sui propri dati personali

Il problema potrebbe porsi anche sotto altri profili: se esistano limiti alla disponibilità del diritto sui propri dati personali e, qualora la disponibilità sia ammessa, quando il relativo consenso sia stato validamente prestato.

Sul secondo tema va ricordato (oltre al profilo della libertà, appena ricordato) che il GDPR prevede la specificità del consenso al trattamento e cioè la chiara distinguibilità da quello prestato ad altro scopo (art. 6.1.a - art.7.2). Ipotesi che probabilmente ricorre nel caso nostro, in cui il consenso riguarda il regolamento contrattuale, del quale la cessione del diritto sui dati è una porzione (o meglio, la sola prestazione a carico dell'utente). Se così è, sarà necessario un consenso specifico sul trattamento dei dati a fini promozionali, distinto non solo (probabilmente) da quello sull'operazione contrattuale nel suo complesso, ma anche da quello sul servizio acquisendo. Infatti, anche limitan-

[29] Il che, per vero, ha a che fare con la libertà: il consenso non è pienamente libero, se non è sufficientemente informato.

[30] Soprattutto per l'effetto di rete, in base a cui più sono gli utenti di quel servizio, più è difficile rimanerne fuori: sicché – alzandosi gli *switching costs* per costoro - si alzano pure le barriere all'ingresso per potenziali concorrenti.

[31] Bundesgerichthof, 23 giugno2020, KVR 69/19, §§ 102-10. Sulla vicenda giudiziaria v. il cit. R. Pardolesi-R. van der Bergh-F. Weber, *Facebook e i peccati da Konditionenmissbrauch* (*passim,* spec. 517) nonché A. Giannaccari *Facebook e l'abuso da sfruttamento al vaglio del Bundergerichthof*, entrambi in *Merc. conc. reg.*, 2, 2020, 408 ss., che ricordano essere proprio questo l'abuso di dominanza addebitato a Fb dalla Corte «Evitare Facebook voleva dire in pratica diventare degli eremiti» (T. Wu, *La maledizione dei giganti. Un manifesto per la concorrenza e la democrazia*, Bologna, 2021, 127).

[32] Così l'Explanatory Report (§ 42, p. 20) della "*Convention 108 +. Convention for the protection of individuals with regard to the processing of personal data*", che aggiorna la *Convention for the Protection of Individuals with regard to Automated Processing of Personal Data* del 1981, conosciuta come "Convention 108".

dosi al problema del consenso al trattamento dati, si tratta di due trattamenti distinti: uno per il funzionamento del servizio digitale cercato, l'altro per le finalità promozionali[33]. Tesi seguita dal Consiglio di Stato laddove censura come pratica ingannevole la mancata distinzione[34].

In questo senso va risolta la questione del se sia sufficiente o meno, come base giuridica per la liceità della profilazione, il consenso rilasciato per l'esecuzione del contratto. Nell'ipotesi qui prospettata, infatti, il diritto alla profilazione viene ceduto (o costituito) in capo alla piattaforma, che eroga il servizio digitale: per cui potrebbe dirsi che, costituendone la controprestazione, il consenso al contratto coprisse anche la fruizione della prestazione dell'utente da parte della piattaforma (art. 6, par. 1, lett. *b*), GDPR). Alcuni hanno risposto negativamente. Si è infatti osservato che in tale scenario la disposizione vada interpretata restrittivamente, per cui il consenso ivi cit. coprirebbe solo l'esecuzione della prestazione "caratteristica" cioè quella scambiata col diritto a profilare: altrimenti basterebbe contrattualizzare un qualsiasi trattamento dati per fruire della base giuridica dell'art. 6, par. 1, lett. *b*) GDPR citato[35]. La risposta preferibile, invece, è che sia bensì necessario un consenso distinto per la profilazione, la cui ragione però riposa sulla prescrizione di "specificità".

Allo scopo, è da vedere se sia sufficiente inserirlo nelle clausole sottoposte a doppia firma (*ex* art. 1341 c.c.): e non è detto che la risposta sia positiva.

Le sentenze europee sul punto della validità del consenso paiono essere soprattutto due: C-673/17, *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV contro Planet49 GmbH*, del 1° ottobre 2019 e C-61/19, *Orange România SA contro ANSPDCP*, che si occupa anche dell'onere della prova relativo[36].

Sul primo tema (se esistano limiti alla disponibilità del diritto sui propri dati), al momento parrebbe esatto ritenere che la disponibilità fosse ammessa dall'ordinamento in limiti piuttosto ampi. Non mi sembrano però utilizzabili in tale senso gli accenni alla libera circolazione dei dati presente nel GDPR[37]. Si tratta bensì di interesse decisamente

---

[33] Si v. A. Addante, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, cit., 903 (il consenso al trattamento è un *quid pluris* rispetto alla mera assenza di vizi della volontà di diritto comune, riferita –par d'intendere- all'operazione complessiva o almeno all'acquisizione della controprestazione in contenuti/servizi digitali); G. d'Ippolito, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, cit., 659 (consenso al trattamento dati da servizio digitale è diverso da quello da elaborare in modo massivo, "gestione in monte" potremmo dire circa i big data, per l'invio proprio o di terzi di comunicazioni promozionali); F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impresa*, 1, 2019, 44 (pare distinguere tra consenso contrattuale –e dunque riferito, intenderei, all'operazione economica complessiva o al servizio da ricevere- e consenso al trattamento dati: come Addante, in sostanza); A. Popoli, *L'adeguamento dei social network sites al GDPR: un percorso non ancora ultimato*, in *Dir. inf.*, 2019,1299 ss. (ove si legge che su questo tema si distingue parzialmente - in bene - Google).

[34] Cons. Stato, sent. 2631/2021, cit., § 10, 30.

[35] Così l'interessante lavoro di G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., 69 ss.

[36] Lo evidenzia M.C. Meneghetti, *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in *questa Rivista,* 1, 2021, 266 ss., spec. 272.

[37] Ad esempio l'incipit nell'art. 1, par. 1 e par. 3 oppure l'art. 51, par. 1, GDPR, per cui tra i compiti delle autorità di controllo c'è pure quello di «agevolare la libera circolazione dei dati personali all'interno dell'Unione».

rilevante nell'ambito del reg. medesimo[38]: però, da un lato, costituiscono affermazione generica, e, dall'altro, non precisano il titolo giuridico di tale circolazione (da soggetto a soggetto, parrebbe), limitandosi a menzionarla come fatto oggettivo socialmente desiderabile.

È difficile sostenere che l'effetto di forza legge del contratto (art. 1372 c.c.) prevalga sempre sulla disciplina specifica della *data protection,* ad es. circa i limiti di revocabilità del prestato consenso al trattamento[39]. Servirà allora un coordinamento tra l'esercizio del diritto di revoca/recesso e l'esecuzione dell'operazione contrattuale concordata: che probabilmente comporterà una sospensione (disattivazione) del servizio digitale fruito fino a quel momento. Si tratterà di un caso di recesso *ex lege* (art. 1372, c. 1, cit.) o quantomeno di sospensione dell'esecuzione (il c.c. ne menziona alcuni casi)[40]. Potrebbe anche esplorarsi la via della risoluzione per impossibilità sopravvenuta, a seguito della revoca del consenso: si tratta di via alternativa a quella proposta qui, secondo cui la revoca al consenso vale recesso *ex lege* nel rapporto contrattuale[41].

L'accennata sinallagmaticità porta alla conseguenza per cui il dovere di liceità del trattamento rientra tra gli obblighi contrattuali a carico della piattaforma[42]. La sua violazione dunque costituirà inadempimento contrattuale, con gli effetti conseguenti: al pari di qualunque facoltà pattiziamente concessa, che importi ingresso nella sfera della controparte, la quale non potrà esercitarsi oltre i limiti legali o pattizi posti a tale ingresso (o meglio, posti per il suo esercizio). Anche le regola, posta autoritativamente ad integrazione della pattuizione privata, infatti, concorre a comporre il complessivo regolamento del rapporto contrattuale (art. 1374 c.c.): per cui la sua violazione è appunto violazione di obbligo e non fatto illecito.

