mediaLAWS

Rivista di diritto dei media
3/2020 ottobre

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

ANNO 2020 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Indice
Index

Editoriale

Saggi
Innovazione, diritto e tecnologia: temi per il presente e il futuro

Altri saggi

Note a sentenza
Sezione Europa

Sezione comparata

Sezione Italia

Commenti
Forum – *Schrems II*

Indice
Index

Editoriale

Articles
Inovation, law and technology: present and future challenges

More articles

Notes and comments
Europe

Comparative Law

Italy

Debates
Forum – *Schrems II*

Su determinazione della direzione, in conformità al regolamento della Rivista, sono stati sottoposti a referaggio anonimo ovvero a referaggio anonimo a doppio cieco, come indicato in calce a ciascun contributo, i saggi di: Sofia Braschi, Giacomo Capuzzo, Massimo Foglia, Daniele Imbruglia, Elena Kaiser e Sofia Monici, Enrico Labella, Silvia Martinelli, Carla Pernice, Serena Quattrocolo, Agostino Sola, Andrea Venanzoni, Lavinia Vizzoni.

Editoriale

I network oscurano Trump: lezioni di giornalismo davanti alle menzogne del potere

Carlo Melzi d'Eril - Giulio Enea Vigevani

Una domanda corre sottotraccia in molti dibattiti sui "diritti e doveri" del giornalista: la stampa ha il dovere di diffondere qualunque messaggio proviene da una figura di rilievo pubblico, poiché ciò è di interesse della comunità di riferimento o un giornalismo serio consente, a volte impone, di compiere scelte, come quella, ad esempio di interrompere la diretta di un comizio, per impedire la diffusione di palesi falsità?

Questa domanda ricorrente è tornata di recente d'attualità. Nello spettacolo eccitante ma insieme penoso del dopo elezioni americane, abbiamo assistito a quella che può essere a buon diritto ritenuta una nuova pagina storica del giornalismo, statunitense e non solo.

Ricordiamo che cosa è accaduto: la notte tra il 5 e il 6 novembre, quando si era ancora nel pieno del conteggio dei voti, il presidente Trump indiceva una conferenza stampa (meglio, un monologo senza domande) nella quale affermava di aver vinto le elezioni «se si contano i voti legali». Tre tra i maggiori canali televisivi - MSNBC, NBC e CBS – hanno deciso di interrompere la diretta, giustificando un simile atto con la volontà di non trasmettere notizie false. Alcuni, poi, hanno stigmatizzato il comportamento dell'uomo politico, che li "costringeva" a limitarne la visibilità: L'anchorman della MSNBC, Brian Williams, ha ritenuto di rendere la propria amarezza esplicita: «ci troviamo ancora nella posizione inusuale non solo di interrompere il presidente degli Stati Uniti ma di correggere il presidente degli Stati Uniti. Non ci risulta una vittoria di Trump». Lester Holt su NBS ha spiegato così la sospensione della trasmissione: «il presidente ha fatto un certo numero di affermazioni false, compresa quella che c'è stato un voto fraudolento. Non ci sono prove». Ancora, Shepard Smith, volto della CBS, si rifiutava di proseguire la diretta in quanto «non c'è stata una scintilla di verità in tutto quello che ha detto».

Diversa la scelta della CNN, che ha continuato a trasmettere e subito dopo ha pubblicato un lungo articolo con l'elenco delle affermazioni false diffuse dal presidente, ognuna accompagnata da una puntuale smentita. Tuttavia, al termine del discorso presidenziale, Jake Tapper, corrispondente da Washington, si è lasciato andare ad un commento scoraggiato: «che triste notte per gli Stati Uniti sentire il presidente che dice certe cose, bugia dopo bugia, sull'elezione rubata, cercando di attaccare la democrazia. Non ci sono prove di quello che sta dicendo. Solo diffamazioni sulla correttezza nel conteggio dei voti. Francamente è patetico».

Ancora differente la condotta di the Fox News, che ha trasmesso il filmato senza aperte contrapposizioni. Tuttavia, persino su una emittente notoriamente vicina alle

posizioni della destra americana, la conduttrice Martha MacCallum, ha preso atto delle accuse di Trump, sottolineando che le prove citate per dimostrare le frodi nella votazione «dovranno essere prodotte, se davvero ce ne sono».

Ora, nel generale biasimo mostrato dal mondo del giornalismo di fronte a una *public figure* (anzi forse alla *public figure* per antonomasia) che diffonde dati falsi o comunque non provati, circa una condotta gravissima come l'esistenza di brogli elettorali, le scelte sono state diverse. Da un blando ammonimento a mostrare le prove di una simile accusa, alla contestazione puntuale delle affermazioni dopo averle comunque diffuse, alla scelta più radicale di non diffondere una voce, soprattutto se così autorevole, quando si fa interprete e assicura la sussistenza di fatti di cui non si ha alcuna evidenza.

La scelta di staccare la spina a uno dei politici più influenti al mondo può essere opinabile per più di un motivo. Proviamo ad elencarne qualcuno. Escludere dal dibattito pubblico, o meglio dai media tradizionali, cioè dagli organi ove l'informazione è presentata e commentata da giornalisti, una personalità con un largo consenso, anche quando diffonde fatti falsi, probabilmente non la condanna al silenzio che meriterebbe. Il filmato, infatti, continua a circolare su circuiti informativi alternativi – in particolare nelle bolle mediatiche di cui tanto ha parlato Cass Sunstein - dove tali voci accedono comunque al "loro" pubblico, in costante adorazione, senza un briciolo di contraddittorio. E, anzi, sventolando, come se fosse una medaglia al valore, lo stigma del martirio, che rischia addirittura di aumentarne la popolarità, in determinati contesti.

Ancora, il principio liberale, cui siamo tanto affezionati, del «conoscere per deliberare» suggerisce di consentire l'accesso ai media di tutte le idee, anche le più irritanti e scioccanti, persino di quelle antidemocratiche e finanche di quelle che affondano e nutrono le proprie radici nelle paludi di falsità conclamate. La fiducia nella capacità delle persone di scegliere non solo l'idea migliore ma anche di espellere quella peggiore e di riconoscere quella basata su fatti falsi, in un sistema pluralista, consente di mantenere intatta una simile libertà. E ciò per di più in un ordinamento come quello statunitense (o come il nostro) nel quale nel quale i "padri fondatori" riponevano un tale credito nella forza della democrazia e nell'attaccamento ad essa della popolazione, da estendere la libertà di espressione anche ai nemici della democrazia, come si dimostra essere, in modo più subdolo di altri, chi non ne accetta le regole se non quando lo vedono prevalere.

Corollario di quella precedente è l'ultima obiezione alla interruzione della trasmissione. Evitare di diffondere per intero un discorso così importante come quello del presidente Trump, in frangente così drammatico, come quello della notte dello scrutinio elettorale, durante la quale il presidente accusa, senza riscontro alcuno, il proprio avversario di averle illecitamente condizionate, priva i cittadini della possibilità di conoscere ogni passaggio, ogni sillaba, ogni accento del suo pensiero e quindi, con ciò, di poterlo giudicare adeguatamente.

Tutte queste critiche sembrano a prima vista ragionevoli e portano con sé argomenti che, soprattutto se astratti dal contesto, potrebbero essere convincenti.

Tuttavia, proprio se ci si cala nel contesto, la scelta dei tre grandi network può essere ritenuta certo non doverosa, ma nel complesso comprensibile e forse anche apprez-

zabile.

Dicevamo "non doverosa". Il dubbio potrebbe legittimamente porsi: in quel particolare momento una presa di posizione così dura ("ho vinto le elezioni, il mio avversario me le ha rubate"), totalmente sfornita di alcuna prova, poteva rischiare di essere interpretata come una istigazione alla rivolta, condotta evidentemente eversiva. La intima convinzione circa la maturità della democrazia americana convince a ritenere che, in verità, nessun colpo di Stato poteva concretamente avere luogo, sicché la libertà di espressione, non limitata da questo argine, può prendersi tutto lo spazio, rendendo legittima quindi l'attività di chi, invece di "togliere la linea" al presidente, ha diffuso l'intero discorso.

Perché la condotta di chi ha ritenuto di bloccare la diretta ci sembra, tuttavia, meritevole di plauso?

Anzitutto perché davvero non si può parlare di atto censorio. Ormai, come si è accennato sopra, i dati, i fatti, ciò che accade, insomma le notizie sono veicolate attraverso moltissimi canali diversi, soprattutto messi a disposizione della rete. Il discorso del presidente degli Stati Uniti, in particolare in un momento in cui tutto il mondo volge lo sguardo oltre oceano, viene senza dubbio registrato integralmente da qualcuno e, una volta immesso in rete, diventa raggiungibile da chiunque.

L'informazione, dunque, e questo è un fatto che difficilmente può essere messo in discussione, non passa più soltanto attraverso gli organi di stampa, che quindi possono permettersi, ancor più che una volta, di concentrarsi sulla opera di mediazione che è loro propria e che ci sembra essere, oggi più che mai, l'*ubi consistam* del giornalismo.

Inoltre, come ha sottolineato Antonio Nicita, «secondo una consolidata prassi, sono proprio le principali emittenti televisive americane a decretare, con le proprie proiezioni statistiche sullo spoglio, gli stati assegnati a uno dei contendenti», sono i notai del voto e non possono assistere passivamente a dichiarazioni false circa l'avvenuta vittoria elettorale, senza abdicare al proprio ruolo terzo di certificatori del risultato (A. Nicita, *Perché interrompere quella conferenza stampa di Trump non è censura*, in *Wired.it,* 10 novembre 2020).

Vi è di più: con questo atto dirompente, il giornalismo compie una sorta di scatto d'orgoglio, rivendicando la propria natura più profonda. Con lo spegnere l'interruttore della autopromozione, i conduttori che l'hanno deciso hanno anzitutto rifiutato di essere la cassetta delle lettere (meglio dei video) del potere politico.

I programmi di cronaca e approfondimento politico, poi, hanno dimostrato di voler restare uno spazio mediato, filtrato da chi esercita appunto il mestiere del giornalista. Essenza del mestiere è anche prendersi la responsabilità di decidere che cosa agli spettatori si debba dire e che cosa agli spettatori si possa o si debba tacere, in un clima, come è accaduto in questo caso, di piena trasparenza. Si spegne il microfono, spiegando il perché. Ed è proprio in questa spiegazione che sta un esempio del valore in più che ogni giornalista e ogni testata può fornire al lettore o allo spettatore, oltre al mero racconto dei fatti. Anzi, si potrebbe dire che questo è il vero racconto: non una mera telecamera fissa e muta, ma un'opera di regia che, partendo dal fatto poi lo integra con un contesto e una spiegazione. Nel compiere questa opera, che è appunto il mestiere del giornalista, si distingueranno la capacità e lo stile di ogni professionista, che ne

dovrebbero decretare il successo o l'insuccesso.

Prendendo a prestito un'immagine utilizzata da Claudio Schirinzi, per anni cronista del Corriere della Sera, le agenzie (o la realtà) ti forniscono gli ingredienti, poi sta al giornalista cucinarli.

In fondo, proprio l'intermediazione giornalistica distingue e distinguerà sempre più un organo di informazione dalle miriadi di canali attraverso cui passano dati e opinioni tramite la rete. E intermediazione significa non solo e non tanto fornire il dato, ma anche, tra l'altro, operare un controllo accurato delle fonti e una verifica maniacale dei fatti e fornire un argine alla propalazione di dati falsi senza contraddittorio. Proprio nell'era della iperinformazione, l'autorevolezza del giornalismo si misura non nella quantità ma nella qualità delle notizie, nella capacità di fornire strumenti per capire la realtà e non armamentari propagandistici.

Questo evento segna un passaggio nel giornalismo, una presa di coscienza del ruolo e della responsabilità di una professione che forse troppo presto era data per morta di fronte all'avanzata dei social, e che invece oggi ha "battuto un colpo". E un colpo forte.

Certo, questo accade nel mondo anglosassone dove, per citare uno tra gli episodi più noti, più di vent'anni fa il conduttore della BBC Jeremy Paxman ripropose a un politico reticente per 14 volte la stessa domanda.

Speriamo sia di buon auspicio perché anche in Italia il mondo dell'informazione alzi la testa contro politici che non accettano domande insidiose, rifiutano il contraddittorio, mettono veti sui giornalisti sgraditi, inviano dichiarazioni preregistrate, eccetera, eccetera, eccetera.

Saggi

Focus: innovazione, diritto e tecnologia: temi per il presente e il futuro

Introduzione

Bianca Gardella Tedeschi - Shaira Thobani

Questa raccolta di saggi prende l'avvio da un progetto europeo, il progetto Erasmus + TechLaw Clinics, di cui l'Università del Piemonte Orientale è partner insieme all'Università Cattolica di Lione, che è capofila, all'Università di Radboud, all'Università di Cracovia e all'Università di Lodz. Scopo del progetto è quello di avvicinare gli studenti e le studentesse alle nuove tecnologie per stimolare la ricerca di soluzioni giuridiche da applicare alle nuove tecnologie. Le TechLaw Clinics si sviluppano quindi in tre fasi. Nella prima, ciascun ateneo organizza una formazione specifica sulle nuove tecnologie e i diritti; la seconda prevede la partecipazione a moot courts su casi pratici di diritto civile predisposti dai colleghi delle università partner; infine, tutti gli studenti dei diversi atenei si ritrovano in un'unica sede per condividere ed ampliare il percorso di apprendimento in chiave comparatistica. Il percorso nasce interdisciplinare e vede coinvolti, oltre che studenti di giurisprudenza, anche di management, economia e ingegneria. La rivista Media Laws ha deciso di ospitare in un volume monografico le lezioni e i seminari giuridici che abbiamo organizzato per gli studenti del Piemonte Orientale, come prima tappa in questo percorso di formazione dedicato alle nuove sfide tecnologiche.

La scelta degli argomenti da proporre agli studenti non è stata semplice, per l'ampiezza del tema e dei diversi approcci metodologici. Abbiamo quindi deciso di offrire a studiosi, non necessariamente specialisti negli argomenti proposti, alcuni esempi particolarmente significativi di come l'innovazione tecnologica abbia di per sé portato alla necessità di rivedere le categorie giuridiche tradizionali, testandone l'elasticità.

A conclusione del percorso formativo, abbiamo potuto seguire, attraverso gli interventi dei diversi relatori, alcune tematiche che caratterizzano ormai il rapporto tra il diritto e lo sviluppo della tecnologia.

A fronte del dirompere della tecnologia, è innanzitutto necessaria una premessa metodologica su come il diritto deve porsi davanti al nuovo. Così, dinnanzi all'emergere dell'intelligenza artificiale (ma il discorso vale, più in generale, di fronte a qualunque innovazione), posto che il diritto deve dare risposte, ci si chiede se, e in che misura, le risposte già fornite dal diritto attuale siano in sintonia rispetto al fenomeno regolato. Per rispondere utilmente, è chiaro che occorre innanzitutto conoscere bene il fenomeno da regolarsi: così, per vagliare le possibili soluzioni offerte dal diritto non si può prescindere dallo studio delle fattispecie concrete per come si presentano nella prassi. Il tentativo di definire i fenomeni (che cos'è l'intelligenza artificiale, ad esempio) non è dunque uno sterile esercizio definitorio, ma costituisce la premessa per una ricostruzione razionale dei problemi fondata su ciò che realmente accade (si veda in apertura il contributo di Daniele Imbruglia).

In questo senso devono essere letti, in particolare, nel campo di diritto privato i contributi in tema di *smart contracts* (Enrico Labella), di criptovalute (Carla Pernice) e di sistemi di reputational feedback e ranking (Silvia Martinelli). Solo un'attenta comprensione di come la tecnologia in pratica funzioni consente di inquadrare correttamente

i problemi giuridici, verificare la riconducibilità del nuovo alle categorie classiche (nel caso di specie, rispettivamente, del contratto, della moneta, delle pratiche commerciali sleali) e valutare dunque i reali termini della portata innovativa. Un'operazione analoga è svolta nel diritto penale, in cui si evidenzia la mutazione a seguito dell'evoluzione tecnologica dei concetti tradizionali di domicilio e comunicazione rilevanti ai fini delle investigazioni (Serena Quattrocolo).

Un dato ricorrente che emerge nello studio dei casi specifici di innovazione è quello dei rischi insiti nelle nuove tecnologie, che, se sfruttate al pieno della loro potenzialità, possono condurre a risultati non desiderabili. Automatismo, spersonalizzazione e invasività sono i profili critici maggiormente evidenziati. Così, nel rapporto medico paziente la spersonalizzazione del rapporto dovuta alla digitalizzazione della comunicazione rischia di risultare poco compatibile con quelle che dovrebbero essere le caratteristiche della relazione di cura e le esigenze del malato (Massimo Foglia). Più in generale, i rischi di spersonalizzazione e di automatismo sono particolarmente evidenti laddove la tecnologia è usata in processi decisionali (Giacomo Capuzzo). Così, nel campo del diritto penale si pone il problema dell'utilizzo di modelli computazionali come strumento per adiuvare i soggetti del procedimento penale ad effettuare valutazioni sulla cui base assumere decisioni. Nel campo del diritto privato, si pensi all'impiego degli algoritmi per adottare decisioni in merito alla sospensione dell'esecuzione di un contratto o alla conclusione di un contratto, con esiti potenzialmente discriminatori.

A questo punto ci si può chiedere se e in che misura il diritto esistente sia in grado di offrire risposte adeguate ai rischi evidenziati. In alcuni casi la risposta potrebbe essere positiva. Si pensi allo *smart contract* che consente di sospendere l'esecuzione della prestazione in caso di inadempimento: le norme in materia di obbligazioni e contratti già sembrano indicare i limiti entro cui un'autoesecuzione di tal fatta sia lecita. Altre volte la risposta è più dubbia. Così, a fronte dell'estensione delle pratiche discriminatorie rese possibili dall'uso di algoritmi ci si può chiedere quanto gli strumenti regolatori attuali siano idonei a dare risposte soddisfacenti al problema.

I rischi derivanti dall'automatismo sono acuiti dall'invasività delle nuove tecnologie, che consentono un elevato grado di intrusione nella vita privata delle persone. Questo è il caso, ad esempio, dell'Internet of things, per cui oggetti utilizzati per esigenze quotidiane (come gli assistenti vocali) sono in grado di raccogliere un'enorme mole di informazioni e dati personali, senza che gli interessati ne siano sempre pienamente consapevoli (Lavinia Vizzoni).

A questo punto, una volta inquadrate le caratteristiche delle fattispecie concrete e le problematiche giuridiche, è possibile intervenire su due fronti. Sul fronte delle regole giuridiche, al fine di adeguare la regola al regolato; e sul fronte del fenomeno empirico, il regolato, attraverso l'auspicio di una evoluzione tecnologica che già di per sé si sviluppi, incorporandole nel proprio funzionamento, alcune direttive dettate da istanze etico-giuridiche.

L'intelligenza artificiale (IA) e le regole. Appunti*

Daniela Imbruglia

Abstract

Le innovazioni digitali caratterizzano la nostra epoca. Praticamente ogni attività professionale e sociale coinvolge l'intelligenza artificiale. Ciò nonostante, non esiste una definizione di intelligenza artificiale e una disciplina giuridica uniforme di queste innovazioni. Questo paper affronta la questione attuale delle regole per l'intelligenza artificiale, indagando le diverse posizioni degli autori e riprendendo la risoluzione del Parlamento Europeo del 2017 sulla robotica e il diritto civile. Nella prima parte, è discussa l'opportunità di regolare queste applicazioni di IA e si riprende la lezione di Stefano Rodotà sul diritto e le nuove tecnologie. Successivamente, il saggio individua gli aspetti più critici dell'applicazione di categorie tradizionali a questi nuovi fenomeni digitali. Particolare attenzione è posta ai c.d. responsability gaps e all'impatto delle applicazioni IA sui diritti fondamentali. Nella parte finale, si individuano i principi più idonei a regolare il fenomeno come proposti dalla dottrina giuridica europea.

Digital innovations mark our age. Virtually every professional and social activity involves artificial intelligence systems. Nevertheless, there is no definition of artificial intelligence and there is no uniform legal discipline of such innovations. This paper addresses the current issue of artificial intelligence rules, investigating the different positions of the Authors and recalling the 2017 Resolution of the European Parliament on robotics and civil law. In the first part, the opportunity to regulate these IA applications is discussed and Stefano Rodotà's lesson on law and new technologies is resumed. Subsequently, the essay identifies the most critical aspects of the application of traditional legal categories to these new digital phenomena. Specific attention is paid to the so-called responsibility gaps and the impact of IA applications on fundamental rights. In the final part, we identify the most suitable principles to regulate the phenomenon as proposed by the European legal doctrine.

Sommario

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

Keywords

Intelligenza Artificiale - diritto - principi - responsabilità - personalità giuridica

Introduzione

Al pari di quelle politiche, le rivoluzioni scientifiche e tecniche sono idonee a sovvertire l'ordine regolato. A differenze delle prime, solo raramente ed eccezionalmente affrontate dalla dottrina[1], la discussione giuridica delle rivoluzioni tecnologiche è particolarmente diffusa e vivace. In questo articolo, darò, in modo parziale e giocoforza imperfetto, conto dell'attuale stato dell'arte, mettendo in risalto le varie contrapposizioni che l'odierna discussione sull'intelligenza artificiale (IA) ha generato[2]. Innanzitutto, esaminerò le posizioni che affrontano il tema della regolazione della realtà digitale, distinguendo tra la tesi conservatrice e quella adeguatrice, più sensibile alle ricadute giuridiche delle diverse applicazioni dell'intelligenza artificiale (§1). In un secondo momento, mi soffermerò sul dibattito relativo al ruolo del diritto davanti a questi nuovi fenomeni, richiamando le analisi della migliore dottrina civilistica (§2). Poi, affronterò la questione di quale sia l'attuale applicazione dell'intelligenza artificiale che interroga il giurista, ponendo in luce come spesso questa discussione sia viziata dal credere i progressi della intelligenza artificiale maggiori di quanto siano (§3) e, quindi, concentrandomi sulle caratteristiche più critiche delle attuali applicazione dell'IA (§4), anche richiamando la Risoluzione del Parlamento Europeo relativa alle norme di diritto civile sulla robotica del 16 febbraio 2017 (nel prosieguo, anche *Risoluzione*) (§5)[3]. In conclusione, darò conto dei possibili principi idonei a regolare il nuovo, consapevole che il discorso sia lungi dall'essere definito (§6): d'altronde, ogni scienza ha i suoi tempi.