Così pure il vizio nel consenso al trattamento, rendendo questo illecito e quindi non più fruibile la prestazione da parte della piattaforma, permetterà a quest'ultima di svincolarsi dal contratto: da vedere se per il medio di vizio genetico (annullamento per errore?) o difetto funzionale (una delle tre risoluzioni), impregiudicata la questione di eventuali danni cagionati dall'utente o all'utente[43]. Tra due parti di paragonabile forza

[38] I due obiettivi del GDPR sono «*to protect "fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" and to guarantee the "free movement of personal data" within the European Union*» per W.G. Voss- H. Bouthinon-Dumas, *EU General Data Protection Regulation sanctions in theory and in practice*, in *Santa Clara High Tech. L.J.,* 37, 2021, 1 ss., spec. 5 (ricordando il considerando 6).

[39] La tesi contraria (prevalenza sempre della *data protection* su quella consumeristica) è stata sostenuta da Facebook nella lite amministrativa contro l'AGCM, allo scopo di sottrarsi alla seconda (pratiche commerciali sleali). Ma è stata rigettata, ora pure in appello: v. Cons. Stato, sent. 2631/2021, §§ 8-9 (e il provvedimento gemello in pari data n. 2630/2021).

[40] Art. 1341; art. 1461; art. 1481 etc. In generale, potrebbe essere ritenuta una condizione sospensiva *ex lege*.

[41] S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit., 188. G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., 184-185, scrive di «diritto di sciogliersi dal contratto per via dell'alterazione della componente patrimoniale dell'operazione negoziale».

[42] Conf. A. Quarta, *Mercati senza scambi. La metamorfosi del contratto nel capitalismo della sorveglianza*, cit., 308-309 (la violazione del GDPR integra difetto giuridico di conformità *ex* direttiva (UE) 2019/770).

[43] Danni a carico della piattaforma, per G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., 178-179. È però da vedere se questo ipotetico errore nella modulazione del consenso sia da imputare solo alla piattaforma: anche se alla fine la risposta dovrebbe essere positiva, alla luce della sproporzione

economica, si rimedierebbe velocemente, integrando il consenso con le dichiarazioni mancanti: è assai dubbio invece che ciò possa avvenire nei rapporti massivi con le piattaforme digitali.
Il tema della conciliazione tra la disciplina da protezione dei dati e quella contrattual-consumeristica meriterà esame approfondito[44].

6. Il recesso e altre conseguenze della contrattualità

Andrebbero indagati poi ulteriori profili discendenti dalla contrattualità (consumeristica): ad es. quelli inerenti all'informativa precontrattuale *ex* art. 49 Codice del consumo (soprattutto circa il prezzo, lett. *e*), ed *ex* art. 51, c. 2, Codice del consumo. Qui il problema è capire se nel concetto di "prezzo" rientri pure il corrispettivo non monetario de quo: parrebbe di no, alla luce del cit. art. 3 dir .770/2019, che distingue nettamente il corrispettivo come prezzo (§ 1) dal corrispettivo consistente in dati personali (§ 2). E in effetti tale è la scelta fatta dall'eurolegislatore con la direttiva (UE) 2019/2161, che ha dovuto aggiungere un § 1 bis all'art. 3 della direttiva (UE) 2011/83 (fonte del cit. art. 49 Codice del consumo), da recepire entro il 28 maggio 2022 (art. 7).
Oppure si potrebbe approfondire il profilo del se tale condotta, laddove oscura la contrattualità nel senso di sinallagmaticità, costituisse pratica commerciale sleale ingannevole, se non addirittura aggressiva[45].
Un cenno ora al recesso. Il diritto di recesso di Facebook (cioè di chiudere l'account) è regolato dalla legge o da contratto. il giudice (§ 4.2) ricorda i casi in cui, secondo le condizioni d'uso, Fb può adottare le cosiddette sanzioni che, in un crescendo di gravità, arrivano alla disabilitazione dell'account come massimo.
Nel caso specifico non è stato invece addotto alcun motivo per la disabilitazione e cancellazione dei dati, tra quelli previsto nelle *terms of service*[46]. Tali non sono stati ritenuti i due addotti in causa: - pretesa indeterminatezza della domanda per l'impossibilità di individuare l'account riferibile all'utente; - l'allegazione di impossibilità di motivare, avendo distrutto il materiale.

di forze economico-cognitive tra le parti e della predisposizione *ex uno latere* delle condizioni di uso.

[44] Già tentato da alcuni interessanti sforzi ricostruttivi: ad es. quello di G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., cap. III, *passim* ma spec. § 4 e di S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, cit. V. pure A. Quarta, *Mercati senza scambi. La metamorfosi del contratto nel capitalismo della sorveglianza*, cit., cap. III, *passim*, 282 ss. e parte IV, *passim.*

[45] A. Addante, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, cit., 915.

[46] Almeno Fb qualcosa prevede, mentre Twitter si riserva poteri di intervento *completely unconditional*: così P. Leerssen, *Cut Out By The Middle Man: The Free Speech Implications Of Social Network Blocking and Banning in the EU,* in *JIPITEC,* 6(2), 2015, § 9 (l'A. poi esamina il contesto giuridico europeo in relazione alla conciliazione dei poteri di *content moderation* delle piattaforme con i diritti fondamentali degli utenti, in primis quello di parola).

7. La distruzione dei documenti (cancellazione dei dati)

La distruzione della documentazione, vero punto nevralgico della lite, secondo il giudice costituisce inadempimento contrattuale, intenzionalmente mirante a provocare danno ingiusto (§ 5.2). Che vi fosse un'obbligazione di mantenere il profilo e il materiale ivi presente, è certo: il giudice lo afferma ma non riporta la pattuizione, anche se in ogni caso ne discenderebbe da interpretazione secondo buona fede[47]. Il dovere di "mantenimento" riguarda la conservazione sia durante la piena operatività del rapporto, sia nelle sue fasi anomale e cioè nel caso Facebook optasse per la disconnessione o a maggior ragione per la sospensione temporanea (la quale potrebbe costituire un'applicazione della regola *inadimplenti non est adimplendum*, se a fronte di violazione dell'utente). Può non essere chiarissimo quando il contratto sia tecnicamente risolto, potendoci essere una disabilitazione non definitiva o comunque una gradualità nella riduzione della prestazione: ma quando fosse invece definitiva, il rapporto contrattuale dovrebbe intendersi giuridicamente risolto.

A quel punto sorgerebbe l'obbligo restitutorio, anche esso governato dalla buona fede, a prescindere dalla sua ricostruzione teorica[48]. Restituzione che, in materia di un servizio digitale di questo tipo, potrebbe dirsi consistere nel dare il tempo all'utente di fare copia dei dati memorizzati[49] e probabilmente anche di metterli a disposizione per il download in un formato fruibile presso analoghe piattaforme[50] (anche per ragioni proconcorrenziali[51], probabilmente, cui è sensibile l'interpretazione di qualunque ramo dell'ordinamento giuridico e quindi anche di quello civilistico).

Al limite, Fb avrebbe potuto limitarsi ad oscurare il profilo per i terzi, conservandolo visibile solo per l'utente (c.d. *shadowbanning*) o comunque ad adottare un rimedio meno drastico[52]. La distruzione invece mi pare inspiegabile, anche in relazione alla lettura "ritorsiva" dell'attore, legata –parrebbe- solo ad una precedente diffida stragiudiziale di costui quale legale di parte (v. poco dopo)[53].

---

[47] Se regolato dal nostro diritto. Ma immagino che analoga regola viga in tutti gli ordinamenti dei paesi occidentali.

[48] È nota la disputa sul se le restituzioni siano governate dall'indebito o dal contratto originario oppure assieme dal contratto e dall'indebito, che ne costituirebbe "cornice sistematica e disciplina residuale" (è la tesi centrale dell'approfondito lavoro di E. Bargelli, *Il sinallagma rovesciato*, Milano, 2010, che affronta la disputa: v. spec. cap. VI e qui sez. II, 449 ss.; il virgolettato è il titolo del § 11 a 458). Anche nel primo caso, infatti, opererebbe il dovere di correttezza *ex* art. 1175 c.c.

[49] Si v. il termine di preavviso posto dall'art. 4 della direttiva (UE) 1150/2019. Anche se questa riguarda il rapporto tra piattaforme e utenti commerciali, non c'è motivo perché analoga regola non viga nel rapporto tra le prime e il consumatore.

[50] Si v. l'art. 20 GDPR sulla portabilità.

[51] Verosimilmente tenute presenti nella redazione della disposizione (conf., direi, G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, cit., 128-129).

[52] Si v. E. Goldman, *Content Moderation Remedies*, in *Michigan Technology Law Review*, in corso di pubblicazione, reperibile in *ssrn.com*, che studia la graduazione dei rimedi possibili, diversi dall'approccio binario *keep up/take down* e intermedi tra i due estremi (parte III), proponendo una policy per le piattaforme, che anche li combini (Parte IV).