---

[1] J. Halperin, *Five Legal Revolutions Since the 17th Century. An Analysis of Global History*, New York, 2014, vii.

[2] In questo lavoro si impiegherà indifferentemente il vocabolo robot, algoritmo, macchine intelligenti etc.: d'altra parte nella letteratura che si occupa del fenomeno dell'Intelligenza Artificiale, divenuta estremamente ampia negli ultimi anni, è ricorrente il rilievo circa l'incertezza del vocabolo da utilizzare con riferimento all'ente che svolge questo genere di applicazioni: talvolta si discute di robot, talaltra di algoritmo o, ancora, di agente elettronico o digitale, umanoide, etc.: in luogo di tanti, si v. G. Teubner, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi* (a cura di P. Femia), Napoli, 2019, 19-20; A. D'Aloia, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *Riv. Biodir.*, 2019, 8.

[3] Parlamento europeo, *Norme di diritto civile sulla robotica. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, (2015/2103(INL), 17 febbraio 2017, in *eur-lex.europa.eu*. Sulla risoluzione si vedano i commenti di G. Taddei Elmi e F. Romano, *Il robot tra* ius condendum *e* ius conditum, in *Inf. Dir.*, 2016, 115; S. Oriti, *Brevi note sulla risoluzione del parlamento europeo del 16 febbraio 2017 concernente le norme di diritto civile sulla robotica*, in *ratioiuris*, 2017, N. Busto, *La personalità elettronica dei robot: logiche di gestione del rischio tra trasparenza e fiducia*, in *Ciberspazio e dir.*, 2017, 499 e G. Passagnoli, *Regolamento giuridico e tutele nell'intelligenza artificiale*, in *Pers. merc.*, 2019, 79.

1. Regole e rivoluzioni scientifiche.

Il tradizionale porsi come oracolo della legge vigente spiega perché davanti ad ogni mutamento proveniente dalla realtà regolata vi sia, tra i giuristi, una più o meno ampia comunità di interpreti che si attesta su posizioni conservatrici, sostenendo la sufficienza del dato normativo esistente a risolvere i conflitti che queste innovazioni portano con sé e che non vi sia, pertanto, bisogno di uno studio specifico di tali conflitti. Tale argomento è comunemente richiamato con la formula, *Law of the Horse*, utilizzata a metà anni Novanta per negare dignità scientifica al *cyberlaw*, il quale, al pari appunto di un ipotetico corso di diritto dei cavalli, non presenterebbe un tratto di organicità e, per la comprensione delle regole sugli scambi o sulla responsabilità, nulla aggiungerebbe alla conoscenza delle «*general rules*» capaci di «*illuminate the entire law*"[4]. Oltre che su questo argomento, la posizione conservatrice, peraltro, sostiene anche che sarebbe inopportuno intervenire normativamente su di una realtà quale la tecnologia che, per definizione, presenta un elevato tasso di dinamicità[5]. Simile osservazione poggia infine su quella tradizionale e ricorrente illusione che vuole la tecnica come un qualcosa di neutrale, che presenta vantaggi per tutti e non determina conflitti, ma, al più, li risolve in modo inedito[6].

A differenza di quanto generalmente accade con le rivoluzioni politiche, tale posizione conservatrice, però, non esaurisce il panorama della letteratura scientifica, abitato anche da chi si sforza di discutere le ricadute giuridiche delle innovazioni tecniche[7]. Senza necessariamente propendere per la tesi che afferma la necessità di una legge per ogni nuova scoperta (c.d. eccezionalismo), tale secondo atteggiamento sostiene che l'esame e lo studio delle concrete implicazioni giuridiche delle innovazioni possa portare all'estensione di certe norme o alla rivisitazione di altri istituti, la cui *ratio* sottostante mal si adatta al nuovo mondo[8]. A tal proposito si deve ben ribadire come tali risultati siano solamente eventuali: essi non sono una automatica conseguenza della novità scientifica, ma dipendono dal concreto manifestarsi di una lacuna (es. *responsability gap*)[9]. Ad esempio, è noto come, davanti ai mutamenti propri della rivoluzione industriale, il

---

[4] F.H. Easterbrook, *Cyberspace and the Law of the Horse*, in *Univ. Chi. Legal. Forum*, 1996, 207.

[5] Con riferimento all'intelligenza artificiale, un saggio di tale secondo argomento è offerto da A. Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*, Arlington, 2016 e da D. Castro – M. McLaughlin, *Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence*, 2019, in itif.org.

[6] Sul tema si veda la discussione svolta in G. Mobilio, *L'intelligenza artificiale e i rischi di una "disruption" della regolamentazione giuridica*, in *Riv. Biodir.*, 2020, 406.

[7] Alla tesi di Easterbrook, si oppongono almeno due non meno famose repliche L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach, Harv. Law Rev.*, 1999, 501 e, più di recente, R. Calo, *Robotics and the Lessons of Cyberlaw*, in *Cal. Law Rev.*, 2015, 513.

[8] U. Ruffolo, *Intelligenza Artificiale,* machine learning *e responsabilità da algoritmo*, in *Giur. it.*, 2019, 1690 e 1696.

[9] Il punto è sostanzialmente pacifico in dottrina. Per tutti si veda, A. Santosuosso, C. Boscarato, F. Caroleo, *Robot e diritto: una prima ricognizione*, in *Nuova giur. civ. comm.*, 2012, 497: «Solo qualora non si dovesse riscontrare una soluzione adeguata, si potrà considerare la possibilità di introdurre nuove regole o di modificare quelle esistenti. In altre parole, si intende evitare un approccio eccezionalista, che è tipico di chi considera a priori le norme attuali inadeguate a disciplinare le questioni che emergono dagli sviluppi tecnologici, ritenendo, quindi, sempre necessario creare nuove regolamentazioni ad hoc».

ceto dei giuristi abbia lavorato affinché le regole della responsabilità civile – tradizionalmente imperniate sul criterio della colpa – mutassero così da rendere più effettiva la possibilità per il lavoratore infortunato di ottenere una tutela[10].
Tra le due posizioni – quella conservatrice e quella adeguatrice – sembra essere preferibile la seconda. In tal senso, a ben vedere, milita l'esigenza propria del diritto quale prodotto della società di assicurare una elevata sintonia tra regola e regolato[11]. Come scrisse uno dei massimi civilisti del secolo scorso, la ragione del notevole interrogarsi da parte dei giuristi circa le rivoluzioni tecnologiche idonee ad alterare la materia regolata si spiega, infatti, con la consapevolezza circa il fatto che il diritto conosce il suo più grande rischio di svalutazione nella perdita della «effettiva capacità regolativa"[12]. Da ciò, allora, una prima ragione per sostenere la verifica del rapporto tra regola e regolato. Non solo. Sempre nel senso della preferenza dell'atteggiamento che ricerca una adeguatezza tra la norma e la realtà milita anche il rilievo per cui «l'estensione delle regole già stabilite, con i rafforzamenti e gli adattamenti necessari» è necessario per assicurare che anche nel nuovo contesto i valori fondamentali della nostra società – es. i diritti umani, la libertà e la dignità dell'individuo – siano rispettati[13].

2. La lezione di Rodotà: afferrare il nuovo per darvi la giusta forma

Una volta convenuto sulle opportunità di studiare il nuovo contesto determinato dalle innovazioni tecniche dal punto di vista giuridico occorre, però, prestare particolare attenzione al come procedere. A tal riguardo, si può muovere proprio da quella compianta dottrina sopra richiamata a proposito del rischio di svalutazione e della necessità del diritto per il rispetto, anche nel nuovo contesto, dei valori fondamentali.
Rodotà svolgeva quella riflessione sull'esigenza di evitare una perdita dell'effettiva capacità regolativa del diritto e sulla impossibilità per il diritto di "distogliere lo sguardo" a margine dell'avvenuta riproduzione di una pecora per clonazione (il "caso" *Dolly*, 1997). D'altra parte, la possibilità aperta dalla tecnica di una riproduzione agamica dell'uomo interroga il diritto e, ciò, in quanto essa segna il superamento di un ordine segnato dal monopolio della natura sulla creazione della vita umana e animale[14]. Nella

[10] P. Rosanvallon, *L'état en France. De 1789 a nos jours*, Paris, 1990, 175. Per la più generale osservazione per cui «*a technology is exceptional when its introduction into the mainstream requires a systematic change to the law or legal institutions in order to reproduce, or if necessary displace, an existing balance of values*", si veda R. Calo, Robotics and the Lessons, cit., 552-553.

[11] In argomento, imprescindibile è la lettura di N. Irti – E. Severino, *Dialogo su diritto e tecnica*, Roma-Bari, 2001.

[12] S. Rodotà, *La vita e le regole*, Milano, 2018, 202.

[13] Ivi, 87. Come vedremo, una prima eco di questa impostazione si ha già nella *Risoluzione*, cit., lett. O e a cui *adde*, lett. U e V.

[14] Sul punto si veda, almeno, S. Rodotà, *Sul buon uso del diritto e i dilemmi della clonazione*, in *Riv. crit. dir. privato*, 1999, 561; H. Atlan, *Possibilità biologiche, impossibilità sociali*, ivi, 571; M. Salvi, *Biotecnologie e bioetica, un ritorno alla metafisica? Terapia genica in utero, clonazione umana e lo statuto morale dell'embrione*, ivi, 587; C.R. Sunstein, *La Costituzione e la clonazione*, ivi, 599; S. Stammati, *Costituzione, clonazione umana, identità genetica*, in *Giur. costit.*, 1999, 4067; F.D. Busnelli, *Il problema della clonazione riproduttiva*, in *Riv. dir. civ.*, 2000, I, 175;

soddisfazione di questa domanda di regole che diano forma al mondo nuovo (perché non più dominato dalle sole leggi della natura), il diritto (privato) commette un grave errore, sia quando non vi provvede sia quando, secondo la convincente impostazione critica di Rodotà, procede al solo fine di rassicurare la società turbata dalla scienza, mimando, peraltro artificialmente, il limite che questa ha superato[15]. Nel momento in cui i giuristi rifiutano di confrontarsi con la nuova realtà e non «afferrano» il nuovo, evitando di «dare corpo ai principi che a quel mondo nuovo possono dare forma» e limitandosi a ripetere principi di riferimento propri di altri sistemi regolativi (religione, economia, scienza, etc.), il diritto si espone al rischio di una sua svalutazione, rappresentata, appunto, da una perdita di effettiva e autonoma capacità regolativa, oltre che della scomparsa dei diritti fondamentali[16].

Orbene e come già detto (*supra*, §1), anche le innovazioni della tecnologia digitale che più caratterizzano questa età della storia umana interrogano il diritto: esse sono tali da porre in discussione il rapporto tra le regole tradizionali e ciò che di quel regolato è più interessato dal digitale, nonché la tenuta dei diritti civili, politici e sociali. Peraltro, anche queste innovazioni si pongono in termini di sfida[17]: le novità insite nei progressi costringono il giurista a rivisitare il dato normativo esistente e a costruire distinte discipline di effettivo governo del "mondo nuovo" in cui siamo entrati da più di un qualche decennio, così da «indirizzare l'intelligenza artificiale verso il bene degli individui e della società»[18]. Si tratta, inoltre, di una sfida decisiva, epocale[19]: attesa la centralità di queste innovazioni nella nostra società (basti pensare che il digitale è stato una delle poche costanti tra il mondo pre-Covid19 e il mondo pandemico), il diritto – si dice – non può sottrarsi e scegliere di non combatterla, rinunziando a disciplinare i conflitti caratterizzati e caratterizzanti il digitale[20]. A ben vedere, come davanti ai progressi della bioetica, anche davanti alle innovazioni proprie dell'IA serve evitare uno scollamento

P. Donadoni, *La disciplina biogiuridica della clonazione umana - Rassegna di materiali nazionali e sovranazionali*, in *Mat. storia cultura giur.*, 2000, 247.

15 S. Rodotà, *La vita e le regole*, cit., 16; Id., *Il diritto di avere diritti*, Roma-Bari, 2017, 351-352. Per ciò che concerne la clonazione, è noto, sul piano normativo, la risposta fu quella di prevedere un divieto, assoluto, per ogni ipotesi di intervento tecnico il cui scopo fosse quello di creare – *rectius*, riprodurre – un essere umano geneticamente identico a un altro essere umano vivo o morto (così, l'art. 1 del *Protocollo addizionale alla Convenzione per la protezione dei diritti dell'uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina, sul divieto di clonazione di esseri umani*, sottoscritto a Parigi il 12 gennaio 1998 nell'ambito del Consiglio d'Europa; nella stessa direzione, si veda poi l'art. 3, EUCFR, nonché la risoluzione non vincolante dell'Assemblea generale delle Nazioni Unite sull'*Human Cloning* (UN GAOR, 59th Session, UN Doc., A/280 (2005)).

16 S. Rodotà, *Il diritto di avere diritti*, cit. 352-353.

17 Il Parlamento Europeo parla espressamente di "sfide" poste dall'apprendimento automatico ai principi di non discriminazione, giusto processo, trasparenza e comprensibilità dei processi decisionali: *Risoluzione*, cit., lett. H. In dottrina, si v., in luogo di tanti, U. Pagallo, *Algoritmi e conoscibilità*, in *Riv. fil. Dir.*, 2020, 94, 101.

18 G. Sartor, *Introduzione*, in *Riv. fil. dir.*, 2020, 69.

19 G. Pascuzzi, *Il diritto nell'era digitale*, Bologna, 2020, 24.

20 *Ex multis*, A. Santosuosso - C. Boscarato - F. Caroleo, *Robot e diritto*, cit., 495; E. Palmerini, *Robotica e diritto: Suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. prev.*, 2016, 1815; U. Pagallo, I*ntelligenza artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sist. Intell.*, 2017, 617; G. Teubner, *Soggetti giuridici digitali?*, cit., 26; A. D'Aloia, *Il diritto verso "il mondo nuovo"*, cit., 9. Sulla centralità del fenomeno e connessa inevitabilità della regolazione, si. v. anche *Risoluzione*, cit., lett. B, E, G, I.

tra la regola e il regolato. Occorre quindi ricostruire, ora con interpretazioni ora con interventi del legislatore, un quadro normativo adatto alla verità effettuale della cosa e in grado di governare il nuovo mondo, fuggendo lacune e vuoti e assicurando la continuità dei valori fondamentali della nostra società[21]. Insomma, "afferrare il nuovo" e "dare corpo ai principi che a quel mondo nuovo possono dare forma".

3. Afferrare il nuovo e il mito del robot intelligente.

Il compito di "afferrare il nuovo" non risulta facile e ciò, in particolare, per una rivoluzione, quale quella digitale, che presenta un notevole ambiguità. Per un verso, molte delle applicazioni tecnologiche che caratterizzano il nostro quotidiano non erano pensabili e pensate dalle generazioni precedenti. Per altro verso, l'idea di una cosa (perché non persona) evoluta (perché animata) alberga nel pensiero umano da tempo immemore[22].

Gran parte dei contributi giuridici aventi ad oggetto la ricerca di una disciplina del robot intelligente fanno ricorso ad immagini con le quali, nel corso della storia, l'uomo ha provato a descrivere la macchina animata. Talvolta, si cita l'etimologia del termine, il cui esordio si vuole risalente al 1923, quale traduzione del vocabolo ceco '*robotnik*' (lavoratore forzato), impiegato dallo scrittore Karel Capek nel suo dramma fantascientifico *Rossum's Universal Robots*, talaltra si richiama il mito di Pigmalione o il personaggio di Frankenstein. Ancora più diffuso è il richiamo alle tre leggi di Asimov, tratte da *Runaround* (1942), e la cui formulazione originaria così si sviluppa: «*A robot may not injure a human being or, through inaction, allow a human being to come to harm; A robot must obey any orders given to it by human beings, except where such orders would conflict with the First Law; A robot must protect its own existence as long as such protection does not conflict with the First or Second Law*». Tale tributo artisitico-letterario non è un vizio esclusivo della dottrina giuridica: la stessa famosa *Risoluzione* si apre rilevando come «gli essere umani» abbiano «fantasticato sulla possibilità di costruire macchine intelligenti, spesso androidi con caratteristiche umane»[23].

L'idea che l'innovazione attuale non sia che una tappa verso il prossimo e certo momento in cui non vi sarà differenza tra uomo e macchina è poi anche alimentata dalla più diffusa narrazione dei progressi dell'intelligenza artificiale: quante volte, infatti, ci si è imbattuti in quella parabola che, continuamente arricchita di riferimenti (o personaggi?: *DeepBlue* che sconfigge Kasparov a scacchi[24], *AlphaGo* che trionfa contro Lee

[21] Uno sviluppo dei principi di IA in parallelo con quelli della bioetica è proposto da L. Floridi - J. Cowls - M. Beltrametti - R. Chatila - P. Chazerand - V. Dignum - C. Luetge - R. Madelin - U. Pagallo - F. Rossi - B. Schafer - P. Valcke - E. Vayena, *AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, 689.

[22] G. Wood, *Edison's Eve. A Magical History of the Quest for Mechanical Life*, New York, 2002.

[23] *Risoluzione*, cit., lett. T.

[24] https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/.

Sedol a Go[25], *Vital* che partecipa al *board* di una società[26], *Sophia* e il suo passaporto[27], *GPT-3* che scrive un articolo per il maggior quotidiano britannico[28]) e di applicazioni (militari[29], finanziarie[30], giudiziali[31], occupazionali[32], etc.), racconta di una macchina lanciata in modo inarrestabile verso (e oltre) l'uomo?

A ben vedere, proprio la circostanza che vuole il mondo nuovo dell'intelligenza artificiale come una rivoluzione il cui esito era già stato anticipato e immaginato (la macchina\persona e il robot intelligente) incide sul perché, anche tra coloro i quali condividono la necessità di verificare la tenuta delle regole rispetto al nuovo mondo, sia tanto difficile convenire su ciò che va afferrato e sia facile imbattersi nella discussione di scenari non attuali[33]. Si pensi, in particolare, alla ampia e vivace discussione circa la personalità elettronica e della piena soggettività dei robot. Come noto, infatti, a fronte di chi nega alle presenti tecniche digitali la capacità di innovare il discorso giuridico e ritiene le *general rules* una disciplina sufficiente, vi è chi esagera la portata effettiva delle scoperte attuali. Come se convinti che le recenti innovazioni digitali siano una tappa del percorso che dal sogno della macchina intelligente inevitabilmente conduce al robot completamente autonomo, tali giuristi accettano, ancorché - giova ripeterlo - in anticipo sui tempi, di discutere l'attribuzione di diritti e doveri a tali enti immaginando di essere già davanti alla macchina completamente autonoma[34]. Più che sulla realtà del regolato, questa apertura alla c.d. piena personalità elettronica poggia sulla capacità che i continui progressi dell'attuale contesto (la realtà) hanno di illudere l'uomo di essere vicino alla fine della storia della macchina come prodotto e alla realizzazione

---

[25] M. Tegmark, *Vita 3.0. Essere umani nell'era dell'intelligenza artificiale*, Milano, 2018, 121.

[26] M.L. Montagnani, *Flussi informativi e doveri degli amministratori di società per azione ai tempi dell'intelligenza artificiale*, in *Pers. Merc.*, 2020, 86.

[27] U. Pagallo, *Vital, Sophia, and Co. - The Quest for the Legal Personhood of Robots*, in *Information*, 2018, 230.

[28] GPT-3, *A robot wrote this entire article. Are you scared yet, human?*, in *Guardian*, 8 settembre 2020.

[29] Per una prima discussione in proposito, G. Tamburrini, *Autonomia delle macchine e filosofia dell'intelligenza artificiale*, in *Riv. filos.*, 2017, 263.

[30] F. Pistelli, *Algoritmi e contratti nel sistema finanziario*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, 249.

[31] Si pensi al *software* Compas, utilizzato da diverse corti statunitensi per valutare la probabilità di recidiva. In argomento, A. Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, in *Duke Law Journal*, 2019, 1043; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Riv. Biodir.*, 2019, 71; G. Pascuzzi, *Il diritto nell'era digitale*, cit., 293; più in generale sul tema, si veda: M. Luciani, *La decisione robotica*, in *Riv. AIC*, 2018, 872.

[32] C. Casadei, *Per Esselunga primo job day di massa interamente virtuale*, in *Il Sole 24-ore*, 10 settembre 2020 (*www.ilsole24ore.com*).

[33] Per tutti, K. Kurzweil, *The Singularity is Near: When Humans Transcend Biology*, New York, 2005 e N. Bostrom, *Superintelligenza, Tendenza. Pericoli. Strategia*, Torino, 2018.

[34] Tale atteggiamento, peraltro, non si ritrova solo in chi auspica il pieno riconoscimento della personalità giuridica alle macchine (più o meno) intelligenti, ma, curiosamente anche in chi nega *in toto* la discussione. Come è stato di recente osservato, infatti, «la vera ragione della resistenza a riconoscere la soggettivazione (parziale) quale unisca strategia dogmatica per la comprensione dell'intelligenza artificiale nel diritto civile non è la troppa distanza tra intelligenza artificiale e umana, ma l'eccesso di prossimità» (P. Femia, *Introduzione. Soggetti responsabili Algoritm e diritto civile*, in G. Teubner, *Soggetti giuridici digitali?*, cit., 10).

del, già tante volte immaginato, sogno del robot intelligente e pienamente autonomo[35]. Orbene, invece di indugiare nella contrapposizione tra *Singularitarians* e *Aitheists*[36] o in altri assolutismi (persona o *res*)[37] che, come recentemente osservato rispetto ad analoghi discorsi di espansione della soggettività giuridica, sono eccessivamente ideologici[38], è necessario afferrare la realtà per quello che è. Per un verso, occorre riconoscere che, allo stato, la possibilità di una macchina pienamente autonoma non è attuale, né tanto meno prossima: nessuna delle diverse applicazioni che compongono la parabola fa a meno dall'apporto umano (che, ora come programmatore ora come utilizzatore, resta pur sempre il soggetto partecipe delle diverse azioni) e nessuna macchina ha mai raggiunto i diversi tratti che vengono comunemente riconnessi all'intelligenza umana[39]. In questo contesto, allora, l'attribuzione della piena personalità elettronica non può che sollevare dubbi e preoccupazioni circa un suo possibile carattere abusivo, traducendosi in un ostacolo formale all'individuazione dell'effettivo responsabile[40]. Per altro verso, invece di trincerarsi dietro l'impossibilità della macchina di provare emozioni, di mimare l'intelligenza umana o comunque di raggiungere quell'indice che, in modo arbitrario e a-tecnico, si ritiene idoneo a giustificare l'equiparazione alla persona[41], si deve riconoscere che una discussione sulla soggettività si renda già oggi necessaria[42].