[53] Quanti avvocati ci sono che hanno un profilo Fb e al tempo stesso hanno diffidato e/o agito contro la piattaforma? Si pensi non solo all'Italia, ove il contenzioso con essa è limitato, ma a paesi esteri (soprattutto agli USA) in cui è frequente: sarebbe interessante verificare se lì si fossero registrati casi

In ogni caso, anche vi fosse un motivo legittimo di recesso da parte di Fb, questo non avrebbe giustificato la distruzione dei dati, come appena sopra suggerito: effetto discendente sempre dalla buona fede *in executivis*, faro che illumina oscurità e/o lacune contenutistiche del regolamento[54].

8. Risarcimento del danno

Il giudice, poi, passando alla questione del danno non patrimoniale, ricorda è che risarcibile nel caso di violazione di diritti con dignità costituzionale, anche se avvenuta tramite inadempimento di un obbligo, anziché commettendo un illecito aquiliano (§ 7, p. 9). Si tratta in effetti di un insegnamento ormai acquisito[55]. Giustamente, poi, ne afferma la ricorrenza nel caso de quo.

Altrettanto giustamente rigetta l'argomento di Facebook, secondo cui l'utente, se avesse tenuto realmente alla conservazione delle memorie, avrebbe potuto utilizzare la funzione "scarica le tue informazioni". Infatti non può ravvisarsi concorso di colpa, dal momento che non figura nelle condizioni di contratto alcun avvertimento il tal senso. Anche vi fosse stato, poi, un'esecuzione secondo buona fede, che tenesse conto della disparità di asimmetria informativa e di forza economico/organizzativa tra le parti, avrebbe imposto che comunque vi fosse un preavviso da parte della piattaforma[56]. Il giudice ritiene che la protrazione nel tempo (circa dieci anni) dell'attività sul social da parte dell'attore ha prodotto una mole di dati tale, per cui la loro perdita ne ha danneggiato in modo grave e irreparabile la vita di relazione (§ 7, p. 10).

Non è di ostacolo la questione della prevedibilità (da riferire al momento in cui il debitore ha scelto di non adempiere, a dispetto del tenore dell'art.1225 c.c.[57]), poiché, come detto sopra, qui ricorreva il dolo, essendoci la consapevolezza di ledere l'altrui diritto

ritorsivi analoghi. Vien quasi da pensare che sia trattato solo di un banale errore, dopo il quale Fb ha ritenuto più conveniente (per chissà quale motivo: reputazionale?) comportarsi come ha fatto, invece che ammetterlo e scusarsi.

[54] Un *safe harbour* ampio come il § 230 Communications Decency Act tutela in modo quasi illimitato le decisioni sulle restrizioni di accesso (v. sub c.2.A) ed anche se l'oscurato è l'attore (id est chi se ne lamenta), anziché il terzo autore di post illeciti, come solitamente avviene (v. la sentenza *Murphy c. Twitter* del 2021 di cui al mio post *Approfondita sentenza d'appello sulla esenzione da responsabilità per gli internet provider (Twitter) ex § 230 CDA*). Sulla necessità di aggiornare il § 230 c'è un'enormità di scritti, tra cui v. la sintesi di G.M. Dickinson, *Rebooting Internet Immunity*, in *Geo. Wash. L. Rev.*, 89, 2021, 347 (che propone di limitarlo rigorosamente alla moderazione dei contenuti altrui: v. sub III.B., a 390). Tuttavia, non avrebbe protetto dalla responsabilità per distruzione dei dati.

[55] Cass. civ., sez. un., 11 novembre 2008, n. 26973, esaminata ad esempio da V. Tomarchio, *Il danno non patrimoniale da inadempimento*, Napoli, 2009, 112 ss. Anche l'ordinanza qui annotata la ricorda (anzi, ricorda la sentenza gemella in pari data n. 26972/2008, spec. 9).

[56] Dropbox ad esempio chiarisce che l'utente ha trenta giorni dall'eliminazione dell'account, dopo di che i dati vengono; si riserva però di conservarli anche dopo «ove necessario per rispettare ... obblighi legali, risolvere dispute o applicare contratti» (così leggo in A. Quarta-G. Smorto, *Diritto privato dei mercati digitali*, cit., 270).

[57] M. Pacifico, *Il danno nelle obbligazioni*, Napoli, 2008, 143 ss., per il quale la presenza del dolo fa uscire il rapporto dal programma contrattuale per farlo entrare in un contesto aquiliano. L'a. poi ritiene esaurita la funzione storica alla base dell'esclusione del limite della prevedibilità in caso di dolo.

(art. 1225 c.c.)[58]. A parte ciò, si tratta di danni ampiamente prevedibili al momento in cui Fb pose in essere l'inadempimento: da un lato, infatti, Fb sapeva cosa stava memorizzato nei propri server in relazione all'utente de quo e, dall'altro, il danno "relazionale" è agevolmente prevedibile per una piattaforma che ha fatto dell'interconnessione tra le persone la sua *headline* pubblicitaria. La connessione tra utenti, del resto, rientra tra i primari interessi dedotti in contratto che la piattaforma non può ledere, sicchè tutta la vita del rapporto giuridico dovrà tenerne conto[59]: le note differenze socio-culturali tra civiltà occidentali (più individualiste) e orientali (più inclini ad una visione olistica)[60], che astrattamente potrebbero portare ad una soluzione opposta, vengono poi in concreto (ed *in parte qua*) ridotte dall'importanza che anche nelle prime (o almeno nel nostro ordinamento) assume la dimensione relazionale del rapporto giuridico *sub iudice* per l'operare di precise regole giuridiche[61].

Si potrebbe poi discutere se l'art. 1225 andasse applicato anche al danno non patrimoniale, come parrebbe; così del resto ritiene l'ordinanza qui esaminata[62].

È piuttosto interessante l'affermazione, secondo cui, pur essendo l'attore gravato di provare il danno, l'onere qui viene invertito per il principio della vicinanza alla prova: la distruzione dei dati per la decisione di Fb di impedirne la produzione in giudizio[63], infatti, ha reso impossibile l'attività probatoria dell'attore. È interessante, poiché normalmente il criterio della vicinanza alla prova è adoperato per interpretare l'art. 2697 c.c. e cioè per dirimere la questione della corretta distribuzione dei fatti di causa tra i

[58] La consapevolezza propria del dolo, infatti, riguarda la violazione, non le sue conseguenze: «in tema di risarcimento del danno da inadempimento contrattuale, il dolo del debitore che, ai sensi dell'art. 1225 cod. civ., comporta la risarcibilità anche dei danni imprevedibili al momento in cui è sorta l'obbligazione, non consiste nella coscienza e volontà di provocare tali danni, ma nella mera consapevolezza e volontarietà dell'inadempimento» (Cass. civ., sez. II, 17 maggio 2012, n. 7759). Il dettato normativo, del resto, è chiaro; ciò nonostante, taluno richiede anche la consapevolezza di arrecare un danno ingiusto (C.M. Bianca, *Diritto civile. 5 La responsabilità*, Milano, 2019, 173), che comunque qui ricorrerebbe.

[59] E' stato giustamente osservato che vanno tenuti in molta considerazione anche i rapporti tra gli utenti (in orizzontale), anziché solo quello singolo e verticale utente/piattaforma (M. Perel-N.Elkin Koren-G. De Gregorio, *Social media as contractual networks: a bottom up check on content moderation*, in *ssrn.com,* 2021, parte V, 44 ss ma spec. 50 ss.).

[60] V. P. Inghilleri, *I luoghi che curano*, Bari, 2021, 22 ss., 40, 96 (libro che ricorda l'importanza dell'empatia e di una visione relazionale dell'esistenza: *passim*, spec. 46-47 e parti 2 e 3, 83 ss., 110 ss., ove si esplora il concetto di "cittadinanza psicologica"). L'individualismo odierno, contrapposto al personalismo che invece valorizza il profilo sociale dell'uomo (sempre nelle società occidentali), è denunciato (tra i molti) da M. Orlandi, *Norme deboli*, in *Liber amicorum Pietro Rescigno*, vol. II, Napoli, 2018, 1451 ss., §§ 1-4. L'individualismo nemmeno sarebbe coerente con l'interpretazione (costituzionale, essenzialmente) di quel diritto, che potrebbe intendersi invece come massimo campo d'azione della libertà individuale, che è il diritto alla salute, secondo A. Nicolussi, *Beni relazionali e diritto dei rapporti etico-sociali*, in *Teoria e critica dei rapporti etico-sociali*, 2014, § 4, 38 ss. (e senza necessità di appoggiarsi a sostegni trascendenti: spec. 44).

[61] Se il contratto è regolato da legge italiana, permettono ed anzi impongono ciò l'interpretazione e l'esecuzione secondo buona fede (la prima è un complemento della seconda: R. Calvo, *Interpretazione del contratto. Art. 1362-1371*, sub art. 1366, in G. De Nova (a cura di), *Comm. cod. civ. Scialoja Branca Galgano* , Bologna, 2021, 104). Anzi, a ben vedere anche il comportamento, tenuto da Fb prima della stipula, porta a ciò *ex* art. 1362 c.c.: è la pubblicità da essa diffusa a valorizzare la connessione tra utenti.

[62] Spec. 11. Conf. V. Tomarchio, *Il danno non patrimoniale da inadempimento*, cit., 95 ss., applicando la disciplina comune dell'inadempimento.

[63] Così intenderei il passaggio alla pagina 10, pur se ivi compare una coordinazione tra le due frasi, anziché una loro connessione in termini causali, come nel testo.

fatti costitutivi oppure impeditivi/modificativi/estintivi. L'interesse allora sta nel fatto che applica una norma costituzionale (l'art. 24 Cost. appunto) in via diretta, anziché semplicemente per il medio della legge ordinaria tramite una sua interpretazione costituzionalmente orientata oppure tramite un opportuno governo delle clausole generali. L'operazione ermeneutica, pur partendo da un'esigenza condivisibile, suscita perplessità: sarebbe stato forse più lineare arrivare al medesimo risultato liquidatorio semplicemente applicando la determinazione equitativa permessa dall'art. 1226 c.c., senza modificare l'onere probatorio sottostante (lasciandolo cioè a carico dell'attore)[64].

9. La domanda (rigettata) di adempimento contrattuale

Pure interessante è la decisione sulla domanda di adempimento contrattuale, assistita da penale per il ritardo (verosimilmente *ex* art. 614 *bis* c.p.c.). La domanda è rigettata, stante l'impossibilità dichiarata da Fb di procedere al ripristino (ciò in cui sarebbe consistito l'adempimento predetto). Tale impossibilità è stata ritenuta processualmente provata (anche qui) per l'operare del meccanismo della non contestazione *ex* art. 115 c.p.c.: avendolo il resistente allegato, toccava al ricorrente contestarla in modo specifico.

È un interessante portato dell'innovazione tecnologica. L'allegazione di irrecuperabilità dei dati, effettuata da una parte, viene data per buona (cioè ritenuto fatto processualmente provato): sicché il rimedio contrattuale dell'adempimento (e relativa penale) viene escluso sulla sola base di tale allegazione, con la conseguenza di dover optare per quello risarcitorio[65]. Sarebbe in effetti stato probabilmente irragionevole accogliere la domanda di adempimento e farla assistere dal comando della penale: o meglio così sarebbe stato solo dopo un'allegazione provata da parte di Fb in tale senso, mentre sembra di capire che non vi sia stata alcuna prova in proposito (se non il citato meccanismo di non contestazione, che però - come detto - non pare applicabile).

[64] Anche questa complicazione ricostruttiva non supererebbe probabilmente la prova del famoso rasoio. In generale, suscita perplessità la tesi favorevole ad una sorta di "diritto libero", sostanzialmente sganciato dal testo normativo e lasciato alla sensibilità del giudicante, propugnata oggi soprattuttto da Grossi e Lipari: oltre alle riflessioni di Irti, v. ora F. Benatti, *Che ne è oggi del testo del contratto?*, in *Banca borsa tit. cred.*, 1, 2021, § 4.3, 8 ss. Nel nostro caso, però, l'esito non è cambiato. Diverso invece sarebbe stato in un caso come quello, accennato poi nel testo, della responsabilità degli amministratori: la condanna in misura pari alla differenza tra attivo e passivo, in assenza di disposizione di legge e solo sulla base di creazione pretoria, non sarebbe stata accettabile.

[65] Risarcimento del danno da violazione contrattuale, parrebbe. Si sarebbe potuto invocare anche il risarcimento del danno da illecito trattamento *ex* art. 82 GDPR, qualora ciò fosse stato utile: ma non parrebbe, dato che anche il secondo dovrebbe essere un risarcimento in senso tecnico e non un danno punitivo (conf. M. Franzoni, *Lesione dei diritti della persona*, cit., 9). Anche la risarcibilità del danno non patrimoniale, ciò in cui consisterebbe l'espressione "danno immateriale" *ex* art. 82.1 GDPR (C. Camardi, *Note critiche in tema di danno da illecito tratttamento dei dati personali*, cit., 797; E. Tosi, *La responsabilità civile per trattamento illecito dei dati personali*, in *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo codice privacy*, cit., 651), non costituisce un *quid pluris* rispetto ai rimedi previsti per l'inadempimento contrattuale: anche questi, infatti, ormai l'ammettono, come osservato nel testo.

Recensioni

"La despazializzazione della giustizia" Un viaggio critico nella fenomenologia del presente*

Benedetta Cappiello

Sommario

1. Come orientarsi: individuazione della meta. - 2. Prima tappa: nuove forme di dipendenza. Dai Governi ai codici. – 3. Seconda tappa: la socialità come senso appartenenza a-critica. - 4. Terza tappa: il processo monodimensionale. - 5. Quarta tappa: la sentenza…del calcolo aritmetico. - 6. Strumenti per una riflessione critica della nuova fenomenologia della realtà.

1. Come orientarsi: individuazione della meta

L'impressionante sviluppo tecnologico non è più solo questione per tecnici, e Antonie Garapon lo sa bene. Nel suo ultimo volume l'intellettuale francese accompagna il lettore in un percorso oltre i confini dello spazio convenzionale. Oltre i confini, ma non alla ricerca dello spazio che è "aldilà". Tutt'altro. Garapon invita a rimanere nel nostro spazio e nel nostro tempo, rivelando cosa e come è cambiato con l'integrazione di teorie astratte e fenomeni reali, comprensibili da tutti. L'autore intende infatti raccontare la nuova fenomenologia dello spazio che le nuove tecnologie hanno privato di confini e di elementi caratterizzanti, inducendo così a parlare di despazializzazione, parola composta, non a caso, dal prefisso de- e dalla parola spazializzazione. La scelta del primo elemento è di sicuro interesse perché implica una sottrazione, portando così a negare il concetto che segue, ossia la collocazione nello spazio. Ma l'assenza di qualcosa si comprende solo avendo chiaro il suo contrario, ossia la presenza. Ecco quindi Garapon che inizia la sua analisi precisando cosa si intende per spazio, concetto che definisce con sintesi puntuale e assai rigorosa, ricordando che la storia del mondo «è stata scandita da cambiamenti, talvolta brutali, della relazione con lo spazio». L'utilizzo di un elemento della natura, mai usato prima di allora, avrebbe nel tempo favorito nuove relazioni dell'uomo con lo spazio; in passato si trattò della conquista per mare di terre ignote, oggi della conquista di "altri pianeti".

Il concetto di spazio ha da sempre rappresentato una «componente di natura culturale» in evoluzione; e la necessità di definire i confini, di qualificare un luogo, individuandone un sovrano (lo Stato) o un proprietario, è propria dell'essere umano. La definizione dello spazio dà certezza a chi lo vive o lo utilizza. L'uomo di fede prova un senso di serenità quando entra in un luogo sacro così come il laico prova un senso di fiducia e *metus reverentiae* quando entra in un Palazzo di Giustizia. Lo spazio è da sempre accompagnato alla delimitazione – qualificata – di un territorio, e la sua normazione è

*Recensione dell'Opera di A. Garapon, *Despazializzazione della Giustzia*; Mimesis, 2021.