---

[35] D'altra parte, in qualche modo sintomatico di quanto si dice nel testo circa il tratto non attuale della discussione sulla piena personalità dell'IA, è la circostanza per cui l'articolo più citato che ne sostiene l'attribuzione all'IA risalga a un contesto (1992) in cui il quotidiano era certamente lontano dagli attuali progressi delle macchine (es. privo di internet!): L.B. Solum, *Legal Personhood for Artificial Intelligences*, in *North Carol. L. Rev.*, 1992, 1231.

[36] L. Floridi, *Should we be afraid of AI?*, in *Aeon*, 2016 (aeon.co).

[37] Centrale nella esperienza giuridica occidentale, come noto, è la dicotomia che divide ogni entità che sia diversa dalla *actio* in persona o cosa (*D.*, 1.5.1.), così che «cosa è la *non*-persona e persona la *non*-cosa» (R. Esposito, *Le persone e le cose*, Torino, 2014, 3). I due termini sono posti dalla tradizione in una relazione di strumentalità (Aristotele, *Pol.* I, 4, 1253b 25 – 1254a 18), dove «il ruolo delle cose è quello di servire, o comunque di appartenere, alle persone» e quello della persona è l'esercitare «una padronanza» sulle cose) e sono caratterizzati da una notevole flessibilità: attesa l'artificialità del diritto, infatti, sono numerose le entità che, in certi momenti e in certi luoghi, rivestono una qualifica differente da quella assunta in precedenza o ricoperta altrove (a tal proposito, l'esempio più diffuso è il riconoscimento della personalità giuridica a fiumi (Te Awa Tupua Act 2017, s. 14: *Te Awa Tupua is a legal entity, and has all the rights, powers, duties and liabilites of a legal person*), foreste (es. Te Urewera Act 2014, s. 12: *Te Urewera is a legal entity, and has all the rights, powers, duties and liabilites of a legal person*) operato dal legislatore neozelandese nonché il (lento) processo di emersione dei diritti degli animali (da ultimo definiti come «esseri senzienti», ex art. 13, TFUE).

[38] Per una intelligente critica di quella tendenza a sviluppare il discorso giuridico della natura in termini di passaggio da *res* a *persona*, si veda M. Spanò, *Perché non rendi poi quel che prometti allor? Tecniche e ideologia della giuridificazione della natura*, in Y. Thomas – J. Chiffoleau, *L'istituzione della natura*, Macerata, 2020, 104.

[39] In questo senso, G. Teubner, *Soggetti giuridici digitali?*, cit., 30, nonché l'*Open Letter to the European Commission Artificial Intelligence and Robotics*, in www.robotics-openletter.eu. Si tratta della lettera con cui centinaia di scienziati hanno criticato la proposta contenuta all'art. 59, *f) Risoluzione*, cit., di istituire la personalità elettronica. Come noto, la Commissione non ha accettato quella proposta del Parlamento.

[40] Sul rischio dei «*robots as liability shields*» si v., per tutti, J.J. Bryson - M.E. Diamantis - T.D. Grant, *Of, for, and by the people: the legal lacuna of synthetic persons,* in *Artif. Int. Law*, 2017, 285.

[41] U. Ruffolo, *Intelligenza Artificiale,* machine learning, cit., 1702-1703.

[42] Si v., ad esempio, le diverse ricostruzioni circa una capacità e una soggettività parziale operate da U. Pagallo, *The Law of Robots. Crime, Contracts and Torts*, Dodrecht-Heidelberg-New York-London, 2013, 103 e da G. Teubner, *Soggetti giuridici digitali?*, cit., nonché la tesi, allo stato isolata, per cui già l'attuale contesto normativo statunitense consentirebbe l'attribuzione di diritti e doveri all'IA avanzata da S.

In effetti, non si può negare che molte delle odierne applicazioni presentano elementi di tensione con la tradizionale categoria di strumenti[43]. A ben vedere, più che nel (mito del) robot intelligente, il nuovo da afferrare risiede proprio in queste tensioni ed è a queste a cui occorre dare la giusta forma.

4. Afferrare il nuovo: l'IA, oggi

Uno dei pochi punti fermi e condivisi nella letteratura giuridica attiene alla inesistenza di una definizione di intelligenza artificiale[44]. Estranea al testo del *seminal work* di Turing[45], la formula dell'IA ricorre per la prima volta a metà degli anni Cinquanta del secolo scorso, con l'intento di indicare un «*attempt*» per «*to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves*»[46]. A questa prima fase, è seguito un periodo in cui l'obiettivo perseguito dalla comunità nella costruzione della macchina non è più rappresentato dalla sua idoneità a riprodurre il cervello dell'uomo (*Artificial General Intelligence*, AGI), ma piuttosto nella soluzione di specifici problemi.
Oggi vi è chi definisce la IA come «*the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable*»[47]. Altri, invece, la definiscono come «la scienza della produzione di macchine e sistemi volti all'esecuzione di compiti che, qualora realizzati da essere umani, richiederebbero l'uso dell'intelligenza per risolvere problemi di apprendimento e conoscenza, di ragionamento e pianificazione»[48]. Ancora, di recente, si è sostenuto che per IA si debba intendere il «*field that studies the synthesis and analysis of computational agents that act intelligently*»[49]. Anche con riferimento al piano normativo e para-normativo, è dato registrare una notevole pluralità di soluzioni. Tra queste, particolare attenzione ha ricevuto quella proposta a livello europeo lo scorso anno e che così recita: «*Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt*

Bayern, *The Implications of Modern Business-Entity Law fot the Regulation of Autonomous Systems*, in *Stan. Tech. Law Rev.*, 2015, 93.

43 Per tutti, *Risoluzione*, cit., lett. AB.

44 In tal senso, tra gli altri, G. Pascuzzi, *Il diritto nell'era digitale*, cit., 289; A. Santosuosso - C. Boscarato - F. Caroleo, *Robot e diritto*, cit., 497 e A. D'Aloia, *Il diritto verso "il mondo nuovo"*, cit., 8.

45 A. Turing, *Computing machinery and intelligence*, in *Mind*, 1950, 433.

46 J. McCarthy - M.L. Minsky - N. Rochester - C.E. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1955, 1.

47 J. McCarthy, *What is Artificial Intelligence?*, 2007, 1 in *formal.stanford.edu*.

48 U. Pagallo, I*ntelligenza artificiale e diritto*, cit., 615. In senso analogo, già, M.L. Minsky, *Semantic information processing*, Cambridge, 1969.

49 D. Poole – A. Mackworth, *Artificial Intelligence*, Cambridge, 2017 (consultabile anche in *artint.info*).

their behavior by analyzing how the environment is affected by their previous actions»[50]. Orbene la mancanza di un consenso attorno a una determinata definizione è spiegata con la difficoltà di affermare «*a bright-line distinction between what constitutes AI and what does not*»[51] ed è impiegata per suggerire ai legislatori di «*to find specific definitions which could prove useful to address narrowly identified problems posed by AI applications*»[52].

Per quanto nella letteratura sull'IA sia ugualmente dibattuto il riferimento all'ente che svolge le applicazioni, ai fini del presente lavoro si può muovere dalla diffusa distinzione del robot in tre distinte categorie: i robot tele-operati, le cui azioni sono completamente controllate dall'uomo e che configurano più o meno semplici strumenti dell'operatore; i robot autonomi, che hanno l'abilità di svolgere un compito senza alcun intervento umano, ma seguendo un programma che gli fornisce regole di comportamento; i robot cognitivi, dotati di un sistema per auto programmarsi, pianificare e apprendere dalla propria esperienza, grazie ad algoritmi evolutivi[53]. All'interno di questa classificazione, poi, si possono isolare i due tratti più rilevanti e centrali: il concetto di autonomia e quello di auto-apprendimento. La prima è definita dalla *Risoluzione* come quella «capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna». Si tratta di una capacità di «natura puramente tecnologica e il suo livello dipende dal grado di complessità con cui è stata progettata l'interazione di un robot con l'ambiente». Il secondo tratto caratterizzante l'IA odierna è rappresentato dalla sua capacità cognitiva, con ciò intendendo «la capacità di apprendere dall'esperienza e di prendere decisioni quasi indipendenti»[54]. Così individuato l'insieme di applicazioni a cui prestare attenzione, occorre porre in evidenza come, allo stato attuale, le funzioni prevalenti dell'IA concernono i processi di assunzione delle decisioni e si distinguono prevalentemente in sistemi decisionali automatici interamente basati su IA (es. auto senza conducenti) e in sistemi di supporto delle decisioni altrui (es: algoritmi di valutazione del cliente nella formazione del contratto)[55].

---

[50] European Commission's High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI* , 2019, 36.

[51] National Science and Technology Council Committee, *Preparing for the future of Artificial Intelligence*, 2016, 7 (in *whitehouse.gov*).

[52] A. Bertolini, *Artificial Intelligence and Civil Liability*, 2020, 31.

[53] La classificazione, che si deve al progetto EUROP (European Robotics Technology Platform) ed è consultabile in www.eu-robotics.net, è ripresa, tra gli altri, da: G. Taddei Elmi e F. Romano, *Il robot*, cit., 124; L. Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Pol. Dir.*, 2018, 716 e, prima, A. Santosuosso - C. Boscarato - F. Caroleo, *Robot e diritto*, cit., 498.

[54] Cons. Z e AA, *Risoluzione*.

[55] A. Mantelero, *Come regolamentare l'intelligenza artificiale*, 2019, in *agendadigitale.eu*. Sul primo aspetto, si v. per tutti, F.P. Patti, *The European Road to Autonomous Vehicles*, in *Ford. Int. Law Journ.*, 2019, 125. Sul secondo, invece, F. Pistelli, *Algoritmi e contratti*, cit., 256, nonché A. Davola, *La valutazione del merito di credito del consumatore*, in E. Pellecchia – L. Modica (a cura di), *La riforma del sovraindebitamento nel codice della crisi d'impresa e dell'insolvenza*, Pisa, 2020, 146.

5. Afferrare il nuovo: rischi e criticità dell'IA oggi

Questo complesso utilizzo dell'IA è idoneo a determinare dei risultati che pongono in crisi gli ordinari criteri di imputabilità della responsabilità e che comportano inedite forme di lesione di diritti fondamentali, richiedendo al diritto uno sforzo interpretativo e, in subordine, legislativo.

Per quanto concerne il profilo della responsabilità, tale tensione è evidente nel confronto tra le applicazioni dell'IA, caratterizzata da autonomia e autoapprendimento, e il contesto normativo di diritto privato europeo, rappresentato dalla fondamentale direttiva sui prodotti difettosi, che compie quest'anno trentacinque anni[56], e dalle più recenti normative in materia di dispositivi medici[57], di sicurezza generale dei prodotti[58], di macchine[59], di giocattoli[60], di strumenti di misura[61] e di apparecchiature radio[62]. Come è stato notato anche di recente, questo *corpus* normativo – creato «in larga parte fra gli anni '70 e '80 del secolo passato, quando si usava il Commodore 64 e nelle case il robot era l'aspirapolvere»[63] – lascia aperte diverse questioni in merito ai danni causati dai robot autonomi e dotati di capacità di adattamento e quindi capaci di azioni imprevedibili per il produttore, programmatore, proprietario e per l'utente[64]. Innanzitutto, ci si domanda se la direttiva sui prodotti difettosi (archetipo di questo *corpus*) ricomprenda i sistemi di IA e riguardi i soli consumatori. In secondo luogo, si osserva quanto risulti complicato, attesa l'opacità e complessità dei sistemi dell'IA, consentire, sulla base dell'attuale contesto normativo euro-unitario, l'individuazione del soggetto effettivamente responsabile e come l'onere probatorio dalla stessa richiesta non sia facilmente assolvibile[65].

Tale incertezza è particolarmente critica e rischiosa per la tenuta dei diritti fondamentali. Difatti, anche maliziosamente opponendo la pretesa neutralità dell'IA al cervello

---

[56] Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi, in *OJ* L 210, 7.8.1985, 29.

[57] Direttiva 93/42/CEE del Consiglio, del 14 giugno 1993 concernente i dispositivi medici, in *GU* L 169 del 12.7.1993, 1.

[58] Direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti, in *OJ* L 11, 15.1.2002, 4.

[59] Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006 , relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione), in *GU* L 157 del 9.6.2006, 24.

[60] Direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli, in *GU* L 170 del 30.6.2009, 1.

[61] Direttiva 2014/32/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014 , concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di strumenti di misura (rifusione), in *GU* L 96 del 29.3.2014, 149.

[62] Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014 , concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/C, in *GU* L 153 del 22.5.2014, 62.

[63] A. Mantelero, *Come regolamentare l'intelligenza artificiale*, cit.

[64] *Risoluzione*, cit., lett. AE, AG, AH, AI.

[65] *Ex multis*, G. Teubner, *Soggetti giuridici digitali?*, cit., 25 e A. Bertolini, *Artificial Intelligence and Civil Liability*, cit., 57-59.

dell'uomo, le cui decisioni sappiamo essere influenzate da una serie notevole di pregiudizi, si assiste sempre più spesso a un impiego dell'IA quale sistema di supporto di decisioni altrui concernenti aspetti centrali della vita delle persone e che, come tali, sono protetti quali diritti fondamentali[66]. Orbene, la cronaca recente smentisce questo assunto (neutralità dell'IA) ed è piena di denunce circa il c.d. *bias in machine learning* o *AI bias*. L'effetto di questi errori di valutazione è spesso penalizzante per minoranze, razziali e non, e, a seconda dell'ambito in cui si manifesta, può rilevare anche come lesione di un diritto fondamentale[67].

6. Principi con cui dare forma al nuovo

Davanti a queste criticità e tensioni, lo si è detto, parte della comunità giuridica si sforza di trovare soluzioni, per un verso, adeguate alla materia, e, per l'altro, idonee ad assicurare la continuità dei principi fondamentali del nostro ordinamento. Come riconosciuto dalla stessa *Risoluzione*, è necessario che «gli sviluppi nel campo della robotica e dell'intelligenza artificiale siano pensati in modo tale da preservare la dignità, l'autonomia e l'autodeterminazione degli individui»[68]. Per raggiungere questo obiettivo, l'interprete e il legislatore possono ricorrere a diversi principi, che appunto diano al nuovo una forma giusta perché conforme ai nostri valori fondanti.

Ad esempio, con riferimento alla responsabilità aquiliana e fermo restando la possibilità di rinvenire nel disciplina nazionale una base giuridica per una interpretazione che sappia fornire regole adeguate sull'illecito determinato da algoritmo[69], è noto che l'opinione maggioritaria propende per l'adozione di regole uniformi, quanto meno per lo spazio europeo, sottolineando come solo in tal modo si può provare a offrire una effettiva regolazione del fenomeno che presenta una dimensione globale[70]. Rispetto a questa ipotesi legislativa, il Parlamento Europeo ha suggerito l'adozione di una disciplina improntata al principio di effettività della tutela, di guisa che il futuro strumento legislativo «non dovrebbe in alcun modo limitare il tipo o l'entità dei danni che possono essere risarciti, né dovrebbe limitare le forme di risarcimento che possono essere offerte alla parte lesa per il semplice fatto che il danno è provocato da un soggetto non umano», e a quello di proporzionalità, cosi che «una volta individuati i soggetti responsabili in ultima istanza, la loro responsabilità dovrebbe essere proporzionale all'effettivo livello di istruzioni impartite al robot e al grado di autonomia di quest'ultimo»[71].

---

[66] Si pensi alla posizione recente e autorevole che giustifica il ricorso all'IA proprio evidenziando come, a differenza di quelli che caratterizzano l'uomo, i bias dell'algoritmo possono essere corretti ed eliminati, una volta individuati: J. Kleinberg - J. Ludwig - S. Mullainathan - C. R. Sunstein, *Discrimination in the Age of Algorithms*, in *Jour. Legal Anal.*, 2018, 113.

[67] Per degli esempi si veda la ricerca di V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*, New York, 2018.

[68] *Risoluzione*, cit., lett. O.

[69] U. Ruffolo, *Intelligenza Artificiale*, cit., 1689.

[70] G. Passagnoli, *Regolamento giuridico e tutele*, cit., 81. Considerazioni più prettamente politiche sono invece rappresentate in *Risoluzione*, cit., lett. R e S.

[71] *Risoluzione*, cit., 52 e 56.

A livello dottrinale, invece, si è auspicato che la disciplina della responsabilità civile dell'IA passi per regolamenti *ad hoc*, così da assicurare la massima uniformità possibile e, al contempo, da evitare norme vaghe e troppo generali in favore di soluzioni tagliate il più possibile sulla singola e specifica innovazione[72].

Invece, nel discorrere della responsabilità contrattuale connessa all'impiego di IA – es. inadempimento del robot nell'esecuzione del contratto - merita di essere segnalata la proposta di riconoscere ai robot una soggettività giuridica parziale avanzata da Gunther Teubner, la quale fa perno sul principio di eguaglianza, ossia su quell'imperativo «che – per gli eventi dannosi e per gli altri conflitti sociali pervenuti al cospetto del diritto – anche nello spazio digitale l'eguale sia trattato in modo eguale e il diseguale in modo diseguale»[73]. Dinnanzi al rischio di autonomia, ossia quello che «scaturisce dalla condotta, in linea di principio imprevedibile, degli algoritmi con autoapprendimento»[74], il grande giurista tedesco propone di considerare ciò che lui chiama «agente software» - e definisce come delle unità individue di interazione con gli uomini nei cui interessi prendono le decisioni – nei termini di un ausiliario del *dominus*\principale, di guisa che questi, anche quando a lui non si imputabile alcuna negligenza, risponderà degli inadempimenti della macchina *ex* art. 278 BGB[75]. Il fondamento di questa interpretazione analogica che consente di attribuire la responsabilità per l'inadempimento della macchina la cui condotta non è prevedibile risiede, lo si è detto, nel principio di eguaglianza: è questo che «reclama la responsabilità» del *dominus*. Difatti, rileva Teubner, se per l'esecuzione del contratto fosse impegnato, in luogo del robot intelligente, un uomo, non vi è dubbio che il suo principale risponda dell'inadempimento altrui, non si può ammettere che il dominus sia liberato solo perché l'esecuzione sia affidata a un robot intelligente[76].

Connesso alle questioni attinenti la responsabilità, aquiliana e contrattuale, è poi la proposta di esportare nel «governo della società algoritmica» il principio di spiegabilità che, sotteso al diritto di contestazione ex art. 22 GDPR, si sostanzia sia nel diritto a comprendere come la tecnologia funzioni sia nel definire chi debba dar conto per come essa funziona[77]. Dall'estensione di tale diritto alle applicazioni IA potrebbe discendere un obbligo di rendere disponibili, secondo una modalità «sufficientemente comprensiva», i dati che spiegano come abbia funzionato l'algoritmo e chi ne sia il responsabile. L'effetto di questa estensione del principio di spiegabilità dalla disciplina sul trattamento dei dati personali all'IA sarebbe notevole. Qualora il titolare del trattamento sostenga che, in ragione della complessità e inconoscibilità dell'algoritmo, egli non può fornire spiegazioni sul funzionamento lesivo della sfera altrui, egli sarà comunque responsabile. In alternativa, qualora quel titolare adempia all'obbligo di spie-

---

[72] A. Bertolini, *Artificial Intelligence and Civil Liability*, cit., 88.

[73] G. Teubner, *Soggetti giuridici digitali?*, cit., 127. Sull'eguaglianza nella costruzione della soggettività parziale dei robot operata da T., si v. anche la bella pagina di P. Femia, *Introduzione*, cit., 15.

[74] Ivi, 38.

[75] Ivi, 82.

[76] Ivi, 84. Sulla distinzione tra *legal agenthood* e *legal personhood*, si v., per tutti, U. Pagallo, *Vital, Sophia,* cit., 236.

[77] U. Pagallo, *Algoritmi e conoscibilità*, cit., 101.

gazione, il soggetto leso dal funzionamento dell'algoritmo sarà posto nelle condizioni di proteggersi e tutelarsi[78].

Per quanto attiene alla lesione dei diritti fondamentali, infine, è noto come il nostro sistema di tutela non ritenga sufficiente la sola risposta *ex post*. Orbene, proprio muovendo dalla consapevolezza che un approccio incentrato unicamente sulla responsabilità – e quindi successivamente alla lesione della sfera giuridica – sia incompatibile con il livello di protezione dei diritti fondamentali, nella dottrina più avvertita si propone l'estensione alla dinamica dell'IA del principio di precauzione (art. 191, co. 2, TFUE)[79]. In altri termini, al fine di fondare una «regolazione effettiva, di livello sovra-nazionale e sovra-legislativo, riguardante le tecnologie, vòlta ad evitare il verificarsi di violazioni delle libertà fondamentali non più (o molto difficilmente) rimediabili una volta che esse sono state diffuse»[80], si suggerisce di ricorrere al principio di precauzione[81], quale base giuridica idonea ad affermare la necessaria priorità della tutela dei diritti dell'uomo sulla tecnica[82].

In conclusione, contratti, responsabilità e diritti si confrontano con l'IA. Tale confronto agita la comunità degli interpreti che si sforza di definire principi – di effettività, di proporzionalità, di eguaglianza, di spiegabilità e di precauzione, etc. – con cui lottare per diventare una società giusta[83]: d'altra parte, ogni scienza ha i suoi tempi.

78 Ivi, 103.

79 Alla previsione eurounitaria, si aggiunga, sempre sul piano normativo internazionale, il principio 15, *Dichiarazione di Rio de Janeiro sull'ambiente e lo sviluppo* (1992): «Al fine di proteggere l'ambiente, gli Stati applicheranno largamente, secondo le loro capacità, il Principio di precauzione. In caso di rischio di danno grave o irreversibile, l'assenza di certezza scientifica assoluta non deve servire da pretesto per differire l'adozione di misure adeguate ed effettive, anche in rapporto ai costi, dirette a prevenire il degrado ambientale».