ben definita da Carl Schmitt che precisa che il diritto è la combinazione di *Ordnung*, inteso quale ordine sistemazione regola, e *Ortung* cioè la «determinazione del luogo»[1].
*Recensione dell'Opera di A. Garapon, *Despazializzazione della Giustzia*; Mimesis, 2021.
Ma, come ricorda Garapon, questo processo «di territorializzazione del diritto», intesa quale combinazione di regola e di spazio, si è affievolita fino a perdersi nel corso del Novecento, quando il combinato di territorio e diritto ha iniziato a erodersi. È infatti nell'epoca delle colonie, e dell'evoluzione del diritto umanitario[2] che l'esercizio della giustizia ha "perso" i suoi confini, acquisendone di nuovi che l'hanno resa a vocazione universale[3]. La globalizzazione ha reso poi tutto alla portata di tutti, annullando i confini e attenuando i limiti intrinsechi alla lontananza. Le variabili spazio-tempo non rappresentano più un'incognita per il raggiungimento del risultato. Almeno sul piano strettamente teorico, tutto è diventato alla portata di tutti in tempi assai rapidi.
L'avvento delle nuove tecnologie ha poi portato a un'ulteriore erosione del rapporto spazio-diritto. Per primo Internet ha eroso alcuni principi tradizionali dello stato sovrano, cioè la sovranità dello stesso e la proprietà privata. Lo Stato fatica infatti a imporsi nei rapporti giuridici e sugli accordi che si stringono nell'etere, proprio come il titolare di una privativa rischia di perderla – e di non poterla proteggere – quando il suo bene circola su Internet. Una canzone, uno scritto, un qualsivoglia documento diventano di tutti (e al contempo di nessuno). Internet ha creato uno spazio de-territorializzato e il suo avvento ha segnato la prima grande sfida all'esercizio della sovranità dello Stato e delle prerogative di potere dei governi e delle istituzioni[4]. La rincorsa dello Stato di diritto in questi nuovi territori non geografici, è divenuta ancora più perigliosa con l'avvento e la rapida diffusione delle nuove tecnologie. La rivoluzione del digitale sta così esasperando la dinamica di «autonomizzazione della società civile rispetto allo Stato» con buona pace, probabilmente, di una tutela effettiva e imparziale dei diritti[5].
Oggi Internet non è più una novità ma una nuova sicurezza, al punto che, combinato con i software a intelligenza artificiale e con le tecnologie a registro distribuito, ha favorito una nuova relazione con lo spazio, questa volta despazializzata. Garapon ricorda che il fallimento della geometria euclidea non solo ha favorito la diffusione della metageometria, fondata su postulati estranei a Euclide, ma ha anche, e soprattutto, segnato la fine della geometria come tale. E, proprio perché la geometria rispettava per sua essenza le forme, il vuoto poteva essere colmato solo da qualcosa di nettamente estraneo a queste, 'vestito' di altri simboli, il digitale appunto. E in questo ritroviamo la grande intuizione di Garapon che coglie questa nuova dimensione, riempiendo un concetto tanto astratto di contenuti precisi e distinguibili.
E proprio lui, del resto, elabora il concetto di despazializzazione della giustizia e in un

[1] C. Schmitt, *Le nomos de la terre dans le droit des gens du jus publicum europeaum*, Parigi 2001.

[2] Cfr. M. Sassoli, *International Humanitarian Law Rules, Controversies, and Solutions to Problems Arising in Warfare*, Cheltenham, 2019; R. Kolb, *Advanced Introduction to International Humanitarian Law,* Cheltenham, 2014; D. Fleck (a cura di), *The handbook of International Humanitarian Law,* Oxford, 2013.

[3] A. A. Anderson, *Universal Justice, A Dialectical Approach,* Londra, 1997.

[4] J. P. Barlow, *A Cyberspace Independence Declaration,* 1996.

[5] R. Dworkin, *I diritti presi sul serio*, Milano, 2010.

viaggio in quattro tappe, indaga come la normazione di ciò che è giusto, la battaglia per il giusto e l'esercizio della giustizia sono radicalmente cambiati nella realtà despazializzata.
Il libro può essere quindi tranquillamente definito un viaggio; un viaggio per chiunque sia interessato alla materia, non solo per tecnici, giuristi e addetti ai lavori. Del resto, Garapon intende raccontare di un cambiamento che sta interessando tutti indistintamente. Il lettore è quindi invitato a cambiare il proprio modo - tradizionale - di intendere lo spazio: deve arrendersi all'assenza di limiti, di confini che delimitano un territorio dall'altro; la mia proprietà dalla tua. Il lettore, dal canto suo, deve solo avere la capacità di provare meraviglia, quel sentimento che Metastasio definiva "dell'ignoranza figlia e madre del sapere"[6].
La struttura del libro ben si integra con il fine che l'autore intende raggiungere: presentare le diverse manifestazioni della despazializzazione. La lettura non è lineare, né consequenziale. Come in una spirale, tra concetti astratti e riferimenti colti che rivisitano in chiave digitale il nostro quotidiano, siamo accompagnati in un viaggio attraverso diverse dimensioni che alla fine scopriamo a noi assai prossime. E basta ripercorrere brevemente le tappe (quattro, una per ogni capitolo) di questo fantastico vagabondare, per essere invogliati a compierlo.

2. Prima tappa: nuove forme di dipendenza. Dai Governi ai codici

Garapon parte dal *nomos*, dalle regole, evidenziando che nel passato - in fondo non così remoto - l'uomo trovava la propria definizione in concetti giuridico-spaziali ben definiti. Lo stravolgimento tecnologico ha invece portato l'uomo a cercare un'autodefinizione all'esterno: le «solide cornici del diritto», come le chiama Garapon, sono sostituite da una iper produzione normativa che prescinde da rigide regole procedurali e da un controllo terzo. Nella realtà despazializzata basta saper usare la tecnica e quindi *saper fare di calcolo*, saper programmare, per legiferare.
Il legislatore non deve più sapere di diritto e di principi costituzionali. Il nuovo legislatore è quello che crea i software e i programmi che poi mette a disposizione della massa.
Il digitale si compone di un linguaggio diverso, fatto appunto di codici e di sequenze alfanumeriche. È interessante però notare che cambia il linguaggio ma non la dinamica del rapporto tra il vecchio e il nuovo legislatore e coloro che sono soggetti alla legge: questi ultimi decidono infatti di rispettare qualcosa che non capiscono fino in fondo. Gli utenti del digitale prendono atto della norma, *rectius* delle regole di procedura di un sistema, senza conoscere chi e come le abbia definite. L'assenza di intellegibilità è ancora più forte di quella che in realtà esisteva tra l'uomo della strada, e la norma scritta. Ecco quindi che, come fa notare Garapon, la despazializzazione non muta i bisogni primari (che siano potere, politica, dominio, necessità di governare gli altri), ma ne

[6] Metastasio, Temistocle, atto 1 scena 1.

cambia la grammatica[7].

E proprio in questa nuova grammatica, la massa (di utenti-cittadini) si sente comunque appagata perché esercita la libertà per la quale sin dall'avvento di Internet ha combattuto. La libertà non è più «il libero esercizio di diritti fondamentali» e l'autodeterminazione del sé nella società; tutt'altro. La libertà rappresenta l'indipendenza dei governati dai governanti. Si annullano le istituzioni e per esse, il ruolo dei terzi garanti. La tecnologia fa infatti da garante non solo di buon funzionamento del sistema, ma anche di partecipazione. E sul piano politico, questa estremizzazione della partecipazione trova immagine nella democrazia partecipata. In proposito, Grapon dimostra tutta la sua sensibilità dialettica quando ravvisa che la democrazia partecipata nasconde in realtà il male di privare l'individuo della propria personalità, annichilendone e così portando alla desublimazione di cui già aveva paventato Marcuse[8].

3. Seconda tappa: la socialità come senso appartenenza a-critica

Garapon ritorna, per approfondirlo, sul tema della perdita della personalità quando nel secondo capitolo indaga la despazializzazione della procedura: dall'aula ai social network.

Il lettore è invitato a fare un tuffo nel passato remoto, ai tempi di Omero e della civiltà della vergogna (poi esasperata nella cultura giapponese[9]). In quell'epoca ci si nutriva del riconoscimento sociale, si era parte di un gruppo perché degni di considerazione. E la considerazione arrivava per le gesta compiute e per la vita *retta*. L'individuo esisteva in quanto riconosciuto dagli altri. Garapon porta a riflettere nuovamente sul concetto di vergogna (già nella Grecia Classica sostituito dal senso di colpa, come scriveva E. Dodds[10]) e suggerisce che le nuove forme di aggregazione e partecipazione proposte e promesse dalle nuove tecnologie abbiano favorito il ritorno di questa forma di civiltà, rivisitata. I social network hanno permesso la costituzione di luoghi di aggregazione despazializzati perché appunto privi di alcun riferimento etico, spaziale, procedurale. All'origine i social offrivano una valida alternativa agli «esclusi», ossia a quelli che non avevano voce per dialogare con il potere, e cominciavano a non poterne «più della giustizia a due pesi e due misure». Il passaggio ricorda un po' il ritorno al politeismo: alla voce unica e incontrastata di un solo Dio si sostituiscono quelle di tanti, che vogliono esercitare un potere illimitato[11].

Con il tempo, però, questi non luoghi di aggregazione passiva hanno dato spazio e voce a forme di contestazione fuori controllo. Il carattere "giusto" dell'azione e dell'attacco ha così legittimato la rinunzia a qualsiasi procedura, e risposta. Nei social non è

[7] J. Lassègue, *Some Historical and Philosophical Remarks on the Rule of Law in the Time of Automation*, in B. Cappiello-G. Carullo (a cura di), *Blockchain, Law and Governance,* Berlino, 2019, 59.

[8] H. Marcuse, *L'uomo a una dimensione*, Milano, 1999.

[9] R. Benedict, *Il crisantemo e la spada. Modelli di cultura giapponese,* Bari, 2009.

[10] E. Dodds, *I greci e l'irrazionale,* Milano, 2009.

[11] P. Tillich, *Christianisme et Judaisme,* Gèneve, 2017.

ammessa la prova a contrario e, soprattutto, non si riconosce il principio sacrosanto degli ordinamenti giuridici nazionali e sovranazionale: la presunzione di innocenza. La *cancel culture* assai diffusa nei tempi attuali, favorisce l'attacco di qualcuno, ben noto, che viene travolto dal giudizio di una massa di utenti che muove nell'anonimato. Ed è così che con un *tweet* o un messaggio breve, la reputazione, risorsa oggi "scarsa" può essere distrutta in soli 280 caratteri[12].

L'etica, ossia la distinzione tra ciò che è giusto e ciò che non lo è, si confonde con il diritto. La despazializzazione del social network permette di «dissolvere complesse questioni politiche in cieca certezza morale». E ciò porta anche al paradosso. Garapon ricorda infatti di quando la vittima che diede inizio al movimento #*Metoo* si schierò poi contro il movimento medesimo perché stava favorendo un clima assai pericoloso, innescando sentimenti profondi e nascosti, quasi primordiali, di odio di genere. Ecco quindi che quello che in origine avrebbe dovuto essere uno strumento per integrare è presto diventato uno strumento per deresponsabilizzare[13] i partecipanti che, come «sagome», si uniscono a una battaglia, indipendentemente dal messaggio, ma solo per farne parte. E basta questo a farli sentire appagati. I valori sono quelli decisi da chi lancia la battaglia, e non ci si cura della legittimità, o meno, delle nuove armi (come il *doxing*) con cui viene combattuta. E alla fine è garantito l'applauso del pubblico che si lascia coinvolgere dallo spettacolo, noncurante del messaggio[14].

All'origine di questo modo di partecipare vi era una necessità legittima: il sentirsi integrati. Ma è nella conseguente perdita del controllo e nello sconfinamento in un non-luogo, despazializzato, che Garapon, intuisce e evidenzia il grande rischio della metamorfosi dell'individuo in un'ombra senza volto. E ancora una volta un parallelismo torna alla mente, quello con l'analisi di Hannah Arendt quando racconta della «banalità del male»[15]. Oggi però gli esclusi stanno escludendo chi vorrebbe tornare allo spazio del dibattito e dell'argomentare; la Scuola di Atene è ricordo lontano, ma certo si possono trovare nuovi spazi di aggregazione, formazione, discussione.

4. Terza tappa: il processo monodimensionale

Oggi più che mai, il ritorno ai simboli e allo spazio dedicato al fare giustizia è necessario. Garapon lo sa bene e così nel terzo capitolo parla di despazializzazione del processo. L'autore rileva che anche le regole di procedura, e per esse i principi del giusto e dell'equo processo, sono stati inglobati dal non-spazio. Il processo si è perso non solo nei social network che hanno dato spazio alla giustizia fai da te, ma anche nelle aule di giustizia. Complice la tecnologia e la contingenza pandemica del periodo in cui Garapon scrive, anche il processo si è avvicinato a procedure "più snelle", de-proceduralizzate. Il processo si può svolgere da remoto; il *metus reverentiae*, il senso di piccolo,

[12] L. Blackwell, *An Eye for an Eye: When online Harassment is perceived to be justified,* citato da R. Badourd, *Internet et la brutalisatioon du débat public,* in *La vie des idées*, 6 novembre 2018.

[13] H. Jonas, *Il principio responsabilità. Un'etica per la civiltà tecnologica,* Torino, 2009.

[14] B. Cannone, *Et si le féministes se remettainte à faire la politque,* in *Le Monde,* 2020.

[15] H. Arendt, *La banalità del male*, Milano, 2019.

che provava l'uomo accedendo a un'aula di giustizia è cancellato dal click al link di accesso alla Camera virtuale. La compresenza di persone, corpi, l'unitarietà del processo si annulla nei molteplici fragmenti-clip in cui è spezzettata la procedura on line. Tanti fragmenti quanti partecipanti, ritagliati in riquadri perfetti e di grandezza uguale, che appaiono ora a destra o a sinistra dello schermo. Si muovono seguendo un ritmo e un percorso che è noto solo a chi ha studiato il software. I ruoli si annullano dietro lo schermo: giudice, difensore, imputato hanno lo stesso campo visuale e sono posti sullo stesso piano. Non vi è più la compresenza ad assicurare la disciplina dei corpi (alzarsi, sedersi, salutarsi, stare in silenzio). La tridimensionalità dell'aula si annulla nella monodimensione dello schermo. Si perde anche quel bisogno di «ascoltare coloro che ascoltano» (Jean-Denis Berdin). Il difensore modulava la propria arringa anche in funzione della reazione umana, immediata, della Corte e della Giura. Il processo digitale rende infatti impossibile lo scambio di sguardi che, in passato, responsabilizzava senza essere gratificante. Oggi qualcosa è cambiato, perché lo schermo ci rende tutti uguali, appiattendo qualsivoglia reazione. Ma non solo. La despazializzazione annulla il rituale, la storia, i simboli (il timbro e il sigillo sono oggi una fascetta stampata a margine del fogli). Tutto è calcolato e privo di rituale. Manca lo spettacolo del processo che permetteva di contemplare la tragica condizione umana (l'uomo in manette fa sempre un po' impressione, anche se cattivo) e i tentativi di superarla, mantenendo viva la speranza del mondo. La necessità del radicamento alla tradizione è forte.

La tradizione diventa tale all'esito di un percorso che ha elevato a tale un dato processo, meccanismo, azione; e ciò significa che le tradizioni sono in continua evoluzione. A ogni epoca storica la propria. Fermo il percorso del tempo, occorre però modulare il nuovo, tenendo conto dei principi del vecchio. Ecco quindi che potremmo anche accogliere una parziale e circoscritta despazializzazione del processo a patto però che, come suggerisce Garapon, si propugni «una nuova etica del processo». Le forme servono, anche in una realtà despazializzata. Il rischio è altrimenti l'appiattimento verso ciò che è facile, *n'importe quoi* e verso l'omologazione di ruoli e, ancor più grave, di pensieri.

Garapon è consapevole che questo rischio può colpire anche l'ultima fase del processo, ossia quella del giudizio[16].

5. Quarta tappa: la sentenza...del calcolo aritmetico

Il quarto capitolo presenta così il tema della despazializzazione del giudizio che arriva all'esito di un argomentare logico-giuridico favorendo, legittimandola, la decisione. Argomentare che, in quanto tale, non è immune da vizi al punto che le regole di procedura ammettono l'impugnazione (e talvolta addirittura la revisione) della decisione medesima. La fallibilità umana può dunque essere corretta. La situazione cambia però quando il giudizio è reso all'esito di un calcolo numerico. Garapon avverte e condivide il pericolo di affidare le decisioni a software predefiniti di giustizia predittiva. Parlare di giustizia predittiva è del resto quasi un ossimoro: o ci si affida al vaticinio di una Pizia, oppure la decisione deve formarsi all'esito dello scrutinio di fatti, sussunti e interpretati

[16] A. Garapon, J. Lassègue, *Giustizia Digitale*, Milano, 2021.