80 A. Simoncini, *L'algoritmo incostituzionale*, cit., 86.

81 Più in generale, è la stessa Commissione ad avere riconosciuto come il principio trova «applicazione in tutti i casi in cui una preliminare valutazione scientifica obiettiva indica che vi sono ragionevoli motivi di temere che i possibili effetti nocivi sull'ambiente e sulla salute degli esseri umani, degli animali e delle piante possano essere incompatibili con l'elevato livello di protezione prescelto dalla Comunità» (*Comunicazione della Commissione sul principio di precauzione*, 2000, (COM(2000)1 *final*, §3).

82 G. Passagnoli, *Regolamento giuridico e tutele*, cit., 83.

83 E. Garin, *La giustizia*, Napoli, 1968, 83.

Gli *smart contract*: riflessioni sulle prestazioni "autoesecutive" nel sistema di *blockchain*[*]

Enrico Labella

Abstract

Il progresso tecnologico e informatico ha portato alla creazione di registri informatici condivisi dove inserire in maniera permanente e immodificabile dati tradotti in codici alfanumerici. Ciò permette di registrare transazioni compiute a velocità superiori a quelle del pensiero umano e, quindi, incomparabili con quelle di un controllo giudiziale. Questo mondo informatico si può porre al di fuori dell'ordinamento, consentendo di autoregolarsi con norme non giuridiche in cui il soggetto debole rischia di non avere adeguate tutele. Un mondo che deve essere analizzato tramite strumenti che si collocano al di fuori della concettualizzazione giuridica tradizionale.

Technological and IT progress has led to the creation of shared IT registers where data being permanently and unchangeably translated into alphanumeric codes can be stored. This process makes it possible to record transactions carried out at higher speed than human thought and which are therefore incomparable with those of a judicial control. This computer world can work outside the legal system and be self-regulated by non-legal rules leaving the weaker subject at risk of not receiving adequate protection. Such world must be analysed through instruments that are outside the traditional legal conceptualisation.

Sommario

Keywords

smart contract - *blockchain* - autotutela esecutiva - innovazione - *disruptive technologies*

[*] Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

1. *Smart contract* e *blockchain*

Una delle rivoluzioni che l'avvento della tecnologia informatica ha portato nel campo del diritto e dell'economia è rappresentata senz'altro dalla *blockchain*. Grazie alla c.d. tecnologia *blockchain*, infatti, si è sviluppato, tra l'altro, un meccanismo completamente informatizzato di creazione e scambio di monete virtuali senza la necessità dell'intermediazione di banche e senza il doveroso controllo statale. E sulla tecnologia *blockchain* si è delineato un nuovo strumento giuridico-informatico, lo *smart contract*, la cui traduzione letterale dovrebbe essere "contratto intelligente" ma che, a ben vedere, di "contratto" ha ben poco (e forse di "intelligente" ne ha ancor meno)[1]. Affrontare il tema degli *smart contract* e della loro natura, se contrattuale o meno a dispetto dell'apparenza data dal *nomen* utilizzato, significa muovere dalla comprensione del meccanismo che sta alla base della tecnologia *blockchain* e, quindi, della *ratio* sottesa al recente intervento del legislatore italiano[2] che, in uno slancio di zelo regolatorio, ha cercato *in primis* di comprendere il fenomeno e *in secundis* di definirlo al fine, si suppone, di (cercare di) disciplinarlo compiutamente.

Il tema degli *smart contract* interseca necessariamente, quindi, quello della tecnologia *blockchain* giacché si può affermare che i primi costituiscono il prodotto giuridico della forza espansiva di quest'ultima. Per meglio dire, la capacità applicativa della tecnologia *blockchain*, molto al di là della seppur rilevantissima – sul piano economico e non solo – utilizzazione per lo scambio "sicuro" di monete virtuali, ha sollecitato la costruzione di un nuovo paradigma contrattuale – per alcuni[3] – ovvero di regolazione delle attività esecutive automatiche di contratti di scambio (e non solo) – per altri[4] – il cui esito è, ovviamente, ancora lontano da un approdo certo e stabile[5].

---

[1] Appare emblematica, sin dal suo titolo, la riflessione di F. Rampone, Smart contract*: né* smart*, né* contract, in *Rivista di diritto privato*, 2, 2020, 241 ss. V. anche J.A. Druck, *"Smart contracts" are neither smart nor contracts. Discuss*, in *Banking & Financial Services Policy Reports*, 10, 2018, 5 ss.

[2] Legge 11 febbraio 2019, n. 12, di conversione del decreto-legge 14 dicembre 2018, n. 135 (c.d. "Decreto Semplificazioni" che qui si indicherà anche con l'anno di emanazione, così da non confonderlo con tutti gli altri "decreti semplificazione" che sono adottati pressoché ogni anno in un Paese che, quindi, dovrebbe essere stato ormai semplificato al massimo).

[3] V. ad esempio L. Piatti, *Dal Codice Civile al codice binario*: *blockchain* e *smart contract*, in *Ciberspazio e diritto*, 3, 2016, 334; D. Di Sabato, *Gli* smart contracs*: robot che gestiscono il rischio contrattuale*, in *Contratto e impresa*, 2, 2017, 392; E. Battelli - E.M. Incutti, *Gli* smart contracts *nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, in *Contratto e impresa*, 3, 2019, 929.

[4] V. ad esempio S. Capaccioli*,* Smart contracts*: traiettoria di un'utopia divenuta attuabile*, ivi, 1-2, 2016, 34 ss.

[5] Nel panorama giuridico la *blockchain* gli *smart contract* sono sovente trattati insieme. Per limitarsi ai soli contributi italiani, tra gli altri, v.: A.U. Janssen - F.P. Patti, *Demistificare gli* smart contracts, in *Osservatorio di diritto civile e commerciale*, 1, 2020, 31 ss.; D. Fauceglia, *Il problema dell'integrazione dello smart contract*, in *Contratti*, 5, 2020, 591 ss.; F. Faini, Blockchain *e diritto: la «catena del valore» tra documenti informatici,* smart contracts *e* data protection*,* in *Responsabilità civile e previdenza*, 1, 2020, 297 ss.; M. Faioli - E. Petrilli - D. Faioli, Blockchain*, Contratti e lavoro. La ri-rivoluzione del digitale nel mondo produttivo e nella PA*, in *Economia e lavoro*, 2, 2016, 139 ss.; F. Bruschi, *Le applicazioni delle nuove tecnologie: criptovalute,* blockchain *e* smart contract, in *Diritto industriale*, 2, 2020*,* 262 ss.; F. Di Ciommo, Blockchain*,* smart contract*, intelligenza artificiale (AI) e* trading *algoritmico: ovvero, del regno del non diritto*, in *Rivista degli infortuni e delle malattie professionali*, 1, 2019, 1 ss.; G. Spoto, *Gli utilizzi della* Blockchain *e dell'*Internet of Things *nel settore degli alimenti*, in *Rivista di diritto alimentare*, 1, 2019; 25 ss.; F. Delfini, Blockchain*,* Smart Contracts *e innovazione tecnologica: l'informatica e il diritto dei contratti*, in *Rivista di diritto privato*, 2, 2019, 167 ss.; C. Frigerio - F. Rajola, Blockchain*, la nuova*

2. La *blockchain* secondo il legislatore italiano

Secondo il legislatore italiano, la *blockchain* è una tecnologia basata su registri distribuiti[6], definita dall'art. 8-*ter* del d.l. semplificazioni 2018 come «tecnologie e protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili». Quarantasette parole per definire in maniera "semplice" un fenomeno tecnologicamente complesso qual è quello della rete di registri distribuiti (DLT: *Distributed Ledger Technology*), senza però che si possa ritenere ci sia riuscito completamente[7].

La "semplicità" della definizione si presta quantomeno a due critiche, al di là dell'infelice formulazione linguistica adottata dal legislatore, certamente non agevolata dalle vicissitudini parlamentari della norma in sede di conversione: la definizione, per quanto articolata e astratta, appare modellata su un tipo ben determinato di *blockchain* quando in realtà vi sono più varianti; la definizione reca l'immodificabilità come elemento della *blockchain*, ma in informatica i concetti assoluti non esistono proprio per via dell'architettura del programma.

La *blockchain* è, dunque, un registro in cui immagazzinare dati, distribuito tra più utenti, i quali interagiscono come pari (*peer to peer*) senza la necessaria intermediazione di un *server* che consenta (e controlli) le transazioni scambiate tra gli utenti. Il *server* c'è, ma è solo una piattaforma che consente lo scambio non essendoci più il necessario rappor-

rivoluzione tecnologica, in *Vita e Pensiero*, 2, 2019, 69 ss.; F. Sarzana di Sant'Ippolito, Blockchain *e* smart contract *nel nuovo decreto semplificazioni*, in *Diritto di internet*, 1, 2019, 17 ss.; A.M. Gambino - C. Bomprezzi, Blockchain *e protezione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 3, 2019, 619 ss. ; M. Giuliano, *La* blockchain *e gli* smart contracs *nell'innovazione del diritto nel terzo millennio*, ivi, 6, 2018 989 ss.; P.P. Piraini, *Gli strumenti della finanza disintermediata: «*Initial Coin Offering*» e «blokchain*, in *Analisi giuridica dell'economia*, 1, 2019, 327 ss.; M. Esposito, *Non solo bitcoin: le potenziali applicazioni della* blockchain*,* in *Aggiornamenti sociali*, 6-7, 2018, 454 ss.; L. Patti, Blockchain*, decentralizzazione e privacy: un nuovo approccio del diritto*, in *Ciberspazio e diritto*, 1-2, 2018, 179 ss.; P. Matera, *Note in tema di* Blockchain *e assemblee delle società quotate nell'età della disintermediazione*, in *Comparazione e diritto civile*, 2018; M. Chierici, *La* blockchain*: una lettura giuridica per uno sguardo verso il futuro*, in *Ciberspazio e diritto*, 3, 2018, 385 ss.; L. Parola - P. Merati - G. Gavotti, Blockchain *e* smart contract*: questioni giuridiche aperte*, G. Cogliano, Blockchain*: un'innovazione tecnologica da studiare, scoprire e inventare*, in *Bancaria*, 12, 2017, 54 ss.; B. Cappiello, *Dallo "smart contract"* computer code *allo* smart (legal) contract. *I nuovi strumenti (para) giuridici alla luce della normativa nazionale del diritto internazionale privato europeo: prospettive* de jure condendo, in *Diritto del commercio internazionale*, 2, 2020, 477 ss.; A.S. Cerrato, *Appunti su* smart contract *e diritto dei contratti*, in *Banca, borsa e titoli di credito*, 3, 2020, 370 ss.; G. Castellani, Smart contracts *e profili di diritto civile*, in *Comparazione e diritto civile*, 2019; T. Pellegrini, *Prestazioni auto-esecutive.* Smart contracts *e dintorni*, ivi, 2019; M. Giaccaglia, *Considerazioni su* Blockchain *e* smart contracts *(oltre le criptovalute)*, in *Contratto e impresa*, 3, 2019, 941 ss.; G. Lemme, *Gli «smart contracts» e le leggi della robotica*, in *Analisi giuridica dell'economia*, 1, 2019, 129 ss.

[6] Per M. Giaccaglia, *Considerazioni su* Blockchain *e* smart contracts *(oltre le criptovalute)*, cit., 945, nt. 23, il rapporto tra la tecnologia basata sui registri condivisi e la *blockchain* sarebbe quello di *genus-species*.

[7] F. Sarzana di Sant'Ippolito, Blockchain *e* smart contract, cit., 1-3, descrive chiaramente l'*iter* di approvazione della disposizione in discorso e la tecnica normativa utilizzata, nonché riporta i dubbi e le critiche che suscita la definizione adottata. Ad esempio, dal punto di vista strettamente informatico (abbandonando, quindi, la specola del giurista), la definizione resa dal Decreto semplificazioni 2018 sembra descrivere un qualunque database cifrato e non solo quello su cui si fonda una *blockchain*.

to tra quest'ultimo e l'utente. Le transazioni sono assicurate tramite un meccanismo di crittografia e vengono archiviate se ritenute "valide" da un numero predefinito (solitamente la metà più uno) di utenti.
La *blockchain* è, quindi, un *database* dove vengono archiviati dei dati tradotti in stringhe o codici attraverso un meccanismo di crittazione basato principalmente sul sistema della chiave asimmetrica (ciascun utente possiede due chiavi, una privata e una pubblica generata da quella privata; ciascun utente critta la transazione con la chiave privata e comunica all'altra parte la chiave pubblica all'uopo generata al fine di decrittare i dati e verificarne la riferibilità alla transazione "concordata"). Tale archiviazione è ritenuta particolarmente sicura (ma non *assolutamente* sicura) giacché tali dati – ad esempio una serie di transazioni in moneta virtuale – sono archiviati in blocchi validati da particolari utenti (i c.d. *miner*) tramite la soluzione di un'operazione matematica. Più transazioni validate sono registrate in un blocco e su tale archiviazione si procede a una nuova archiviazione di blocchi di operazioni successive parimenti validate.
Rileva immediatamente una mancanza, quella di un intermediario che gestisca la catena. La validazione delle transazioni, poi chiuse e registrate in blocchi, non contempla la presenza di un "nodo centrale" della rete giacché il controllo è affidato a più *miner* che, per validare le transazioni e chiuderle in un blocco della catena, devono risolvere un'operazione matematica e tutti i *miner* (o comunque un numero predefinito) devono concordare con quell'esito. Il tutto avviene centinaia di volte in un singolo giorno per centinaia di migliaia di operazioni.
È possibile identificare, quindi, due momenti dell'intera operazione: la transazione vera e propria (ossia il trasferimento, ad esempio, di una somma di "denaro virtuale" da un conto all'altro); la validazione e registrazione della transazione in un blocco chiuso e, quindi, immutabile.
La transazione è quindi registrata sia per quanto riguarda il suo contenuto (la "somma di denaro" è, infatti, sostanzialmente una stringa alfanumerica che viene registrata come operazione passiva sul portafoglio virtuale del disponente e come operazione attiva su quello dell'accipiente), sia per quanto riguarda il tempo in cui è stata posta in essere, sia per quanto riguarda i soggetti coinvolti.
In realtà quest'ultimo è un elemento critico del meccanismo *blockchain* nel suo archetipo *permissionless*, ossia pubblico: chiunque può accedere alla rete da un qualsivoglia dispositivo senza necessità di autenticazione certa[8]. Va da sé che un sistema del genere consente l'utilizzo della tecnologia *blockchain* da parte anche di chi vuole sfruttare tale tecnologia per fini criminali approfittando dell'anonimato[9] (le altre due varianti sono la *blockchain permissioned* e quella ibrida: nella prima l'accesso è riservato previa registrazione e consegna delle credenziali dal server, mentre nella seconda l'accesso è

[8] M. Sarzana di Sant'Ippolito, Blockchain *e* smart contract, cit., 2, nt. 4, e F. Sarzana di Sant'Ippolito e M. Nicotra, *Diritto della* blockchain*, intelligenza artificiale e* IOT*,* Milano, 2018, 21 ss.

[9] Più precisamente, si tratta di sostanziale anonimato per via dell'utilizzo di pseudonimi (v. L. Piatti, *Dal Codice Civile al codice binario*, cit., 327, n. 7). Di particolare importanza è, comunque, il contrasto all'uso criminale del *web* e, più in particolare, della tecnologia *blockchain* tramite metodi in costante evoluzione (v. P. Dal Checco, Blockchain analysis*,* digital forensics *e indagini digitali attraverso la* blockchain*,* in R. Battaglini - M.T. Giordano (a cura di), Blockchain *e* smart contract. *Funzionamento, profili giuridici e internazionali, applicazioni pratiche*, Milano, 2019, *passim*).

libero ma la validazione e la conservazione delle transazioni avviene solo da parte di utenti selezionati). E proprio un quadro di tal guisa costituisce un'autentica sfida per il giurista, chiamato a confrontarsi con un mondo virtuale dove si sviluppa una certa socialità, ma con regole sovrapponibili – almeno in parte – a quelle che regolano gli scambi nella dimensione sociale c.d. reale.

3. Caratteristiche e benefici della *blockchain*

Dal quadro così sinteticamente tracciato è possibile desumere quattro caratteristiche della *blockchain* su cui il giurista deve confrontarsi: *i)* libertà di accesso e di registrazione: chiunque può accedere alla *blockchain*, interagire con gli altri utenti e conservare le transazioni della catena; *ii)* decentralizzazione: il *server* centrale rappresenta la piattaforma, ma senza funzioni di intermediazione (e quindi di controllo), mentre ogni "nodo" (ossia utente) ha la duplice funzione di *client* e di *server*; *iii)* immodificabilità dei blocchi di transazione una volta validati; *iv)* sicurezza delle transazioni[10].
I benefici di tale tecnologia sono ben evidenti. L'accesso e l'interazione libera e senza filtri, unita al mezzo telematico utilizzato, consente una facilità e rapidità delle transazioni nonché un abbattimento dei costi per barriere pressoché inesistenti (salvo quella del "linguaggio informatico" particolarmente tecnico che, per essere appieno compreso – anche se in realtà la completa conoscenza non è necessaria per il suo utilizzo – necessita di una preparazione altamente specialistica).
La decentralizzazione della registrazione delle transazioni rende più complessa la manipolazione dei blocchi, non consente un controllo accentrato delle transazioni in favore di un controllo più "democratico" (la validazione è consentita se concorda un numero predefinito – ad es. il 50%+1 dei "nodi" da parte degli utenti qualificati). Per poter manomettere il blocco occorre intervenire su più della metà dei nodi in cui è registrato il blocco di transazioni.
La transazione, una volta ultimata, validata e chiusa in un blocco, non è più modificabile e proprio sul blocco così chiuso (l'ultimo anello della catena, anche se la metafora non è tecnicamente corretta) verrà poi posto il blocco successivo contenente altre transazioni validate. Ciò scongiurerebbe il fenomeno del *double spending*, ossia la trasmissione più volte del medesimo contenuto digitale, come ad esempio criptovalute (si evita così che un utente spenda più volte lo stesso "denaro digitale"), e produce anche gli effetti giuridici della validazione temporale elettronica secondo quanto previsto dal reg. UE 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
Tutto ciò (l'assenza di barriere all'accesso del sistema, la decentralizzazione delle operazioni di controllo, la crittazione delle transazioni e la registrazione in blocchi immutabili) comporta una certa sicurezza delle transazioni giacché il contenuto digitale della stessa è "tradotto" in una stringa alfanumerica – che può contenere tanto queste poche pagine quanto tutta la biblioteca centrale giuridica – e di tale stringa vi sarà

[10] L. Piatti, *Dal Codice Civile al codice binario*, cit., 329 ss.; P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract*,* in *Nuova giurisprudenza civile commentata*, 1, 2017, 109.

solo una registrazione: un'altra transazione con la medesima stringa non potrà essere validata.

Fin qui la *blockchain* sembra la tecnologia perfetta per le transazioni immateriali, ma a ben vedere gli stessi punti di forza possono apparire come punti deboli, quantomeno dal punto di vista giuridico, e per evidenziare ciò si può riavvolgere il filo dei "punti di forza" appena esposti.

L'accesso e l'interazione libera e senza filtri, propria della *blockchain* che si può definire "pura" (ossia *permissionless*) può non consentire l'identificazione degli utenti e quindi di chi trasferisce o riceve il "bene digitale" come ad esempio la criptovaluta. Ciò può alimentare – anzi, senz'altro alimenta – il trasferimento di ricchezza praticamente senza alcuna traccia, agevolando transazioni criminali e bypassando qualsivoglia tipo di controllo, ma non solo. Oggetto di trasferimento tramite la *blockchain* può essere un qualsiasi file e quindi anche dati sensibili o, ed è ancor più grave, file illegali come video o foto a sfondo pedopornografico. Materiale, quindi, il cui trasferimento deve essere tracciato – e questo il sistema *blockchain* lo consente anche piuttosto bene – garantendo l'identificazione degli utenti (ad eccezione delle reti *permissionless*)[11].

Tutto il meccanismo di transazione avviene tramite stringhe alfanumeriche e algoritmi, ossia un linguaggio sconosciuto ai più e di difficile "traduzione": ciò determina una difficoltà particolare per definire il contenuto dello *smart contract*.

La facilità di accesso e transazione fa apparire la tecnologia *blockchain* come uno strumento futuristico che abbatte anche le barriere di costo infrastrutturale, ma così non è. Tutto il sistema poggia su "nodi", ossia su *computer*. Anzi, qui la parola più calzante è proprio la traduzione letterale che fin troppo presto è stata abbandonata in favore di quella inglese: *calcolatori*. E le macchine per poter calcolare hanno bisogno di un quantitativo di energia ormai non più trascurabile, il che genera un costo economico non solo per l'utente, ma anche per la collettività, diventando un costo sociale di cui l'ordinamento deve tener conto[12].

La decentralizzazione della registrazione in blocchi delle transazioni validate conferisce un potere diffuso di controllo e di validazione, ma non la sicurezza al cento per cento che, è bene ribadirlo, in informatica non esiste. Sicuramente la decentralizzazione rende complicatissimo manomettere le operazioni di validazione e registrazione, ma la complicazione non è data tanto da meccanismi "antintrusione", bensì dalla potenza che un dispositivo dovrebbe avere per "superare" gli altri dispositivi nel risolvere le operazioni matematiche. Ciò che ora è talmente complicato da rendere praticamente impossibile sviluppare la potenza di calcolo necessaria non è detto che lo sia anche domani. Anzi, è notizia di "ieri" che il più noto motore di ricerca su internet del mondo abbia sviluppato un calcolatore quantistico risolto capace di risolvere in

[11] P. Cuccuru, Blockchain *ed automazione contrattuale*, cit., 110.

[12] Si pensi che tutta la tecnologia delle varie *blockchain* sparse nel mondo ha comportato l'utilizzazione di un quantitativo di energia nell'anno 2017 pari a circa 35 terawatt (cioè 35 milioni di megawatt, 7 in più di quelli consumati da tutta l'Irlanda nello stesso anno) mentre per l'anno 2019 si stima che il consumo sia arrivato a 48 tW (cfr. L. Parola - P. Merati - G. Gavotti, Blockchain *e* smart contract, cit., 682, nt. 12). Sul punto si vedano anche le stime dell'Università di Cambridge, la quale ha creato uno strumento in grado di fare una stima – aggiornata costantemente – del consumo di energia di un *bitcoin* (il CBECI - Cambridge Bitcoin Estimate Index, consultabile sul sito *cebeci.org*).

qualche ora un'operazione che il più potente calcolatore tradizionale affronterebbe in diecimila anni.
Il meccanismo di *blockchain* dovrebbe scongiurare il fenomeno di *double spending* e, più in generale, garantire la tenuta del sistema da buchi, ma in realtà la seppur breve storia della *blockchain* ha già assistito ad un fenomeno di sfruttamento del rigido meccanismo di transazione, validazione e registrazione in favore di un vero e proprio "furto"[13].

4. L'utente "debole" e i pagamenti in criptovalute

La traduzione in una stringa alfanumerica del contenuto digitale rende necessario l'intervento di un "interprete" che renda intellegibile tale contenuto. Questo è il più grande limite all'applicazione della tecnologia *blockchain* e più in generale all'uso degli *smart contract*. Il linguaggio giuridico è fisiologicamente tecnico ma i concetti possono essere semplificati (a volte devono esserlo per legge) perché il soggetto coinvolto possa accedere all'istituto personalmente. Qui invece è assolutamente necessario un "interprete", ossia un informatico che abbia ricevuto una particolare formazione tecnica che gli consenta di "dominare" il meccanismo.
Ciò potrebbe sembrare in contrasto con uno degli aspetti positivi della tecnologia *blockchain* citati, ossia l'accessibilità a chiunque. Ovviamente il "chiunque" deve essere in possesso delle basi tecniche per interagire, ma neanche ciò è sempre vero. Occorre distinguere, infatti, gli utenti che usano la piattaforma per il solo scambio di contenuti digitali (ad esempio l'utente paga con un semplice *clic* e così facendo trasferisce somme di "denaro virtuale" o magari reale ma solo dematerializzato: in questo caso non occorre avere una particolare conoscenza che vada oltre quella che consente a chiunque di prenotare biglietti aerei tramite *smartphone*) dagli utenti che invece contribuiscono allo sviluppo del sistema, come ad esempio i *miners*.
La difficoltà del linguaggio informatico sostanzialmente divide gli utenti in due categorie: coloro che non hanno alcun dominio sul procedimento della *blockchain* e che, quindi, compreso il meccanismo base, si limitano a dare i comandi alla macchina affinché proceda con l'invio del "bene digitale"; coloro che, compresa la tecnologia *blockchain*, diventano utenti attivi e partecipano allo sviluppo della rete traendone un certo vantaggio. Va da sé che la stragrande maggioranza degli utenti appartiene alla prima categoria, ossia entra a far parte di una rete di cui non ne comprende le potenzialità e, soprattutto, i possibili rischi.
Uno dei settori di applicazione più importante e diffuso della *blockchain* è il *FinTech*[14], ossia quello della fornitura di servizi finanziari attraverso la tecnologia dell'informazione. Il sistema *blockchain* si è sviluppato realmente, infatti, attorno al fenomeno della criptovalute[15] divenendone parte integrante: non esisterebbe mercato di criptovaluta

[13] Si pensi ad esempio al "caso CoinDash" della rete *Ethereum*, ossia "furto" di 60 milioni di dollari in *Ether* nel 2016.

[14] S. Capaccioli, *Smart contracts*, cit., 25; per l'applicazione nel settore bancario v. E. Battelli - E.M. Incutti, *Gli* smart contracts *nel diritto bancario*, cit., *passim*.

[15] M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, in *Rivista di diritto civile*, 1, 2019, 197 ss., preferisce

senza il sistema di trasmissione *blockchain* e non esisterebbe una rete così estesa di *blockchain* se non ci fosse la criptovaluta. Si finisce per confondere, quindi, «lo scambio con la cosa scambiata».

Dal punto di vista fenomenologico, la criptovaluta è paragonabile all'acqua: assume la forma che gli si vuol dare. In termini di più ampio respiro, i concetti che ruotano attorno alla *blockchain*, alle criptovalute e agli *smart contract* vanno ben al di là dell'orizzonte analitico del giurista e sfuggono a una identificazione concettuale e di definizione difficilmente colmabile, salvo correndo il rischio di limitare, per l'appunto concettualmente, il fenomeno in discorso[16].

La criptovaluta è definibile, quindi, come moneta, valore, bene immateriale, diritto di credito, mezzo di pagamento, strumento finanziario, prodotto finanziario. Certo non è una moneta avente corso legale giacché è "coniata" da un programma informatico del tutto privato in cambio di denaro "vero" o in cambio di "attività" prestata alla rete (è il caso dei *miners* che, nella rete *blockchain* più famosa, ossia Bitcoin, sono "pagati" in bitcoin per la loro opera di validazione e archiviazione), per poi essere "scambiata" tra gli utenti, ma anche questo assunto è destinato ad essere ridimensionato[17].

Appaiono evidenti le caratteristiche delle unità di conto delle criptovalute: esse sono né più né meno che beni di carattere immateriale a cui la "comunità di utenti" attribuisce un valore ai fini dello scambio con altri beni immateriali, scambio che avviene secondo delle regole dettate dalla stessa comunità, o meglio dallo stesso *software* su cui le transazioni avvengono. Per usare le parole di Lessig «il codice è la legge»[18], con ciò evidenziando come gli ordinamenti giuridici siano in affanno, se non impotenti, nel cercare di regolare un fenomeno che in realtà si regola da sé, senza bisogno di interventi esterni come quelli dello Stato.

---

il termine *criptomonete* giacché le criptovalute non possono essere considerate valute in senso giuridico, dovendosi limitare il concetto di valuta alla sola moneta avente corso legale. Sul rapporto tra moneta e valuta v. T. Ascarelli, *Obbligazioni pecuniarie*, in *Comm. Scialoja-Branca*, Bologna-Roma, 1959, 8 ss., e B. Inzitari, *Moneta e Valuta*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, VI, Padova, 1983, *passim*.

[16] Ciò che è avvenuto, per l'appunto, con la definizione resa dall'art. 1, c. 2, lett. *qq)*, d.lgs. 25 maggio 2017, n. 90, secondo cui la moneta virtuale è «la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente». Ma la criptovaluta non è solo questo, ma è anche uno strumento di immagazzinamento e, quindi, di rappresentazione di una ricchezza apparentemente solo immateriale, ma che diventa materiale allorquando è la moneta virtuale stessa ad essere l'oggetto di transazioni operate su mercati non solo virtuali in uno schema non molto dissimile alle operazioni compiute su valuta estera negli usuali mercati di scambio di valute. V. in proposito R. Bocchini, *Lo sviluppo della moneta: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto dell'informazione e informatica*, 1, 2017, 27 ss.

[17] In realtà ai fini tributari la detenzione di criptovalute è considerata come investimento all'estero ai sensi degli artt. 1 e 4 d.l. 28 giugno 1990, n. 167, così come modificati dagli artt. 8 e 9 d.lgs. 90/2017. Di recente la giurisprudenza amministrativa ha anche chiarito che: «Le valute virtuali devono qualificarsi come "beni" immateriali, non svolgendo le funzioni tipiche della moneta, benché convenzionale, di unità di conto e riserva di valore, per via dell'estrema volatilità, nonché della mancanza di potere liberatorio nei pagamenti» (Tar Lazio, sez. II-ter, 27 gennaio 2020, n. 1077, in *Società*, 5, 2020, 566, con nota di N. De Luca - M. Passaretta, *Le valute virtuali: tra nuovi strumenti di pagamento e forme alternative d'investimento*).

[18] L. Lessig, *Code and Other Laws of Cyberspace*, 1999, *passim*.

In realtà il fenomeno di per sé non è così distante da quello ben più tradizionale della cessione di un bene immateriale da un soggetto all'altro: cessione di un bene immateriale (unità di conto della criptovaluta) a cui le parti coinvolte danno un certo valore. Lo scenario, però, si complica notevolmente intendendo la criptovaluta come moneta, ma non è questa la sede per approfondire il tema. Basti qui evidenziare, però, come il sistema della *blockchain* e delle criptovalute sia utilizzabile dai privati liberamente vista l'assenza di divieti o limitazioni particolari e, soprattutto, la riconosciuta libertà per i consociati di scegliere il mezzo tramite il quale soddisfare i propri bisogni economici e non. In questo caso il "mezzo" è, per la verità, un "sistema" basato su regole proprie, vincolanti per gli utenti, rigide, automaticamente applicabili a qualsivoglia transazione e poco, se non per nulla, controllabili da un'autorità statale.

5. La *blockchain* e lo *smart contract*

Chi entra nella rete *blockchain* accetta il suo "codice", informatico ma non giuridico, impermeabile a perturbazioni esterne quali l'intervento di un'autorità amministrativa o giudiziaria, o anche dalla stessa volontà delle parti, salvo che ciò non sia previsto dallo stesso codice (come, ad es., gli interventi soggetti esterni a cui la rete affida il potere di risolvere i contrasti tramite operazioni c.d. *multi-signature*[19]). Una volta che una transazione è avviata (e conclusa in una frazione di tempo calcolata in secondi o anche meno) non si può più tornare indietro, anche se ad esempio il negozio alla base di quella transazione sia stato dichiarato nullo. Semplicemente il codice, la "legge del rapporto informatico", non lo consente.

La rigidità del sistema delle *blockchain* può essere sfruttata in campo negoziale e proprio il suo utilizzo ha comportato una vera e propria svolta per lo *smart contract*, definito da Nick Szabo nel 1994 come un «protocollo di transazione computerizzato che esegue i termini di un contratto»[20]. Sempre secondo il suo ideatore, lo *smart contract* serve per «il soddisfacimento di condizioni contrattuali comuni (come ad esempio i termini di pagamento, i privilegi, la riservatezza e anche l'esecuzione), la riduzione al minimo delle eccezioni sia dannose che accidentali [ossia quelle dolose e non; *n.d.a.*] e la minimizzazione della necessità di intermediazioni fiduciarie. Gli obiettivi economici correlati includono l'abbassamento dei costi di perdita a causa di frodi, di arbitrato e di esecuzione e degli altri costi di transazione»[21].

La tecnologia *blockchain* consente di congegnare un contratto in cui l'esecuzione di determinate prestazioni – non sempre informatiche – è completamente automatica. Al verificarsi di un certo *input* il programma esegue la prestazione automaticamente, senza che né una delle parti né un terzo (come anche un'autorità giudiziaria) possano bloccare l'*output*. Il tutto alla velocità di un *clic*. Anzi, senza neanche un *clic* giacché l'esecuzione della prestazione è "certa".

Velocità e sicurezza (e quindi inevitabilità) dell'esecuzione della prestazione riducono a

[19] P. Cuccuru, Blockchain *e automazione contrattuale*, cit., 109-110.

[20] N. Szabo, *Smart contracts*, 1994.

[21] *Ibidem*.

zero – o quasi – il rischio di inadempimento giacché non vi può essere alcun comportamento del debitore che possa rendere il creditore insoddisfatto. Ma anche senza che l'esito dell'eventuale controllo giudiziale, fisiologicamente tardivo rispetto al momento in cui gli interessi in gioco vengono soddisfatti o in cui l'abuso viene perpetuato, possa incidere sul rapporto negoziale.

6. L'autoesecuzione dello *smart contract*

Il protocollo informatico è, quindi, un codice algoritmico su cui sono sostanzialmente riportate le clausole contrattuali e, quindi, gli *input* che determinano gli *output*, ossia le prestazioni che automaticamente vengono eseguite in base agli impulsi in entrata secondo la logica dell'ITTT (*If This Then That*): se si verifica A (o non si verifica entro un determinato termine) allora B.

Gli esempi possono essere i più vari e non tutti necessariamente presuppongono un rapporto totalmente informatizzato[22]. Ad esempio lo *smart contract* può facilitare le transazioni virtuali che destano ancora un certo scetticismo: l'utente non compra quel particolare bene immateriale perché non ha la certezza che al suo pagamento consegua l'adempimento dell'altra parte magari situata in un altro Paese. Ed ancora, un investitore non sottoscrive un determinato prodotto finanziario giacché al raggiungimento di un determinato valore di mercato non ha la certezza che gli verrà accreditata la cedola. Sul piano non completamente virtuale, lo *smart contract* può essere applicato al mercato energetico, dei beni strumentali, di quelli alimentari, al mercato degli acquisti con consegna a domicilio tramite una necessaria integrazione con il sistema di automazione di parti della casa. I piani di applicazione degli *smart contract* sono perciò due: il primo inerisce ai rapporti esclusivamente telematici, mentre il secondo contempla l'utilizzazione in una dimensione non solo virtuale.

Lo *smart contract* può però anche essere utilizzato in settori dominati da contratti con prestazioni corrispettive dove la valutazione sull'esatto adempimento di un'obbligazione che giustifichi l'esecuzione della prestazione dell'altra parte contrattuale non è sempre così netta. L'adozione dello *smart contract* in questo caso rischia di non lasciar margini di discrezionalità non tanto alla parte contrattuale (e anche su questo punto occorrerebbe un'approfondita valutazione) quanto all'intervento del giudice. La regola del mezzo tecnico (il "codice") prevale in cogenza sulla regola normativa.

A complicare ancor di più il quadro vi sono i rapporti negoziali in cui l'inadempimento non definitivo ha un certo margine di tolleranza o che comunque non giustifica l'interruzione dell'adempimento dell'altra parte. Si pensi, ad esempio, alla locazione dove l'inadempimento che conduce alla risoluzione del contratto e al successivo rilascio deve essere pari al valore di due mensilità del canone locatizio (e comunque occorrono una pronuncia giudiziale e una conseguente esecuzione particolarmente protettive nei confronti del conduttore inadempiente). Oppure il mercato del credito immobiliare ai consumatori, al credito fondiario assistito da un moderno patto marciano, o ancora al contratto di vendita con patto di riservato dominio, dove il mancato pagamento di

[22] V. l'ampia disamina di T. Pellegrini, *Prestazioni auto-esecutive*, cit., *passim*.

una sola rata che non superi l'ottava parte del prezzo non può dar luogo a risoluzione. Si immagini l'applicazione di uno *smart contract* in ciascuno dei summenzionati esempi. L'effetto nell'economia dei rapporti e più in generale in quella di mercato è dirompente.

Nel primo esempio (un locatore inadempiente all'obbligo di pagare il canone di locazione) il mancato incasso del canone, per qualsivoglia motivo, è l'*input* che genera l'*output*, ossia il blocco della serratura di accesso – debitamente collegata alla rete internet – affinché l'inquilino moroso non possa più godere del bene che non sta pagando.

Nel secondo esempio (acquisto di un immobile con nuovo patto marciano) il mancato pagamento di una o più rate determinate provoca istantaneamente il trasferimento del diritto di proprietà alla banca mutuataria, la valutazione del bene tramite algoritmo e l'accredito della somma al debitore detratto il debito verso la banca (se la posta è attiva).

Nel terzo esempio (acquisto in *leasing* di un'autovettura) il mancato pagamento del canone di locazione finanziaria determina il blocco del veicolo (magari consentendo comunque una manovra di messa in sicurezza che comunque il *computer* di bordo saprebbe valutare in tempo reale) o comunque il preavviso di blocco entro un prestabilito lasso temporale utile al locatario per condurre il veicolo a destinazione.

Si potrebbe obiettare che nella scrittura dell'algoritmo si possono prevedere le ipotesi in cui deve esserci una tolleranza del tardato adempimento, e quindi procedere al blocco della serratura dell'immobile in locazione solo con una mora pari a due canoni oppure al trasferimento del bene immobile dopo che l'inadempimento abbia raggiunto le diciotto mensilità. Più in generale, l'algoritmo può prevedere miliardi di ipotesi di *input* diversi, ma quello che più rileva è che sì lo *smart contract* può prevedere anche le clausole a contenuto obbligatorio o comunque la tolleranza dell'inadempimento, o ancora una valutazione sopraffina della prestazione dell'altra parte che fa scattare la controprestazione da parte dell'algoritmo, ma resta il problema di fondo: il controllo su una qualunque previsione contrattuale, demandato in teoria al giudice, semplicemente può non essere previsto dall'algoritmo e nessuna autorità può intervenire per contrastare gli effetti dell'automatismo, quantomeno alla stessa velocità dello *smart contract*. Cosa sia inadempimento, quali siano le cause del mancato pagamento – e imputabili o meno ovvero se sia la reazione a ciò che si ritiene un inadempimento dell'altra parte – se l'inadempimento deve considerarsi grave o meno ecc. lo deve decidere il giudice e non il *computer* poiché, in ultima analisi, ciò significherebbe delegare la "decisione" a chi ha creato l'algoritmo (ossia una parte o il terzo). Certo, è sempre possibile che il codice algoritmico preveda l'intervento di un giudice o di un terzo che agevoli l'adeguamento del contratto alle varie vicissitudini umane o naturali che possono verificarsi nella fase esecutiva del rapporto, ma ciò è sempre rimesso all'algoritmo e, quindi, si torna all'automatismo contrattuale.

Questo automatismo è, quindi, la cifra dello *smart contract* e occorre chiedersi se ciò lo proietti in una dimensione negoziale a sé stante ovvero se possa rappresentare solo un elemento applicabile a contratti "tradizionali".

7. La natura giuridica dello *smart contract*

La definizione che il legislatore italiano ha dato agli *smart contract* sembra propendere per la loro natura non negoziale in continuità con quanto espresso dal loro ideatore[23].
Per il secondo comma dell'art. 8-*ter* del Decreto Semplificazioni 2018 si definisce *smart contract* un «programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse».
Lo *smart contract* sarebbe, quindi, solo una modalità di esecuzione del contratto molto particolare, ma nulla di più. Una modalità di esecuzione che però prescinde da qualsivoglia attività umana, sia delle parti sia dei terzi. Ma tale qualificazione non risolve il problema dell'irreversibilità dell'effetto e della marginalizzazione del ruolo della tutela giudiziale.
L'automatismo delle prestazioni fuori dalla sfera di controllo delle parti non è, però, l'unica caratteristica rilevante dello *smart contract* giacché occorre evidenziare che l'applicazione della tecnologia *blockchain* consentirebbe il loro utilizzo tra utenti tra loro sconosciuti e che rimarrebbero tali anche dopo la conclusione del negozio.
L'accordo quale elemento costitutivo di ogni contratto prevede quantomeno una certa riconoscibilità delle parti al fine di poter decidere se e come contrarre, ma nel caso di *smart contract* applicato a una *blockchain permissionless* ciò non è possibile.
Ed ancora, lo *smart contract* è un programma fondato su un algoritmo. In esso vi è il regolamento contrattuale, la determinazione delle prestazioni e le modalità di adempimento, il tutto in un linguaggio per la stragrande maggioranza degli utenti completamente inaccessibile.
A ben vedere, quindi, si possono tracciare tre elementi caratteristici dello *smart contract*: *immutabilità* della dinamica negoziale sia agli interventi delle parti (o almeno una di esse) sia a quelli dell'autorità pubblica (sia giudiziale sia amministrativa); *incomprensibilità* ai più delle regole che governano la vita dello *smart contract*; *inimputabilità* delle prestazioni ad una parte certamente e giuridicamente individuata.
Ad interpretare lo *smart contract* determinando quando considerare completo un *input* non è più l'uomo, ma la macchina stessa, ovvero altri "soggetti" (che in realtà possono essere uomini o anche altri programmi informatici) chiamati *oracoli*, i quali trasformano gli *input* del mondo esterno in codici da inserire nello *smart contract* al fine di far scattare l'esecuzione ovvero variarne il contenuto.
Tutto ciò si discosta molto dall'idea di contratto fornita dal codice civile[24].
Per converso, secondo la normativa in esame, «gli *smart contract* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con le linee guida da adottare», con ciò considerando lo *smart contract* come un contratto avente forma

[23] Per T. Pellegrini, *Prestazioni auto-esecutive*, cit., la questione non è centrale come, al contrario, dovrebbe essere quella di regolazione delle prestazioni auto-esecutive, vero perno non tanto del "contratto intelligente" quanto delle "obbligazioni intelligenti" che lo compongono.

[24] Si assiste a una vera e propria «divaricazione […] tra *civil law* e *lex cryptographia*» (G. Lemme, Blockchain, smart contracts, privacy*, o del nuovo manifestarsi della volontà contrattuale*, in E. Tosi (a cura di), Privacy *digitale*, Milano, 2019, 323).

scritta.

In realtà neanche il legislatore ha preso una posizione netta sul fenomeno, anche se va dato atto che uno dei primi ordinamenti ad aver codificato lo *smart contract* è proprio l'Italia.

Una sorta di posizione di compromesso può essere rintracciata nell'ambito in cui è utilizzato lo *smart contract*: se applicato a contratti tradizionali, in cui vi è identificazione delle parti e certezza sul regolamento contrattuale, esso assume il ruolo di modalità di esecuzione informatica e automatizzata di un accordo sul quale però vi è comunque spazio per l'intervento umano ("filtri umani" da considerare nella programmazione del codice); se invece è applicato in un più ampio rapporto completamente virtuale, lo *smart contract* sarebbe il "contratto virtuale"[25] a cui sono legate le varie "prestazioni" poi validate, archiviate[26] ecc. Occorre evidenziare, però, che ciò in realtà non può essere considerato un compromesso tra natura negoziale o non negoziale dello *smart contract*, bensì una sorta di considerazione dello *smart contract* inteso come mero protocollo informatico di autoesecuzione di prestazioni e la fonte dell'obbligo di esecuzione di tali prestazioni: un "nuovo" contratto non inteso come nuovo tipo contrattuale contraddistinto dalla sussistenza delle esecuzioni automatiche e informatizzate delle prestazioni, bensì come operazione di carattere negoziale in cui la fonte è un rapporto negoziale "nuovo", dai contorni inediti rispetto a quanto può essere definito con i concetti tradizionali di "contratto", contraddistinto *anche* da prestazioni autoesecutive. In altre parole, con "*smart contract*" si può definire sia l'oggetto del contratto[27] sia, a volte (*recte*, in tutte le altre volte in cui le prestazioni autoesecutive informatiche non sono inserite in un negozio giuridico tradizionale), il contratto stesso. Per quest'ultimo caso è stata coniata una definizione: *smart legal contract*[28], ma ciò può risultare fuorviante. Lo *smart legal contract* (inteso, quindi, come sorta di rapporto negoziale da cui scaturiscono le prestazioni autoesecutive) non si colloca a metà strada tra il tradizionale negozio giuridico e lo *smart contract* inteso solo come protocollo informatico origine delle prestazioni autoesecutive, ma come fonte alternativa delle prestazioni autoesecutive medesime rispetto al contratto codicistico. Qui si finisce, però, in un'altra dimensione del diritto, dove si potrebbe chiamare questa nuova fonte negoziale come *post-contratto* o *contratto*

---

[25] Per il quale si pone il rilevante problema della formazione della volontà contrattuale delle parti (cfr. Lemme, Blockchain, smart contracts, privacy*,* cit., 311 ss.; v. anche N. Irti, *Scambi senza accordo*, in *Rivista trimestrale di diritto e procedura civile*, 2, 1998, 360 ss., la G. Oppo, *Disumanizzazione del contratto?*, in *Rivista di diritto civile*, 5, 1998, 525 ss., e la controreplica di N. Irti, *"È vero ma…" (replica a Giorgio Oppo)*, ivi, 1, 1999, 273 ss.