alla luce di categorie giuridiche predefinite.
Oggi invece le corti nazionali nei sistemi di common e di civil law si stanno dotando di sofwtare di giustizia predittiva che sarebbero in grado di valutare le chance, ad esempio di recidiva, dell'imputato elaborando i dati di volta in volta inseriti (età, sesso, etnia)[17]. Ecco quindi che la decisione si riduce a un calcolo, eseguito su parametri e dati individuati, organizzati dagli sviluppatori; e dai tecnici informatici. L'azione dell'uomo vien così, come dice Garapon, «inserita in griglie e tabelle». Il software permette quindi di controllare l'incertezza attraverso il calcolo, convertendo le attività umane a una quantità numerica. I non tecnici ignorano però il processo di sviluppo e di funzionamento del software; subiscono solo il risultato.
Come per il giudizio umano, anche la predizione può essere sbagliata magari perché proprio il programma è stato costruito adottando un modello errato, ovvero inserendo i dati in modo confuso o deformato all'origine. È il caso, ad esempio, di COMPAS il sistema di giustizia predittiva adottato da alcune Corti americane e che presto ha dimostrato di "essere" razzista. La colpa non era però del sistema, ma dei dati inseriti che risalivano a un periodo storico in cui le condanne per recidiva di uomini di etnia afro-americana erano più numerose di quelle di imputati di etnia bianca. Forse i neri erano più pericolosi o forse, anzi sicuramente, COMPAS era "manipolato" da un sostrato di razzismo inespresso. Tra COMPAS e il giudice vi è però una differenza non marginale: la decisione viziata di un giudice può essere impugnata mentre quella a firma COMPAS rischia di rimanere inappellabile. Non vi è modo, infatti, di risalire al vizio logico che ha portato alla conclusione viziata. In teoria, si potrebbe risalire alla responsabilità dei programmatori; loro, però, sono tecnici cui non si può chiedere molto di più della definizione del programma. Al giudice, viceversa, si può e si deve richiedere il rigore del giudizio.
«L'operazione di verità», come la chiama Garapon, passa dunque attraverso i numeri non più il linguaggio. La giustizia predittiva esaspera il ruolo delle cifre, che si sostituiscono all'essere la realtà[18]. Il calcolo ha però un limite intrinseco: l'evento non è spiegato e non ne viene colto il significato. Esso è semplicemente incasellato nel riquadro giusto della griglia predefinita.

6. Strumenti per una riflessione critica della nuova fenomenologia della realtà

Le espressioni della realtà despazializzata incontrate nel viaggio lasciano il lettore con un certo disagio, soprattutto verso quella parte di tecnologia che non se ne può cogliere con l'intelletto. I numeri, del resto, sono per pochi.
Il viaggio in cui ci guida Garapon è intenso, perché si concentra (e approfondisce) solo ~~su~~ alcune manifestazioni della despazializzazione: norme, procedura, processo,

[17] Cfr. Mesure judiciare d'investigation educative (MJIE), distribuisce punti positivi e negativi concentrandosi sui rischi relativi a un minore; si tratta di un *"dispositivio scientifico di ricerca-azione"*. COMPAS, Correctional Offender Management Profiling for alternative Sanctions.

[18] E. Sadin, *Critica della ragione artificiale,* Roma, 2018.

decisione. Il viaggio partito dalla necessità di esplorare il fenomeno della despazializzazione, si conclude con il riconoscimento che questo fenomeno è espressione polimorfa della realtà in cui tutti viviamo. Ma in conclusione, spunto di riflessione positivo, l'autore ci ricorda che «la conversione del mondo in indicatori, cifre, è collocata in un processo storico di ben più lunga durata». Il senso di sacro e di ignoto che avvolge i numeri è proprio dell'essere umano. Con l'avvento del digitale si è aperta una nuova e ulteriore fase che deve essere ancora conosciuta, capita e quindi inquadrata. Le cornici del diritto non possono essere sostituite da griglie. Tutt'altro. Le griglie devono essere costruite nel rispetto delle cornici del diritto, che poi non sono altro che le espressioni dei principi e dei valori della tradizione del presente. E in questo processo di ricomposizione ordinata della realtà in numeri, occorre coinvolgere i più, per evitare di generare un nuovo senso di emarginazione che, se estremizzata, porta a rifiutare anche il senso più genuino di giustizia.

La despazializzazione della giustizia

Antoine Garapon

Mimesis
Anno di edizione: 2021
Pagine: 176
ISBN: 9788857577661

Recensione a Gianpaolo Maria Ruotolo, *Scritti di diritto internazionale ed europeo dei dati*, Cacucci Editore, Bari, 2021, Collana di Studi sull'integrazione europea

Giovanna Naddeo

È noto come la diffusione di Internet abbia innescato un'autentica rivoluzione copernicana, determinando la nascita di questioni giuridiche di stringente attualità strettamente connesse alla tutela di diritti e libertà fondamentali. L'antico *gap* tra diritto e sviluppo tecnologico è acuito dalla crescita costante del volume di dati trattati, oggetto di circolazione e commercializzazione, oltre che attributi fondamentali dell'identità personale.

Nell'ormai ampissimo panorama dottrinale sull'argomento, si distingue l'ultima opera del Prof. Gianpaolo Maria Ruotolo dedicata alla regolamentazione dei dati informatici nel diritto internazionale ed europeo; trattasi di un percorso politematico volto ad approfondire istituti e modelli giuridici all'apparenza distanti (*e.g.* commercio elettronico, *transborder data access* nei procedimenti penali), oggi accomunati dall'impiego sempre più pervasivo e invasivo delle tecnologie digitali e, dunque, della loro imprescindibile "materia prima", i dati appunto (personali e non).

Lungi dall'essere un ennesimo "Manuale sulla privacy", l'opera fornisce un quadro complessivo dello stato dell'arte relativo alla regolamentazione dei dati informatici in contesti diversificati, regolamentazione che, a causa della natura ontologicamente transnazionale della Rete e delle fattispecie che vi si realizzano, ha luogo per il tramite di norme di diritto internazionale e, nel nostro contesto regionale, europeo.

Tale prospettiva rappresenta, al contempo, un osservatorio privilegiato su questioni di primo piano nell'ordinamento internazionale contemporaneo, tra tutte quella relativa all'emersione di procedimenti decisionali, forme di cooperazione con attori non statali e strumenti normativi del tutto "atipici" ascrivibili al fenomeno del cd. *informal international lawmaking (IN-LAW)*.

Il taglio innovativo del volume emerge iconicamente sin dalla copertina, con un tributo alla matita di Jack Kirby tratto da una scena del fumetto "*Challengers of the Unknown*" nel quale i quattro eroi protagonisti lottano contro Ultivac, un *robot* capace di pensiero autonomo ribellatosi al suo costruttore, uno scienziato dell'ex Germania nazista.

L'impianto *full circle* dell'opera (supportata da una robusta bibliografia e da una ricca casistica giurisprudenziale nazionale e sovranazionale), muove dalla progressiva erosione del ruolo della Comunità Internazionale nella gestione di quel *global public good* che è Internet fino al crescente peso dell'attività para-legislativa e para-giurisdizionale posta in essere da soggetti privati in materia di tutela e bilanciamento tra diritti fondamentali nel cyberspazio (è lo stesso Autore a proporre il caso dell'*Indipendent Oversight Board* di

Facebook, organo collegiale di controllo istituito dallo stesso *Facebook* al quale gli utenti possono appellarsi per lamentare l'indebita rimozione dei propri contenuti).

Ed è in tale scenario che si inseriscono questioni in materia sia penale che civile di indubbia centralità nell'attuale dibattito giurisprudenziale e dottrinale con riguardo alle nuove frontiere del progresso tecnologico.

Il tema dell'acquisizione extraterritoriale di dati archiviati su *server* situati all'estero, e dunque la questione della competenza ad adottare provvedimenti autoritativi nell'ambito di procedimenti penali (cd. *transborder data access*) va inquadrato come un'ipotesi di conflitto tra entità statali dotate di autonoma *jurisdiction*, qualificandosi, in via potenziale, come un caso di violazione del rispetto della sovranità territoriale dello Stato di allocazione dei dati. Pertanto, come sottolinea l'Autore, «l'unica modalità di esercizio internazionalmente legittimo del transborder data access implica l'acquisizione, preventiva o quanto meno successiva, del consenso del sovrano territoriale competente, in una forma generale o specifica».

A tal proposito, l'art. 32 della Convenzione del Consiglio d'Europa sulla criminalità informatica consente agli Stati che l'abbiano ratificata l'accesso transfrontaliero ai dati disponibili al pubblico («*open source*») o a quelli rispetto ai quali sia stato ottenuto «*the lawful and voluntary consent*» della persona autorizzata a divulgarli, qualora siano conservati su *cloud server* collocati sul territorio di altro Stato Parte, senza che a tal fine sia necessario chiedere un'autorizzazione *ad hoc* a quest'ultimo.