[26] Esemplare la legge dello stato americano del Tennesse (Senate Bill no. 22 marzo 2018, 47-10-202 C) laddove circoscrive l'area di applicazione degli *smart contract* alle attività di: *a)* custodire e istituire il trasferimento di attività sul registro distribuito; *b)* creare e distribuire risorse elettroniche; *c)* sincronizzare le informazioni; *d)* gestire l'identità e l'accesso degli utenti alle applicazioni *software*.

[27] Appare chiaro come anche i concetti giuridici per descrivere il "fenomeno" *smart contract* non siano usati in senso rigorosamente tradizionale non per sciatteria linguistica, bensì per inidoneità degli strumenti giuridici tradizionali ad essere applicati a concetti più informatici che legali.

[28] J. Stark, *Making Sense of Blockchain Smart Contracts*, in *www.coindesk.com/making-sense-smart-contracts/* (contributo del 4 giugno 2016), concetto poi ripreso e ampliato da M. Durovic - A.U. Janssen, *The formations of Blockchain-based Smart Contracts in the Light of Contract Law*, in *European Review of Private Law*, 6, 2018, 756 ss. Cfr. anche L. Piatti, *Dal Codice Civile al codice binario*, cit., 334-335.

postmoderno[29], con ciò evidenziando la "fuga in avanti" di tali concetti rispetto alla dimensione giuridica tradizionale e l'aspetto prevalente del dato informatico rispetto a quello legale.

In tutto questo, tuttavia, va tenuto fermo un punto: dal novero dei rapporti contrattuali su cui applicare gli *smart contract* vanno ovviamente esclusi quelli in cui la rilevazione dell'inadempimento e delle sue conseguenze deve necessariamente contemplare l'intervento giudiziale. Qui in gioco ci sono diritti di soggetti strutturalmente più deboli (come, ad esempio, il locatario) dove la vasta prateria del mondo informatico si può facilmente trasformare in una giungla in cui le regole esistono, ma sono quelle del più forte, cioè di chi sa destreggiarsi in un mondo più veloce e articolato (e oscuro) di quello del diritto.

[29] Con ciò identificando sia una dimensione ultronea rispetto a quella del contratto "tradizionale", sia anche un concetto in cui si evidenzia la crisi delle categorie giuridiche che si traduce in debolezza del concetto stesso identificato come post-moderno. Cfr. la condivisibile visione critica di S. Mazzamuto, *Il diritto post-moderno: un concetto inutile o addirittura dannoso?*, in *Europa e diritto privato*, 3, 2018, 845 ss., spec. 851., e cfr. anche i contributi sull'argomento, tra i tanti, di C. Salvi, *Diritto postmoderno o regressione premoderna?*, ivi, 865 ss.; E. Gliozzi, *Postmoderniscmo giuridico e giuspositivismo*, in *Rivista trimestrale di diritto e procedura civile*, 4, 2003, 801 ss.; M. Barcellona, *Diritto e nichilismo: a proposito del pensiero giuridico postmoderno*, in *Rivista critica di diritto privato*, 3, 2005, 207 ss.

I modelli di valuta virtuale: sistematica e definizione*

Carla Pernice

Abstract

Lo scritto, dopo aver esaminato l'eterogeneo panorama fenomenologico che compone la neonata categoria delle valute virtuali, si propone di indagare la natura giuridica dei vari tokens digitali attualmente in circolazione al fine di fornire proposte regolative adeguate nelle more di una disciplina civilistica di questi innovativi ritrovati tecnologici.

The paper, after examining the heterogeneous phenomenological panorama that makes up the newborn category of virtual currencies, aims to investigate the legal nature of the various digital tokens currently in circulation in order to provide adequate regulatory proposals pending a civil law regulation of these innovative technological goods.

Sommario

Keywords

valute virtuali – inquadramento giuridico – regolamentazione – moneta – obbligazioni crittomonetarie.

1. I modelli di valuta virtuale

Uno studio che voglia occuparsi dell'inquadramento giuridico delle crittovalute non può articolarsi in un discorso unitario. La neonata categoria, infatti, convoglia al proprio interno fattispecie estremamente eterogenee insuscettibili di *reductio ad unum*. Ogni specifica moneta digitale presenta meccanismi peculiari di funzionamento e qualità differenti, da tale distinguo, pertanto, occorre prendere le mosse.

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

Secondo la tassonomia al momento più accreditata, seppur non unanimamente condivisa[1] è possibile distinguere, con specifico riguardo alla "funzione" svolta dai gettoni elettronici, 3 tipologie di tokens:
- payment token (anche detti tokens di classe uno): mezzi di pagamento che consentono l'acquisto di beni e servizi su di una pluralità di piattaforme online, anche diverse da quella dalla quale il token trae origine. Questi gettoni digitali sono privi di diritti incorporati o passività e svolgono una funzione analoga alle valute tradizionali sebbene la loro volatilità talvolta ne determini l'uso a scopo di investimento (esempio paradigmatico è Bitcoin).
- ultility token: valute digitali a "circùito chiuso", ovvero a spendibilità limitata, che consentono l'acquisto di beni e servizi solo all'interno del sistema da cui traggono origine. Trattasi di tokens sovente emessi per agevolare lo sviluppo di progetti innovativi. Il prenditore del gettone, attraverso l'acquisto dello stesso, infatti, assume allo stesso tempo la veste di finanziatore e quella di futuro utente, precostituendo all'impresa una platea di clientela idonea a sostenerne lo sviluppo.
- security token (anche detti token di classe tre): gettoni digitali rappresentativi di diritti economici (quale il diritto di partecipare alla distribuzione dei futuri dividendi) e/o di diritti amministrativi (quale il diritto di voto su alcune materie).
Con particolare con riguardo agli attributi di *governance* invece si distinguono:
- Criptovalute decentralizzate, create e sviluppate in via diffusa da tutti gli aderenti al *network* (ne è un esempio Bitcoin)
- Criptovalute centralizzate, create e sviluppate da un unico soggetto proprietario del relativo protocollo informatico (ne costituiscono esempi Ripple, NEO, NEM e le Central Bank Digital Currency);
Ulteriore classificazione viene tradizionalmente condotta sulla base della maggiore o minore stabilità del valore delle Valute Virtuali. Nella prima categoria rientrano i c.dd. stablecoin, il cui valore è ancorato alla moneta fiat (es. Tether). Presentano un valore più altalenante le crittovalute il cui andamento è legato ad un bene materiale di riferimento come l'oro, o esclusivamente alla legge della domanda e dell'offerta, ossia al rapporto fra disponibilità sul mercato e numero di acquirenti.
Da ultimo si è soliti distinguere tra crittovalute convertibili o non convertibili a seconda che sia o meno possibile commutarle in valute fiat. Più nel dettaglio, tenuto conto della loro modalità di interazione con le monete correnti e con l'economia reale si definiscono:
– monete virtuali chiuse (tipo 1) quelle che non hanno interazioni con l'economia reale, non essendo acquisibili o convertibili con denaro "ufficiale", ma reperibili solo tramite attività online e spendibili solo per acquisti di beni virtuali o servizi offerti all'interno di una comunità virtuale.

[1] Il riferimento è a FINMA, *Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle* initial coin offering *(ICO)*, edizione del 16 febbraio 2018, in *finma.ch*. Ulteriori classificazioni si rinvengono nell'occasional paper della Banca d'Italia intitolato *Aspetti economici e regolamentari delle criptoattività* e reperibile sul sito dell'Autority. In dottrina cfr. R. Bocchini, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Dir. inf.*, 2017, 32 s.; S. Capaccioli, *Bitcoin e criptovalute*, in G. Cassano - N. Tilli - G. Vaciago (a cura di), *Tutele e risarcimento nel diritto dei mercati e degli intermediari*, Milano, 2018, 505 ss.; R. Vampa, *Fintech e criptovalute: nuove sfid per la regolazione dei mercati finanziarie*, in F. Fimmanò - G. Falcone (a cura di), *Fintech*, Napoli, 2019, 582 ss.

– monete virtuali unidirezionali (tipo 2) i tokens che possono essere acquistati anche con valuta corrente per essere utilizzate per l'acquisizione di beni o servizi virtuali o reali, ma che non possono però essere convertiti nuovamente in moneta legale.
– monete virtuali bidirezionali (tipo 3) i gettoni digitali pienamente convertibili, acquistabili e vendibili con valute correnti e utilizzabili per acquistare beni e servizi reali o virtuali (esempi sono Linden Dollars, Bitcoin).

2. *Criptocurrency* ed *e-money*: Analogie e differenze

A fronte di un così eterogeneo panorama fenomenologico il legislatore, italiano prima ed europeo poi, nel tentativo di offrire una sia pur embrionale disciplina del fenomeno, è intervenuto in materia con una definizione di valuta virtuale volutamente ampia. Ai sensi dall'art. 1, c. 2, lett. *qq)*, d.lgs. 231/2007, come modificato dal d.lgs. 4 ottobre 2019, n. 125 (attuativo della V direttiva antiriciclaggio) è «valuta virtuale: la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente». Secondo la direttiva europea n. 843 del 30 maggio 2018 è valuta virtuale: «una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo *status* giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente»[2].
Chiara e netta è la differenza tra le nozioni testè riportate e quella di moneta elettronica contenuta all'art. 1, c. 2, h-ter del Testo Unico Bancario che descrive *l'e-money* come «il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento […] e che sia accettato da persone fisiche e giuridiche diverse dall'emittente». La disciplina in materia utilizza tre criteri fondamentali per definire la moneta elettronica, che deve: 1) essere conservata elettronicamente; 2) essere emessa dietro ricezione di fondi di importo non inferiore al valore monetario memorizzato; 3) essere accettata come mezzo di pagamento da soggetti diversi dall'emittente.
Sebbene la maggior parte degli schemi di moneta virtuale differiscano dai sistemi di moneta elettronica per il fatto di non fare riferimento ad alcuna valuta corrente con valore legale, deve rilevarsi che alcuni gettoni digitali potrebbero rientrare nella nozione di *e-money*, si pensi agli stablecoins prima esaminati. Essi, frequentemente, sono emessi da un soggetto giuridico a fronte di una unità moneta - secondo un rapporto di

[2] Rileva F. Di Vizio, *Le cinte giudiziarie del diritto penale alla prova delle valute virtuali degli internauti*, in *penalecontemporaneo.it*, 2018, 52, che nelle definizioni elaborate è posto in risalto l'impiego delle valute virtuali quale mezzo di scambio, restando invece tralasciata la loro possibile detenzione a scopo di investimento. Difatti, prima della riforma di cui al d.lgs. 125/2019, anche la nozione italiana di Valuta Virtuale faceva esclusivo rifermento alla possibilità di impiegare i gettoni crittografici quali strumenti di scambio.

uno a uno con le monete aventi corso legale - segregata presso il soggetto emittente. Laddove risultino integrate le caratteristiche operative di cui all'art. art. 1, c. 2, h-*ter* TUB tali valori potrebbero essere ricondotti alla disciplina sulla moneta elettronica.
Diversamente non sono certamente riconducibili alla nozione di moneta elettronica i tokens di prima classe (anche detti autoreferenziali poiché non rappresentano null'altro che se stessi), come Bitcoin. Bitcoin è conforme al primo e al terzo dei requisiti indicati nella nozione di *e-money*, ma l'aspetto chiave dell'attività di *mining*[3], che porta alla creazione decentralizzata di moneta, in quanto svincolata dalla ricezione di fondi di valore equivalente al valore monetario emesso (o estratto), impedisce l'applicazione a tale ritrovato tecnologico del quadro normativo sulla moneta elettronica. Bitcoin non rappresenta un mezzo di pagamento alternativo pur sempre regolato in valuta avente corso legale, bensì una moneta convenzionale espressa in una propria unità di misura accettata per eseguire pagamenti e talvolta impiegata per finalità speculative. La riconducibilità di questa crittovaluta al concetto di moneta elettronica deve dirsi, pertanto, pacificamente esclusa.

3. Valute virtuali e criptomonete "istituzionali"

Lo sforzo definitorio compiuto dai legislatori europei, seppur apprezzabile poiché evidenzia le principali caratteristiche delle criptovalute[4], esclude dal proprio perimetro applicativo le *central bank digital currencies* vale a dire le monete criptate che riproducono sul piano digitale le attuali monete fiat. Trattasi di vere e proprie valute aventi corso legale, come tali emesse dallo Stato ed irricusabili, la cui unica peculiarità riposa nella tecnologia che ne governa il sistema di creazione e scambio[5]. Tanto il d.lgs. n. 231 del

[3] Il *Mining* è l'attività svolta in seno alla blockchain che conduce alla creazione e all'attribuzione di nuove unità di Bitcoin. Le nuove unità di valuta virtuale, segnatamente, vengono generate come premio accordato dalla rete agli utenti (miners) che contribuiscono, in concorrenza fra loro, alla sua gestione ed alla sua sicurezza, mettendo a disposizione le capacità di calcolo dei propri computer per verificare, tramite la soluzione di complessi problemi informatici, l'univocità e la sicurezza delle transazioni effettuate.

[4] La comunità virtuale, ad onor del vero, non ha accolto con favore definizione di valuta virtuale contenuta nella direttiva europea n. 843 del 30 maggio 2018. Non si condivide, ad esempio, l'impiego della congiunzione con valore avversativo «ma» (non presente nel d.lgs. 90/2017), quasi a sottolineare che "benché" le valute virtuali non siano nulla di quanto descritto prima, "ciononostante" ed "inspiegabilmente" vengono comunque accettate in pagamento.
Si contesta il silenzio, nella descrizione, di due elementi fondamentali che stanno alla base della efficacia tecnica delle criptovalute come mezzo di scambio: la circostanza che è basata sulla crittografia (caratteristica che ne rende univoco ed irripetibile l'utilizzo) e che è registrata nella *blockchain* (tecnologia che ne archivia e certifica l'uso in termini planetari). S. Rizzini Bisinelli, *Una definizione europea di Criptovalute*, in *bitconio.net*, ad esempio, propone quale definizione alternativa la seguente: «"la valuta virtuale è un mezzo di scambio accettato da persone fisiche e giuridiche, non emessa o garantita da una banca centrale o da un ente pubblico, che può essere trasferita, memorizzata e scambiata elettronicamente come rappresentazione digitale di valore"; magari aggiungendo tra le parole "scambio" e "accettato" la locuzione "basata sulla crittografia e registrata sulla *blockchain*"».

[5] Sul tema si veda lo studio della *Committee on Payments and Market Infrastructures* intitolato *Central bank digital currencies* e reperibile in *bis.org* nonché L. Scipione, *Le valute digitali sovrane tra stabilità e concorrenza. Perno di un nuovo sistema finanziario globale o inganno demagogico?*, in *Inn. dir.*, 3, 2019, 3, 1 ss. e ivi ulteriore bibliografia.

2007 quanto la direttiva europea n. 843 del 2018, infatti, testualmente discorrono di «rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica».

Il motivo dell'estromissione può, probabilmente, essere compreso solo avendo a mente il contesto normativo entro cui la nozione di valuta virtuale è dettata. Tanto la disciplina italiana, quanto quella europea, difatti, si occupano del fenomeno criptomonetario al fine di prevenirne il possibile impiego per finalità illecite[6]. Il principio di stretta legalità che governa le sanzioni pubblicistiche in un con il divieto di applicazione analogica delle previsioni penali ha presumibilmente reso necessario l'introduzione di un concetto autonomo che consenta la punibilità delle condotte proibite aventi ad oggetto questi nuovi beni digitali. Esigenza, questa, non avvertita per le CBDC potendo le stesse essere ricondotte alla nozione di moneta avente corso legale.

Ulteriori rilievi però possono essere compiuti a margine delle disposizioni poc'anzi esaminate. Colpisce, in *primis*, l'inciso «non possiede lo *status* giuridico di valuta o moneta» contenuto nella disciplina europea ma non anche in quella domestica. L'esclusione della natura valutaria verosimilmente si lega al frammento normativo che precede la precisazione: poiché la neonata categoria per volontà legislativa non comprende le monete emesse da autorità pubbliche, giocoforza non può discorrersi di valuta. Più ambiguo il disconoscimento della natura monetaria di questi nuovi valori virtuali, vieppiù considerato che la stessa Corte di Giustizia, chiamata a pronunciarsi in via interpretativa sull'applicabilità della direttiva IVA all'attività di conversione di Bitcoin in moneta avente corso legale, ha equiparato in fatto di regolamentazione fiscale le valute virtuali a quelle battute dalle banche centrali[7]. Invero, la ragione dell'inciso può trovare giustificazione nella circostanza che le disposizioni in parola non si preoccupano di fornire una precisa qualificazione civilistica del fenomeno, ad esse premendo esclusivamente pervenire alla tracciabilità delle operazioni effettuate in criptomonete[8]. A tali norme pertanto deve essere riconosciuta una limitata funzione, che seppur rilevante sul piano interpretativo, deve tener conto degli scopi ed i confini ordinamentali entro i quali è dettata. La specifica funzionalità settoriale della previsione, in uno con l'estrema eterogeneità e dinamicità delle valute virtuali, lascia dunque ancóra aperto il quesito relativo alla disciplina privatistica di questi innovativi gettoni crittografici privati.

---

[6] Si veda però, piú di recente, la proposta di regolamento europeo sui mercati in cripto-attività del 24 settembre 2020. Sul punto F. Annunziata, *Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE*, in *Dirittobancario.it*.

[7] CGUE, C-264/14, *Skatteverket c. David Hedqvist* (2015). Nel 2016 l'Agenzia delle Entrate, con la risoluzione 2 settembre 2016, n. 72/E (in risposta all'interpello di un operatore intermediario in criptovalute), sulla scia di quanto affermato dalla Corte di Giustizia, ha assimilato l'attività di intermediazione in criptovalute alle operazioni relative a divise, banconote e monete con valore liberatorio, previste dall'art. 135, par. 1, lett. *e)*, della direttiva 2006/112/CE.

[8] Concorde V. De Stasio, *Le monete virtuali: natura giuridica e disciplina dei prestatori di servizi connessi*, cit., 216. Si esprime nel senso che la nuova definizione escluderebbe «in maniera *tranchant*» la possibilità di considerare le valute virtuali non quali monete I. Bixio, *Le valute virtuali nella V Direttiva antiriciclaggio*, in *Corr. trib*., 2018, 1989 s. Se cosí fosse, però, la nozione comunitaria allontanerebbe, se non addirittura impedirebbe, l'assimilazione delle valute virtuali a quelle aventi corso legale, contraddicendo la stessa disciplina posta dalla direttiva europea (e non solo) che invece si muove nel senso di una progressiva equiparazione dei mezzi di pagamento istituzionali e convenzionali.

4. Un possibile inquadramento dei gettoni digitali "privati"

Acclarata la profonda disomogeneità con la quale, in concreto, può manifestarsi il fenomeno crittomonetario appare chiaro che l'inquadramento giuridico dei vari tokens digitali "privati" non può che procedere dall'analisi dello scopo e dalla funzione perseguiti dal singolo gettone. I tokens "meno problematici" da questo punto di vista appaiono quelli che incorporano diritti nei confronti di chi li ha generati o soggetti terzi. Quelli che attribuiscono il diritto ad un pagamento specifico o a pagamenti futuri sono stati paragonati ai valori mobiliari; quelli che consentono di usufruire di un determinato servizio sono stati ricondotti ai c.dd. vouchers[9], ovvero, a seconda del diritto contemplato, ai titoli rappresentativi di merci (quando con il possesso del token possa riceversi un bene anche immateriale) o ai documenti di legittimazione (qualora il token legittimi a ricevere una prestazione anche presso terzi); i gettoni che attribuiscono diritti amministrativi o economici, invece, sono stati assimilati alle azioni societarie[10]. La categoria più controversa rimane quella dei tokens che non rappresentano alcun valore sottostante e non attribuiscono al proprietario diritti ulteriori rispetto a quello di proprietà del gettone medesimo. Questa classe di tokens, rispetto alla quale rappresenta esempio emblematico Bitcoin, viene sovente utilizzata come mezzo di scambio per il pagamento di beni e servizi, ciononostante si registra una certa ostilità ad attribuirgli il valore giuridico di moneta. Le obiezioni mosse a tale qualificazione, tuttavia, non appaiano dirimenti: non quella che fa leva sul necessario monopolio dell'emissione. In materia il dibattito è ancóra acceso e gli stessi economisti sono divisi tra quanti sostengono la teoria sociale del denaro e quanti ne asseriscono l'essenza istituzionale[11]. Che l'emissione statale non rappresenti un requisito indefettibile del concetto, però, pare trarre conferma nella circostanza che essa costituisce un'acquisizione relativamente recente. L'opportunità di riconoscere ad un unico soggetto il potere di battere moneta, infatti, era ancóra nella prima metà del sec. XIX al centro di un acceso dibattito fra tre correnti di pensiero: la scuola bancaria classica, la *currency school* (o scuola metallica) e la *free banking school* (scuola bancaria liberista)[12].

[9] Cfr. l'atto dell'Agenzia delle Entrate n. 14/2018 reperibile su *agenziadelleentrate.gov.it.*

[10] Sul Punto, S. Aceto di Capriglia, *Illeciti criptovalutari. Note comparatistiche*, Napoli, 2020, 74 ss. al quale si rinvia per ulteriori approfondimenti sulla letteratura straniera in materia.