A detta dell'Autore in tale circostanza il consenso dello Stato in questione «risulta esse stato già espresso in occasione della ratifica della Convenzione, la quale costituisce, dunque, il titolo di legittimazione internazionale dell'attività transfrontaliera».

Alla luce della lacunosità del sistema convenzionale che, nel caso di conflitto di giurisdizione, non prevede meccanismi di riparto della competenza all'azione penale ma deferisce la questione a meri obblighi di cooperazione tra le altre Parti contraenti, al fine di stabilire la competenza più appropriata per esercitare l'azione penale, l'Autore rilancia la proposta di un approccio del tutto sganciato da ogni riferimento territoriale o personale, con riguardo al criterio del cd. *power of disposal* in virtù del quale una data autorità nazionale, in casi preventivamente individuati, avrebbe accesso legittimo ai dati, ovunque detenuti e indipendentemente dalla nazionalità del loro titolare, conservati su un *cloud* di cui fosse riuscita ad ottenere, in modo legale le credenziali di accesso, senza la necessità di chiedere la collaborazione del loro titolare o del fornitore del servizio di *cloud.*

Nell'ambito, invece, dell'attività normativa in materia di scambi commerciali via Internet in seno alle principali organizzazioni internazionali (WTO, NU, OECD), particolare attenzione è rivolta all'UE e al suo mercato unico digitale - inteso quale nuova frontiera del processo di integrazione - a fronte non soltanto della mera appartenenza geografica, bensì del peculiare obiettivo europeo, in un ambiente giuridico stabile, trasparente e affidabile, di una crescita economica radicata sul rispetto dei diritti fondamentali.

Facendo il punto sui risultati positivi finora ottenuti come l'abolizione delle tariffe di *roaming*, la portabilità transfrontaliera dei servizi di contenuti *online* e il divieto di blocchi geografici ingiustificati, una dettagliata esegesi è riservata al Regolamento 524/2013/

UE relativo al sistema di risoluzione extragiudiziale delle controversie *online* (cd. *online dispute resolution, ODR*) nell'ambito di contratti di vendita o di servizi conclusi tra consumatori residenti in Stato membro e professionisti stabiliti nell'Unione alla luce del suo esplicito scopo di «contribuire, mediante il raggiungimento di un livello elevato di protezione dei consumatori, al corretto funzionamento del mercato interno, in particolare della sua dimensione digitale» (art. 1), ferma restante la possibilità di adire l'autorità giurisdizionale nell'esercizio del diritto a un ricorso effettivo e a un giudice imparziale *ex* art. 47 della Carta dei diritti fondamentali dell'Unione.

Strumentale allo sviluppo del mercato ma anche a una maggior efficienza nel settore pubblico è l'impiego dei cd. *big data*, ossia agglomerati di dati (personali e non) gestiti e trattati in blocco mediante algoritmi informatici per l'individuazione di correlazioni, tendenze e modelli, ai quali l'Autore dedica ben due capitoli, l'uno in merito ai profili di diritto sostanziale, l'altro a quelli di diritto "processuale", ponendo sotto la lente di ingrandimento questioni giuridiche per certi aspetti inedite relative tanto ai pericoli, derivanti dal loro utilizzo, per il buon funzionamento del mercato (distorsione della concorrenza, sfruttamento abusivo di posizione dominante, forme di discriminazione indiretta dei gruppi di persone accomunate dall'appartenenza a *dataset*), quanto alla necessità di individuare forme di tutela individuale o collettiva degli interessati. Muovendo da un'interessante approfondimento dei meccanismi di ricorso collettivo e della tutela degli interessi dei gruppi nella giurisprudenza delle Corti di Strasburgo e Lussemburgo, alla luce delle difficoltà connesse alla determinazione della legittimazione ad agire in sede giurisdizionale, la proposta dell'Autore (sul modello della Raccomandazione 2013/396/UE della Commissione) va nella direzione dell'individuazione *ex ante* di organizzazioni legittimate ad avviare azioni rappresentative di una pluralità di individui con interessi comuni per la tutela dei confronti dei *big data*; in alternativa, l'ulteriore soluzione prospettata fa riferimento alla costruzione di un sistema di risoluzione extragiudiziale sulla falsariga della piattaforma ODR.

Ampio spazio è successivamente dedicato al bilanciamento tra i diritti di proprietà intellettuale (art. 17, par. 2, della Carta dei diritti fondamentali e art. 1 del Protocollo 1 alla CEDU) con altri diritti parimenti fondamentali come quelli di informazione ed espressione nell'ormai consolidata giurisprudenza delle Corti di Strasburgo e Lussemburgo, nonché alle novità normative di diritto derivato in materia di copyright (il riferimento è alla discussa direttiva (UE) 2019/790) finanche al profilo della responsabilità degli *host/provider,* oggetto di attuale discussione a seguito delle due proposte di Regolamento in materia di servizi digitali e responsabilità delle piattaforme (il "*Digital Services Act*") e di competitività del mercato europeo nel settore digitale (il "*Digital Market Act*"), nonché nei sempre più frequenti casi di "censure private" autonomamente predisposte dalle piattaforme a seguito di episodi di *fake news* ed *hate speech* (in tale contesto si inserisce l'analisi delle tre ordinanze cautelari con le quali il Tribunale di Roma ha deciso in modo opposto casi analoghi in cui *Facebook* ha disattivato le pagine di due associazioni politiche di estrema destra, *CasaPound* e *Forza Nuova*).

Sullo sfondo del volume la questione (di indubbia centralità nel contesto attuale segnato dalla pandemia da Covid-19) relativa alla qualificazione del diritto di accesso a Internet (inteso come *final global public good*) come diritto fondamentale "autonomo"

oppure come strumento (*intermediate global public good*) per garantire l'effettivo esercizio ad altri diritti nella dimensione del web*:* una questione quest'ultima ritornata in auge nell'ultimo periodo anche nel contesto nazionale con l'idea di costituzionalizzare il diritto di accesso a Internet mediante l'inserimento di un art. 21-*bis*, in termini di libertà di espressione, o di un art. 34-*bis*, inteso come diritto sociale.
In conclusione, l'opera rappresenta un aggiornato strumento di studio e di approfondimento di tematiche giuridiche del tutto innovative e, per certi aspetti, inedite afferenti alla dimensione digitale, distinguendosi per organicità sistematica e rilevante chiarezza espositiva, supportata dai numerosi rinvii e collegamenti interni. Scontato è l'auspicio di un secondo volume che possa seguire gli sviluppi delle magmatiche questioni sin qui proposte e quelle future con riferimento all'evoluzione legislativa e giurisprudenziale del regime giuridico dei dati nel contesto europeo ed internazionale.

Scritti di diritto internazionale ed europeo dei dati
Gianpaolo Maria Ruotolo

Cacucci Editore
Anno di edizione: 2021
Pagine: 320
ISBN: 9788866119838

Elenco autori

Lorenzo Albertini
avvocato in Verona
Juan Francisco Sánchez Barillao
professore ordinario di diritto costituzionale, Universidad de Granada
Marco Bassini
avvocato in Milano
Sofia Braschi
assegnista di ricerca in diritto penale, Università di Pavia
Benedetta Cappiello
ricercatrice in diritto internazionale, Università di Milano
Valentina De Nicola
avvocato in Venezia
Camilla Della Giustina
cultrice della materia in diritto costituzionale, Università degli Studi di Padova
Giusella Finocchiaro
professore ordinario di diritto di Internet e diritto privato, Università di Bologna
Hu Guiping
dottoressa di ricerca in pedagogia e collaboratrice ed esperta linguistica, Università di Bologna
Alessandro Lauro
dottorando di ricerca in diritto, persona e mercato, Università Ca' Foscari Venezia
Milena Mursia
avvocato in Milano
Giovanna Naddeo
dottoranda di ricerca, curriculum internazionalistico-europeo-comparato, Università di Salerno
Valerio Natale
avvocato in Roma
Laura Ninni
avvocato in Milano
Federica Paolucci
LL.M. candidate, Law of Internet Technology, Università Bocconi
Oreste Pollicino
professore ordinario di diritto costituzionale, Università Bocconi
Giulia Priora
assegnista di ricerca, Scuola Superiore Sant'Anna - Istituto DIRPOLIS (Diritto, Politica e Sviluppo)
Maria Luisa Stasi
senior legal officer, Article 19
Carmine Trovato
avvocato praticante in Milano
Silvia Vimercati
assegnista di ricerca in diritto costituzionale, Università di Milano - Bicocca

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

mediaLAWS

ANNO 2021 - CODICE ISSN 2532-9146