[11] Ritiene che possa essere definita moneta solo quella battuta dallo stato F.A. Mann, il cui pensiero è riportato da C. Proctor, *Mann on legal aspect of money*, Oxford, 2012, 15 ss. In Italia il pensiero di Mann sembra essere condiviso da B. Inzitari, *La moneta*, in B. Inzitari - G. Visentini - A. Di Amato (a cura di), *La moneta-la valuta*, Padova, 1983, 6. Alla teoria statalista delle valute si contrappone la teoria di Savigny, poi sviluppata da Nussbaum, secondo il quale è la società a decidere quale valuta adottare (cfr. A. Nussbaum, *Money in the law*, Chicago, 1939, 28). In verità il contrasto tra le due vedute è piú apparente che reale considerato che persino i piú rigorosi difensori della teoria statalista, come Knapp, sostengono che lo Stato è in fondo il regolatore ed il piú antico organizzatore di una *payment community* (G.F. Knapp, *The State theory of money*, London, 1924, 128, scrive: *«any other payment community may create money of its own»*). Cosí come i fautori della *society theory of money* sono costretti a riconoscere la centralità dello Stato nella promozione e difesa della moneta.

[12] Secondo gli esponenti di quest'ultima dottrina (*free banking*) (in particolare Hayek, il quale scrisse il famoso testo intitolato *Denationalisation of money*, London, 1976, e Friedman, le cui teorie sono espresse nel volume *Should There Be an Independent Monetary Authority?*, in L.B. Yeager (a cura di), *In Search of*

Non persuade altresì l'eccezione legata all'instabilità del valore. Com'è stato recentemente osservato dalla Corte d'Appello di Berlino chiamata ad esprimersi su questioni analoghe, in alcuni paesi esistono valute estremamente deboli e volatili ma ciò non osta alla loro considerazione quali monete[13].

Nè vale asserire che può essere qualificata "moneta" soltanto il mezzo di pagamento universalmente accettato che è espressione delle potestà pubblicistiche di emissione e di gestione del valore economico[14]. Questa ricostruzione non convince per molteplici ragioni: anzitutto postula che la moneta sia uno strumento ad accettazione totalitaria[15], laddove, non esistendo nel mondo un bene dotato di utilità universale deve per forza di cose sposarsi una teoria di moneta relativa[16]. Inoltre, come rilevato dalla giurisprudenza tedesca poc'anzi citata, alcune monete aventi corso legale non godono di un riconoscimento generale nemmeno nel paese di emissione in quanto si preferisce ricorrere a valute più stabili[17]. Tale requisito pertanto non dovrebbe essere richiesto.

---

a Monetary Constitution, Cambrige Massachusetts, 1962) l'emissione di biglietti doveva essere libera, il sistema bancario doveva funzionare secondo i princípi del libero scambio anche su questioni cruciali quali l'emissione di mezzi monetari convertibili in oro. Si auspicava che tutte le banche avessero potere di emissione e non si riconosceva il ruolo di un'autorità monetaria centrale (Banca Centrale). Tale impostazione estrema fu confutata sia dagli esponenti della scuola bancaria classica (Fullerton, Tooke e John Stuart Mill) sia da quelli della scuola metallica (dottrina, sorta in Gran Bretagna nella prima metà del XIX secolo, facente capo ad un gruppo di statisti ed economisti tra i quali R. Torrens, S.J. Lloyd, McCulloch e Lord Overstone), entrambi favorevoli all'istituzione di una Banca Centrale dotata di potere di monopolio sull'emissione di moneta. Tuttavia, mentre i secondi proponevano che fossero stabilite delle regole di proporzionalità tra le variazioni della quantità di banconote in circolazione e le riserve in oro, i primi non lo ritenevano necessario, in quanto per mantenere costante il livello dei prezzi si riteneva sufficiente il semplice mantenimento della regola di convertibilità aurea. Innegabilmente il progetto Bitcoin affonda le proprie radici nel pensiero di Hayek, tuttavia differisce da questo in quanto il valore della moneta libera non è garantito da un sottostante (oro). Sotto tale aspetto Bitcoin evoca la proposta keynesiana avanzata durante gli accordi Bretton Woods, che prevedeva la creazione di un ente sovranazionale che avrebbe emesso una moneta a circolazione universale, il *bancor*, non convertibile in oro, dal quale tuttavia differisce, appunto, proprio per l'assenza di un centro emittente. Per approfondimenti sull'evoluzione storica del denaro sia consentito il rinvio a C. Pernice, Digital currency *e obbligazioni pecuniarie*, Napoli, 2018, 9-34 e ivi ulteriore bibliografia.

[13] Recentemente in questo senso la Corte d'Appello di Berlino, 25 settembre 2018: *«Es gibt demnach auch äußerst schwache oder wertunbeständige Devisen. Dass diese ungern und deswegen selten international verwendet werden, ändert nichts an ihrer Einordnung als Devisen. Der Gesetzgeber hat keine Vergleichbarkeit zu "wertstabilen Devisen" oder "häufig und gern verwendeten Devisen" vorausgesetzt. Eine Vergleichbarkeit mit Devisen ist also nicht schon deswegen abzulehnen, weil Bitcoin erheblichen Wertschwankungen unterliegen»*.

[14] Cass., 2 dicembre 2011, n. 25837, in *Dejure online*.

[15] Afferma che «lo strumento di scambio di denaro deve essere necessariamente universale» B. Inzitari, *La natura giuridica della moneta elettronica*, in S. Sica - P. Stanzione - V.Z. Zencovich (a cura di), *La moneta elettronica: profili giuridici e problematiche applicative*, Milano, 2006, 25.

[16] In argomento E. Betti, *Teoria generale del negozio giuridico*, ristampa, Napoli, 2002, 53 nota 14: «che del resto la valutazione di utilità sociale sia per se stessa qualcosa di essenzialmente relativo ad un soggetto, ad un'epoca storica e ad un determinato ambiente di cultura, quindi qualcosa di storicamente contingente e variabile, si comprende senza difficoltà». L. Mosco, *Gli effetti giuridici della svalutazione monetaria*, Milano, 1948, 27 ss. scrive: «la storia economica ci insegna che le cose assunte come danaro nel mondo degli affari sono svariatissime secondo i tempi e i luoghi». In ragione di ciò «non è possibile delineare secondo un criterio generale l'evoluzione monetaria, poiché ciascun paese, in tale scelta, agí secondo circostanze sue proprie».

[17] La Corte d'Appello di Berlino, 25 settembre 2018, cit., a proposito della comparabilità di Bitcoin alle valute straniere ha osservato: *«Ferner ist die Voraussetzung einer allgemeinen Anerkennung nicht herleitbar. Es gibt Devisen, die sich keiner allgemeinen Anerkennung erfreuen. Es ist allgemein bekannt, dass es teilweise Fremdwährungen*

In una prospettiva funzionale, piuttosto, può osservarsi che Bitcoin, come la *fiat money*, si distingue dagli altri beni giuridici per il fatto di non soddisfare l'immediato bisogno della controparte, rinvenendo la propria utilità nella possibilità di essere impiegato per il successivo acquisto di beni e servizi. Al pari degli attuali mezzi di pagamento legali esso non è né bene di consumo (non essendo idoneo a soddisfare in via immediata un bisogno dell'individuo) né bene "produttivo" (non essendo impiegato per la produzione di altri beni) ma entità naturalmente destinata alla circolazione in quanto non ha altra possibilità di utilizzo se non quella di fungere da intermediario nei commerci[18]. In ciò differisce da altri asset, come ad esempio l'oro che è bene dotato anche di valor d'uso. Bitcoin funziona come moneta tra gli attori che lo impiegano, e l'interesse di colui il quale riceve o dispone di una moneta virtuale è il medesimo di quanti si accingono a compiere transazioni per il tramite di valute correnti: ottenere o conferire un potere economico d'acquisto spendibile all'interno di un determinato circùito economico[19].

L'analisi "strutturale" di questo ritrovato tecnologico conferma l'assunto. Bitcoin possiede le medesime caratteristiche empiriche del denaro: è un bene giuridico generico, fungibile, inconsumabile, indeteriorabile e fruttifero. Difatti la crittovaluta viene presa in considerazione per la sua appartenenza ad un genere e non nella sua individualità specifica[20]. È inconsumabile ed indeteriorabile essendo volta alla infinita circolazione.

gibt, die selbst im Ausgabestaat nur ungern angenommen werden, da man eher auf stabilere Fremdwährungen (z. B. US-Dollar) zurückgreifen möchte. Diese Fremdwährungen erfreuen sich auch in Form von Devisen keiner allgemeinen Anerkennung Diese Fremdwährungen erfreuen sich auch in Form von Devisen keiner allgemeinen Anerkennung. Selbst das vom Gesetzgeber genannte Beispiel des ECU belegt dies. Dieser war nicht allgemein anerkannt. Er wurde nur vielmehr von einem bestimmten Kreis von Personen und Einrichtungen genutzt. Für den allgemeinen Rechtsverkehr war er mehr oder weniger bedeutungslos. Der Rechtsverkehr nutzte vielmehr die jeweiligen nationalen Währungen. Demnach müsste es genügen, dass eine bestimmte Gruppe die fragliche Einheit nutzt. Eine allgemeine Anerkennung ist nicht zu fordern. Eine solche beschränkte Gruppe von Nutzern von Bitcoin lässt sich erkennen. Allein die Tatsache, dass einige Händler Bitcoin zu Zahlungszwecken akzeptieren belegt dies».

[18] Afferma che Bitcoin è moneta in quanto strumento di pagamento «accettato dalle parti di una transazione quale mezzo di pagamento alternativo […] (non avente) altre finalità oltre quella di un mezzo di pagamento» CGUE, C-264/14, cit. *Contra* M. Mancini, *Valute virtuali e "Bitcoin"*, in *An. giur. econ.*, 2015, 1, 122 e R. Razzante, *"Bitcoin" e monete digitali. Problematiche giuridiche*, in *Gnosis*, 2014, 2, 113; G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del "Bitcoin": miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. inf.*, 2015, 419.

[19] *Contra* E. Girino, *Crirptovalute: un problema di legalità funzionale*, in *Riv. dir. banc.*, 2018, 10, 18 ss. secondo il quale un acquisto che preveda il pagamento del corrispettivo in crittovalute ha quale unica funzione quella di realizzare un investimento speculativo: «E l'assolve per entrambe le parti. Se nella prospettiva del venditore non v'è alcuna plausibile e oggettiva ragione di esporre a rischio il valore certo di un incasso se non la volontà di trasformare istantaneamente quell'incasso in uno strumento di speculazione, nella prospettiva dell'acquirente, la spendita della criptovaluta sottende egualmente un atto di speculazione, con la sola differenza che la cessione della valuta virtuale materializza, con certezza, il risultato di una speculazione pregressa, costituendone il completamento. Non v'è anche qui alcuna razionalità nel pagare in criptovaluta, al cambio attuale della stessa, il controvalore del bene se non nel caso in cui la valuta virtuale sia stata acquistata ad un cambio inferiore a quello corrente al momento del pagamento».

[20] In tal senso recentemente Trib. Firenze, 21 gennaio 2019, n. 18, in *Le Corti fiorentine*, 2019, 2, 71 ss. Non persuade al riguardo l'obiezione di quanti asseriscono che il codice informatico che individua univocamente ciascuna valuta virtuale varrebbe a rendere a ciascun pezzo di crittovaluta unico e irripetibile (G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del «Bitcoin»: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, cit., 428) . Com'è stato giustamente osservato «il fatto che un bene generico possa essere riconoscibile non fa venir meno […] la circostanza che esso sia perfettamente sostituibile con gli altri dello stesso genere. Si pensi al fatto che ogni pezzo cartaceo di

Trattasi inoltre di bene fruttifero poiché, similmente al denaro, qualora venga dato in prestito è idoneo a produrre interessi. conclusione questa che discende dal fatto che Bitcoin ha acquisito nel corso del tempo il valore di mezzo di scambio riconosciuto da una larga parte della comunità virtuale[21].

Non sembrano allora sussistere ostacoli teorici alla possibilità di estendere l'applicazione alcune regole previste in tema di prestazioni pecuniarie alle obbligazioni aventi ad oggetto Bitcoin[22]: con la precisazione che in ragione del caso concreto e delle esigenze di tutela sottese al singolo episodio potranno altresì operare tutte le norme presenti nell'ordinamento che pur pensate per contesti giustificativi differenti[23], risultino compatibili ed adeguate alla fattispecie controversa[24].

5. Obbligazioni crittomonetarie e art. 1278 c.c.

Piú nel dettaglio, laddove trovi applicazione il diritto italiano[25], le obbligazioni aventi ad oggetto il pagamento di un corrispettivo da affettuarsi in Bitcoin potranno essere disciplinate dall'art. 1278 c.c. che regola le ipotesi di prestazioni pecuniarie espresse in moneta diversa da quella avente corso legale nello Stato. Il codice civile italiano, diversamente da altri ordinamenti, non utilizza la formula "debito di moneta estera" ma una espressione più ampia capace di includere non solo le valute straniere ma

denaro è identificato con un numero di serie, cosa che non indice minimamente sulla pacifica definizione del denaro come bene fungibile» (così A. Caloni, *Bitcoin, Profili civilistici e tutela dell'investitore*, in *Riv. dir. civ.*, 2019, 159 ss., spec. nota 41).

21 Sul punto si veda S. Aceto di Capriglia, *Illeciti criptovalutari. Note comparatistiche*, cit., 67.

22 Cfr. M. Semeraro, *Moneta legale, moneta virtuale e rilevanza dei conflitti*, in *Riv. dir. banc.*, 2019, 237 ss.

23 In particolare, sui possibili rischi derivanti dall'impiego delle criptovalute e la necessità di predisporre adeguate tecniche di tutela per gli investitori cfr. C. Pernice, *Digital currency ed obbligazioni pecuniarie*, cit., 272 ss.; E. Girino, *Crirptovalute: un problema di legalità funzionale*, cit., 22 ss.; R. Vampa, *FinTech e criptovalute: nuove sfide per la regolazione dei mercati finanziari*, cit., *passim*; A. Caloni, *Bitcoin: profili civilistici e tutela dell'investitore*, cit., 159 ss.

24 Sulla valutazione di compatibilità e sulla distinzione tra i criteri di compatibilità ed adeguatezza G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, 91 ss., spec. nota 230; Id., *Il patto di famiglia tra bilanciamento dei princípi e valutazione comparativa degli interessi*, in *Rass. dir. civ.*, 2008, 190 ss.; Id., *La scelta della disciplina applicabile ai c.dd. «vitalizi impropri». Riflessioni in tema di aleatorietà della rendita vitalizia e di tipicità e atipicità dei contratti*, ivi, 2015, *passim*, spec. 532 ss.; Id., *L'inesistenza della distinzione tra regole di comportamento e di validità nel diritto italo-europeo*, Napoli, 2013, *passim*, spec. 85 s. e 118 ss. In estrema sintesi può dirsi che mentre il giudizio di compatibilità impone una valutazione di tipo formale (o logico-razionale che dir si voglia) e si risolve nel dovere di ogni operatore di evitare la coesistenza di regole in contraddizione rispetto al medesimo caso e nel medesimo tempo, il giudizio di adeguatezza si svolge secondo una prospettiva funzionale e assiologica. Le Istituzioni europee e internazionali, nell'interrogarsi sui possibili rischi derivanti dall'impiego delle criptovalute hanno evidenziato la necessità di predisporre adeguate tecniche di tutela per gli investitori.

25 L'art. 1278 c.c. trova applicazione in presenza tre presupposti: che la legge cui è sottoposto il rapporto sia quella italiana: che la moneta dovuta non sia italiana; che il pagamento debba aver luogo in Italia. La dottrina sul punto è pressocché unanime. Cfr. T. Ascarelli, *Obbligazioni pecuniarie*, in *Comm. c.c.* Scialoja e Branca, Bologna-Roma, 1959, 368; B. Inzitari, *La moneta*, cit., 159 ss.; D. Sinesio, *Studi su alcune specie di obbligazioni. Artt. 1277-1320 codice civile*, Napoli, 2004, 27; U. Breccia, *Le obbligazioni*, in *Tratt. dir. priv.* Iudica e Zatti, Milano, 1991, 295 ss.; Cass. civ., sez. II, 7 novembre 1956, n. 4174, in *Foro it.*, 1956, I, 600.

anche: 1) le specie monetarie originariamente aventi corso legale nello Stato e poi andate fuori corso (fattispecie però, già prevista e risolta, dall'art. 1277, c. 2, c.c.[26]; 2) le monete aventi valore intrinseco ma non in corso al tempo del sorgere del debito[27]; 3) le monete c.dd. contrattuali (o complementari), non associate cioè al sistema valutario proprio di uno specifico ordinamento[28].

È d'altro canto significativo che nella piú comune interpretazione della dottrina e della giurisprudenza italiana, probabilmente complice la relazione di accompagnamento al codice civile del guardasigilli[29], la fattispecie di cui all'art. 1278 c.c. venga esclusivamente collegata al debito di moneta estera[30].

Trattasi tuttavia di una "chiusura" che non trova riscontro nel dettato positivo e che trascura i "precedenti" storici della disposizione in esame. Già l'art. 39 del Codice di commercio del Regno d'Italia del 1882 (norma considerata applicabile anche in materia civile, al quale notoriamente si è ispirato il legislatore del 1942), infatti prevedeva che si potesse pagare con moneta del paese non solo nel caso in cui la moneta indicata in contratto avesse mero corso "commerciale" (art. 39) ma anche quando la moneta non avesse alcun corso[31]. Ed in una riunione del 30 maggio 1940 avente ad oggetto

---

[26] Tale norma stabilisce il principio secondo cui nel caso in cui al tempo del pagamento la moneta dovuta non abbia piú corso legale, questo deve essere effettuato in moneta legale ragguagliata al valore della prima.

[27] L'ipotesi di pagamento da effettuarsi con moneta avente valore intrinseco e dotata di corso legale è disciplinata dall'art. 1280 c.c.

[28] L'art. 1278 c.c. statuisce che «Se la somma dovuta è determinata in una moneta non avente corso legale nello Stato, il debitore ha facoltà di pagare in moneta legale, al corso del cambio nel giorno della scadenza e nel luogo stabilito per il pagamento. Similmente, sia pur con riferimento alla "valuta", l'articolo 6.1.9 (Currency of payment) dei Prinicpi Unidroit: «(1) *If a monetary obligation is expressed in a currency other than that of the place for payment, it may be paid by the obligor in the currency of the place for payment unless*
(a) that currency is not freely convertible; or
(b) *the parties have agreed that payment should be made only in the currency in which the monetary obligation is expressed.*
(2) If it is impossible for the obligor to make payment in the currency in which the monetary obligation is expressed, the obligee may require payment in the currency of the place for payment, even in the case referred to in paragraph (1)(b).
(3) Payment in the currency of the place for payment is to be made according to the applicable rate of exchange prevailing there when payment is due.
(4) However, if the obligor has not paid at the time when payment is due, the obligee may require payment according to the applicable rate of exchange prevailing either when payment is due or at the time of actual payment» (corsivo nostro).

[29] Si veda la Relazione d'accompagnamento, § 592: «la possibilità di prestare moneta diversa da quella dedotta è anche considerata quando il debito pecuniario è espresso in moneta estera; in tal caso il codice civile, come già l'art. 39 cod. comm., autorizza, nell'atto di pagamento, la sostituzione della moneta straniera con moneta nazionale (art. 1278). La moneta straniera diviene infungibile solo per volontà delle parti, cioè quando queste convengono la clausola "effettivo" (art. 1279)».

[30] V. A. di Majo, *Le obbligazioni pecuniarie*, in *Enc. dir.*, XXIX, Milano, 1979, 279; T. Ascarelli, *Divisa e divisa estera*, in *Noviss. dig. it.*, V, Torino, 1938, 88; Id., *Obbligazioni pecuniarie*, cit., 368 ss.; E. Quadri, *Le obbligazioni pecuniarie*, in *Tratt. dir. priv.* Rescigno, IX, Torino, 1984, 503 ss.; Cass. civ., sez. II, 2 dicembre 2011, n. 25837, in *Giust. civ.*, 2012, 29 ss.

[31] L'art. 39 statuiva: «Se la moneta indicata in un contratto non ha corso legale o commerciale nel Regno e se il corso non fu espresso, il pagamento può essere fatto colla moneta del paese, secondo il corso del cambio a vista nel giorno della scadenza». A proposito di tale previsione cfr. T. Ascarelli, *La moneta*, Padova, 1928, 107 e C. Vivante, *Trattato di diritto commerciale*, IV, Milano, 1906, 71, il quale tuttavia ricollega il corso commerciale alle contrattazioni di piazza (ossia quelle che

proprio la disciplina delle obbligazioni pecuniarie si evidenziò come non vi fosse ragione per vietare di contrattare con una moneta non avente corso legale nel territorio dello Stato, dovendosi la disciplina riferire anche ai contratti ove le prestazioni fossero espresse in crazie, scudi toscani, scudi lucchesi, paoli ecc. (ovvero monete non statali)[32].

Del resto un testuale riferimento specifico alle "monete estere" è presente sia nella legge sugli assegni sia a quella sulla cambiale di poco precedenti all'adozione del codice civile[33]. Se il legislatore avesse voluto limitare l'àmbito di applicazione dell'art. 1278 c.c. alle sole monete aventi corso legale in altri Stati ben avrebbe potuto esplicitarlo. La locuzione impiegata dall'art. 1278 pertanto, probabilmente, non può considerarsi casuale.

In verità, com'è stato giustamente osservato, l'art. 1278 c.c. è enunciativo del principio in virtú quale in queste ipotesi il debitore ha facoltà di liberarsi pagando con moneta nazionale piuttosto che con quella pattuita (*una in alia solvi potest*) [34]. La *ratio* della previsione riposa nell'esigenza di non determinare in capo al debitore un eccessivo onere adempitivo allorquando il creditore non abbia palesato l'interesse ad ottenere il mezzo monetario di uno specifico ordinamento attraverso l'apposizione della c.d. clausola di effettività[35]. Consentendo il pagamento nella "*local payment rule*", l'obbligato di una somma di denaro non avente corso legale viene infatti equiparato, almeno sotto questo aspetto, ai normali debitori pecuniari (cioè di moneta nazionale). Tale regola pare applicabile ben oltre gli angusti confini dei debiti di valute estere, riassumendo il piú equilibrato contemperamento degli interessi tutte le volte in cui l'oggetto del debito assunto sia una moneta diversa da quella avente corso legale nel territorio nazionale.

Il disposto dell'art. 1278 c.c., dunque, si presta ad abbracciare anche i sistemi di paga-

risultano da un listino ufficiale di borsa). *Contra* G. Pacchioni, *Appunti critici sui pagamenti dei debiti convenuti in moneta estera*, in *Dir. comm.*, 1923, 27, il quale nota che non sempre al corso di piazza si affianca quello commerciale.

[32] Questa l'opinione espressa da Barcellona al quale si contrappose Asquini. Si vedano a tal proposito i *Lavori preparatori del codice civile (anni 1939-1941). Progetti preliminari del libro delle obbligazioni, del codice di commercio e del libro del lavoro. Volume II. Progetto preliminare del libro delle obbligazion*i, Roma, 1942, 24 ss. Verbale n. 1, Riunione del 30 maggio 1940.

[33] Si vedano gli artt. 47 r.d. n. 1669 del 1933 e 39 r.d. n. 1736 del 1933. Entrambe le disposizioni al primo comma fanno generico riferimento alla possibilità di pagare l'assegno o la cambiale in «moneta che non ha corso nel luogo di pagamento» per poi stabilire al c. 2 che «il valore della moneta estera è determinato dagli usi del luogo del pagamento». Sembrerebbe che solo la regola sulla determinazione del valore sia limitatamente pensata solo per le valute estere. Tuttavia occorre considerare che il c.3 di entrambe le previsioni, nel richiamare «le disposizioni precedenti» si riferisce testualmente alla «clausola di pagamento effettivo in moneta estera».

[34] B. Inzitari, *Obbligazioni pecuniarie*, in *Comm c.c.* Scialoja e Branca, Bologna-Roma, 2011, 182.

[35] Ai sensi dell'art. 1279 c.c.: «La disposizione dell'articolo precedente non si applica, se la moneta non avente corso legale nello Stato è indicata con la clausola "effettivo" o altra equivalente, salvo che alla scadenza dell'obbligazione non sia possibile procurarsi tale moneta». Si veda il commento all' art. 6.1.9 (*Currency of payment*) dei Princípi Unidroit: «As a general rule, the obligor is given the alternative of paying in the currency of the place for payment, which may have definite practical advantages and, if that currency is freely convertible, this should cause no difficulty to the obligee. If, however, the currency of the place for payment is not freely convertible, the rule does not apply. *Parties may also exclude the application of the rule by agreeing that payment is to be made only in the currency in which the monetary obligation is expressed (effectivo clause). If it has an interest in the payment actually being made in the currency of account, the obligee should specify this in the contract*» (corsivo nostro).

mento convenzionali e le ipotesi in cui lo scambio intervenga tra un bene provvisto di valore d'uso e un altro provvisto di solo valore di cambio ma non oggetto di monopolio da parte di alcuna Autorità Sovrana[36]. In tali ipotesi non è ravvisabile una permuta, che traduce giuridicamente l'antica pratica del baratto ed in cui l'attuazione del programma traslativo è modellata sulla valutazione del valore d'uso dei beni scambiati, ma una compravendita, poiché l'utilità marginale dell'alienante è valutabile esclusivamente in riferimento ai vantaggi che i successivi acquisti sono in grado di assicurare[37].

Questa ricostruzione, proposta qualche anno fa in uno dei primi scritti in cui ci siamo occupati del tema ha recentemente trovato adesione da parte della dottrina[38] e della giurisprudenza italiana[39]. Emblematico il lodo arbitrale marcianise del 14 Aprile 2018[40]. Il caso concerneva un corrispettivo da conferirsi in parte in crittovalute. L'arbitro ha ravvisato un rapporto di similitudine tra la fattispecie di debito di somma di «moneta non avente corso legale dello stato», disciplinata dall'art. 1278 c.c., e quella di debito di somme da corrispondersi pattiziamente in criptovaluta, non oggetto di specifica regolamentazione, e ha ritenuto che al fenomeno delle obbligazioni pecuniarie espresse in valute virtuali, in mancanza di esplicita disciplina legislativa, debba applicarsi, analogicamente, l'art. 1278 c.c. Ciò «in quanto entrambe le fattispecie attengono alle ipotesi di adempimento di obbligazione pecuniaria da soddisfarsi con consegna di moneta

[36] Queste monete non hanno corso legale secondo il tradizionale intendimento della locuzione ma possono considerarsi legalmente correnti nella comunità che ha scelto il medio medesimo per veicolare un credito al proprio interno. Interessante al riguardo la definizione offerta dall'*Oxford Dictionary* inglese, che descrive la valuta (*currency*) come un sistema di denaro in uso generale in un determinato paese, ponendo l'accento non sull'emissione statale quanto sull'impiego quale mezzo di scambio nell'àmbito di un dato territorio. Del resto nemmeno l'euro, che è moneta avente corso legale nell'Unione europea, è oggetto di monopolio statale. L'Unione Europea non è Stato, e la storia dell'euro dimostra che la moneta non è altro che una convenzione sociale, in questo caso tra Stati, talvolta tra gli uomini. Sul punto A. Chirico, *La sovranità monetaria tra ordine giuridico e processo economico*, Padova, 2003, 164 ss., la quale al riguardo discorre di edificazione di un nuovo modello di sovranità monetaria senza Stato. Analoghi rilievi sono compiuti con riferimento alla moneta bancaria, la quale appunto è oggetto di emissione ad opera di un soggetto privato, da G. Lemme, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, in *Riv. dir. banc.*, 2016, 11, 3. G.L. Greco, *Monete complementari e valute virtuali*, in M.T. Paracampo (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2018, 214, afferma che «dal punto di vista della funzione svolta [...] parrebbero non cogliersi differenze apprezzabili [...] tra moneta scritturale e moneta complementare (e valuta virtuale)».

[37] *Contra* M. Krogh, *Transazioni in valute virtuali e rischi di riciclaggio. Il ruolo del notaio*, in *Notariato*, 2018, 2, 158 e S. Capaccioli, *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015, 153, secondo i quali la cessione di beni e servizi contro criptovalute integra una permuta. Sui rischi di una compravendita realizzata pagando in Bitcoin N. Mancini, *"Bitcoin": rischi e difficoltà normative*, in *Banca impr. soc.*, 2016, 137, nota 83. Sugli aspetti "notarili" della questione, (ed in particolar modo sull'applicabilità dell'art. 35, c. 22, d.lgs. 223/2006, a norma del quale «le parti hanno l'obbligo di rendere apposita dichiarazione sostitutiva di atto di notorietà recante l'indicazione analitica delle modalità di pagamento del corrispettivo») M. Krogh, ivi, 169.

[38] Recentemente in questo senso anche M. Rubino de Ritis, *La moneta digitale complementare: modelli convenzionali di adempimento in criptomonete e prospettive per il sud*, in F. Fimmanò - G. Falcone (a cura di), *Fintech*, cit., 558; M. Passaretta, *Il primo intervento del legislatore italiano in materia di 'valute virtuali'*, in *Nuove leggi civ. comm.*, 2018, 1171; M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, in *Riv. dir. civ.*, 2019, 183 ss.

[39] In giurisprudenza si veda anche, oltre a Trib. Firenze, 21 gennaio 2019, n. 18, cit., App. Brescia, 30 ottobre 2018, in *Società*, 2019, 26 ss. In senso parzialmente difforme però, più di recente Tar Lazio, 27 gennaio 2020, n. 1077, in *Società*, 2020, 566 ss.

[40] Visionabile in *giustiziacivile.com*, 2018, 11, con nota di M.R. De Ritis, *Obbligazioni pecuniarie in criptomoneta.*

non avente corso legale nello Stato italiano». Con la conseguenza che «il creditore di una prestazione di somma di denaro determinata in criptovaluta non può richiedere l'adempimento della prestazione in moneta avente corso legale. Al contrario, il debitore dell'obbligazione pecuniaria determinata in criptovaluta è tenuto ad adempiere corrispondendo la somma in criptovaluta ma ha la facoltà di adempiere pagando in moneta legale».

Aspetto non indagato dalla pronuncia ma che tuttavia è interessante approfondire è come debba operare in tali ipotesi la regola, sempre prevista dall'art. 1278 c.c., secondo cui il pagamento in moneta legale deve avvenire «al corso del cambio nel giorno della scadenza e nel luogo stabilito per il pagamento» visto che per Bitcoin non esiste un corso di cambio "ufficiale"[41]. A tale riguardo deve osservarsi che così come non esistono ostacoli teorici a ricondurre le monete convenzionali nel perimetro di operatività dell'art. 1278 c.c., similmente non sussistono preclusioni letterali a riferire il "corso del cambio" a quello in uso nella prassi commerciale. Soluzione questa del resto sposata da autorevole dottrina, che già in passato aveva optato per una lettura estensiva della formula «monete non aventi corso legale nello Stato», e che coerentemente aveva affermato che «il riferimento dell'art. 1278 al "corso di cambio" deve intendersi con riferimento a un corso di mercato dei pezzi monetari risultante da libere (ma lecite) contrattazioni nelle quali i pezzi monetari vengono considerati come merce (contro un prezzo in valuta)»[42]. Sicché dove un cambio ufficiale manchi, ai sensi dell'art. 1278 c.c. si potrebbe ben fare riferimento al corso di cambio praticato sui mercati. Soluzione questa avvalorata oltre che dalla pregressa disciplina di cui all'art. 39 del codice del commercio[43], anche dalla disciplina sulla cambiale e sugli assegni. L'art. 47 del r.d. 14 dicembre 1933, n. 1669 e l'art. 39 del r.d. 21 dicembre 1933, n. 1736 prevedono infatti che allorquando la moneta del titolo non sia quella avente corso nel luogo del pagamento, la somma può essere pagata in moneta del paese al valore del giorno della scadenza «determinato dagli usi del luogo di pagamento», ove il richiamo agli usi evidentemente supera la necessità di un cambio ufficiale. Piuttosto deve dirsi che essendo le crittomonete trattate in mercati virtuali che applicano tassi di cambio sensibilmente diversi, potrebbe essere difficoltoso individuare un mercato di riferimento. Presumibilmente l'unico criterio ragionevolmente applicabile potrebbe essere quello di applicare il tasso medio di cambio delle piattaforme "lecitamente" site dove l'obbligazione deve essere adempiuta[44].

---

[41] Pone acutamente il problema M.F. Campagna, *Criptomonete e obbligazioni pecuniarie*, cit., 204 ss.

[42] T. Ascarelli, *Obbligazioni pecuniarie*, cit., 377. Sulla necessità di considerare il contratto di cambiovaluta un contratto di compravendita sia consentito il rinvio a C. Pernice, *Digital currency e obbligazioni pecuniarie*, cit., 64 e ivi ulteriore bibliografia, nonché, più recentemente, M. Cian, *La crittovaluta. Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca borsa tit. cred.*, 2019, 331.

[43] L'art. 39 infatti statuiva che in assenza di un corso di cambio doveva farsi riferimento al «corso della piazza più vicina».

[44] Si veda l'art. 6.1.9 dei Princípi Unidroit che si riferisce al «the applicable rate of *exchange prevailing* there when payment is due» (corsivo nostro). Per testuali riferimenti alla «media dei corsi di cambio» e alle «libere e lecite contrattazioni» T. Ascarelli, *Corsi di cambio e parità della lira*, in *Foro it.*, 1953, 704 ss.; App. Genova, 8 settembre 1952, *ivi*; App. Roma, 15 maggio, 1952 e App. Roma, 26 febbraio 1952, in *Foro it.*, 1952, 1413 ss. Si ricordi in proposito che la disciplina italiana impone ai «prestatori di servizi relativi all'utilizzo di valuta virtuale» l'iscrizione in apposita sezione del registro dei cambiovalute. Sul

Da ultimo occorre interrogarsi sul momento al quale riferire il cambio, quesito che potrebbe apparire di non poco conto ove si considerino le considerevoli fluttuazioni di valore che le valute virtuali incontrano talvolta anche nel corso della stessa giornata. Assumendo che il pagamento sia tempestivo[45], tre sono le possibili soluzioni prospettabili: momento in cui viene effettuato il pagamento; tasso medio del giorno della scadenza; tasso di cambio dell'inizio del giorno della scadenza.

La prima soluzione sembrerebbe trovare un argomento di sostegno nell'art. 39 del cod. comm., che per le monete non aventi corso legale si riferiva al «corso del *cambio a vista* nel giorno della scadenza» e nella relazione al codice civile n. 592 ove si legge «La possibilità di prestare una moneta diversa da quella dedotta è anche considerata quando il debito pecuniario è espresso in moneta estera; in tal caso il codice civile, come già l'art. 39 cod. comm., autorizza, *nell'atto del pagamento*, la sostituzione della moneta straniera con moneta nazionale (art. 1278 del c.c.)». Sennonché l'art. 1278 c.c., ovvero la relazione che ha accompagnato la sua adozione, non si riferiscono al *momento* del cambio bensì a quello della *scelta*, che secondo la giurisprudenza può operare anche in corso di causa e senza necessità di una specifica forma[46].

Più "problematico" potrebbe apparire il dato testuale di cui all'art. 39 cod. comm., esso tuttavia non è insuperabile. Numerose ragioni militano infatti in senso contrario. Prima di addentrarci in tale discorso occorre però compiere una premessa onde sgomberare il campo da possibili equivoci. Si potrebbe infatti pensare che ancorando il momento del cambio a quello del pagamento si potrebbe offrire al debitore un *escamotage* idoneo ad avvantaggiarlo poiché costui potrebbe selezionare il momento più conveniente per esercitare la *facultas solutionis* al fine di prestare una somma minore rispetto a quella contrattualmente pattuita. In disparte il rilievo che una simile conclusione postulerebbe

punto cfr. S. Aceto di Capriglia, *Illeciti criptovalutari. Note comparatistiche*, cit., 69 il quale, pur muovendo dal presupposto secondo cui le obbligazioni crittomonetarie andrebbero ricondotte alla categoria dei debiti di valore e non di valuta, ritiene che in caso di inadempimento per determinare il valore della prestazione il giudice debba avvalersi dei listini dei mercati finanziari.

[45] Non può in questa sede esaminarsi, per la vastità e complessità del tema, l'ulteriore profilo del danno da ritardo nelle obbligazioni espresse in moneta non avente corso legale per il quale sia consentito il rinvio a C. Pernice, Digital currency *e obbligazioni pecuniarie*, cit., 66 ss. ed ivi ulteriore bibliografia. Compara sul punto i Princípi Unidroit in nota 27.

[46] Cass. civ., sez. II, 22 gennaio 1998, n. 555, in *Dejure online*: «in tema di adempimento di obbligazioni pecuniarie determinate in valuta estera, l'art. 1278 c.c., nel limitarsi ad attribuire al debitore la facoltà alternativa di pagare in moneta avente corso legale, non indica anche le specifiche modalità secondo cui tale facoltà abbia ad essere esercitata, restando, per l'effetto, rimessa al debitore ogni determinazione circa i tempi e le forme della relativa scelta, con la conseguenza che, svincolata da ogni rapporto di contestualità con l'effettivo pagamento, quest'ultima ben può manifestarsi per *facta concludentia*, posti in essere in qualunque tempo dall'obbligato prima del concreto adempimento, purché risulti inequivoca, secondo il prudente apprezzamento del giudice di merito, la volontà di pagare in moneta nazionale anziché estera. Deve, pertanto, ritenersi espressione legittima della ricordata facoltà di scelta l'offerta (non formale), in corso di causa, da parte del debitore, di una somma di denaro in moneta nazionale - sempreché non ostino alla inequivocità di tale manifestazione di volontà altri elementi che ne contrastino la apparente significazione - così che il giudice di merito, vincolato a detta scelta, dovrà, in sede di emanazione della sentenza, disporre necessariamente il pagamento in valuta nazionale, senza che possa spiegare influenza, sul contenuto della pronuncia, la richiesta - formulata dall'attore in citazione e non modificata per tutto il corso del procedimento - di pagamento in valuta estera, così come originariamente convenuto tra le parti».

improbabili capacità predittive dell'obbligato[47], deve osservarsi che in verità il problema è più apparente che reale, posto che nel momento in cui pagherà il debitore offrirà sempre al creditore una somma in moneta legale idonea ad acquistare l'equivalente in moneta virtuale (e viceversa). La diminuzione patrimoniale del debitore, quale che sia il mezzo di pagamento prescelto ed il momento selezionato per l'adempimento, sarà sempre il medesimo. Un esempio potrà meglio chiarire il concetto. Immaginiamo che l'obbligazione preveda il pagamento di 100 Bitcoin l'1 maggio. Alle ore 9:00 un Bitcoin vale 10 euro; alle 18:00 un Bitcoin vale 1 euro. Se il debitore adempirà alle 9:00 dovrà conferire al creditore 100 Bitcoin o 1000 euro. Se pagherà alle 18:00 trasferirà 100 Bitcoin o 100 euro. La circostanza che il valore di Bitcoin muti nel corso del giorno ha un impatto relativo visto che tanto alle 9:00 quanto alla 18:00 il debitore farà pervenire al creditore un equivalente potere economico d'acquisto espresso in moneta legale previsto per la cifra pattuita in moneta convenzionale. Dal canto suo il debitore si impoverirà del medesimo valore in qualunque momento egli adempia. Perché anche laddove il debitore pagasse alle 18:00 (momento in cui il cambio è a lui apparentemente favorevole) in moneta nazionale egli non trarrebbe un vantaggio maggiore rispetto all'ipotesi in cui decidesse di pagare in moneta contrattuale. Lo sforzo economico su lui gravante sarebbe il medesimo. Per intenderci, laddove non si avvalesse della *facultas solutionis* o ad esempio fosse prevista la clausola di pagamento effettivo, se il debitore non possedesse i Bitcoin sempre 100 euro spenderebbe per acquistarli e farli giungere al creditore. Detto altrimenti, quale che sia la moneta ed il momento prescelto il debitore farà pervenire al creditore in ogni caso il medesimo potere economico d'acquisto. È un corollario del principio nominalistico al quale non si sottraggono le obbligazioni espresse in monete non avente corso legale (ivi incluse le monete estere)[48] e che in fondo caratterizza tutti i rapporti di obbligazione, non solo quelle pecuniarie, tosto che, salvo diversa previsione, nei contratti ad esecuzione differita vale il "*nomen*" della prestazione promessa, non il valore dei beni pattuiti[49]. Con il ché non si vuol dire che

[47] Nessuno può sapere se il corso del cambio nell'arco della giornata muterà a proprio vantaggio o svantaggio.

[48] Sull'applicabilità del principio nominalistico alle fattispecie di cui all'art. 1278 c.c. T. Ascarelli, *Messa fuori corso della valuta e debiti pecuniari*, in *Foro it.*, I, 1953, 73 ss.; Id., *La moneta*, cit., 284; M. Giuliano, *Considerazioni sul principio nominalistico in obbligazioni pecuniarie di moneta straniera nel caso di rinnovamento monetario*, in *Temi*, 1963, 897 ss.; F. Mastropaolo, *Obbligazioni pecuniarie*, in *Enc. giur.* Treccani, XXI, Roma, 1990, 11, il quale a tal proposito cita D. Barbero, *Sistema del diritto privato italiano*, II, Torino, 1962, 44; E. Quadri, *Le obbligazioni pecuniarie*, cit., 509 ss.; Cass. civ., sez. II, 30 marzo 1966, n. 842, cit.; Cass., 16 settembre 1980, n. 5275, in *Giur. it.*, 1981, 1678; Cass. civ., sez. III, 25 febbraio 2005, n. 4076, in *Dir. trasp.*, 2006, 638.

[49] C. Viterbo, *Debito in valuta estera e clausola oro*, in *Foro it*, 1947, cit., 196 s. scrive «il principio nominalistico della moneta, di cui tanto spesso si ragiona come di un principio speciale, non è in fondo che l'applicazione nel campo della moneta del principio secondo il quale le variazioni nelle qualità, anche essenziali, della cosa nella obbligazione a termine durante il decorso del termine stesso non affettano il contratto se non vi è vera e propria trasformazione della cosa stessa, o se le trasformazioni non sono avvenute per colpa del debitore. E ciò che vale per una cosa determinata, vale naturalmente anche per il *genus*, quando cause generali ne modifichino la qualità: come sarebbe ad esempio, se l'eccezionale umidità della stagione modificasse il potere dolcificante di tutto lo zucchero esistente. Del resto gli stessi principi si applicano alle merci acquistate dai commercianti per rivenderle, cioè in considerazione del loro valore, analogamente a quanto avviene per la moneta, senza ricorrere al principio nominalistico; pur senza che si sia mai pensato che l'aumento o la diminuzione di valore delle medesime potesse avere

un eccessivo mutamento del valore della prestazione dedotta in obbligazione sia sempre irrilevante. L'ordinamento appresta vari rimedi al riguardo, sia legali (si pensi alla eccesiva onerosità sopravvenuta)[50] che convenzionali (il riferimento è alla clausole di indicizzazione), semplicemente si vuol significare che il "rischio" paventato è insito a qualsivoglia rapporto obbligatorio. Un problema analogo del resto potrebbe porsi anche nell'ipotesi inversa, allorquando cioè il debitore decidesse di adempiere in moneta convenzionale. Anche in tale ipotesi potrebbe rilevare l'andamento di valore all'interno della giornata, ed è fin troppo ovvio che se il creditore richiedesse la prestazione alle 9:00 otterrebbe un valore "reale" ben diverso da quello che riceverebbe se avanzasse la richiesta alle 18:00.

Ciò che induce a rifiutare la tesi del tasso di cambio al momento del pagamento, dunque, non è la necessità di prevenire condotte abusive dell'obbligato, ma piuttosto un'esigenza di certezza dei traffici giuridici, la stessa che anima il principio nominalistico (acquisito dalla maggior parte degli ordinamenti giuridici mondiali)[51]: se si agganciasse il momento del cambio a quello del pagamento tanto il debitore quanto il creditore non sarebbero in grado di valutare l'esatto ammontare della prestazione dovuta. Tale circostanza spiega altresì perché sia di difficile attuazione la proposta, pur autorevolmente suggerita[52], di far riferimento alla media del corso di cambio del giorno della scadenza. Il parametro di riferimento sarebbe ricostruibile solo *ex post* con inevitabile nocumento per la sicurezza dei rapporti.

Invero, considerato che la prestazione diviene esigibile in un dato giorno, e che l'adempimento può essere richiesto sin dall'inizio dello stesso, la soluzione più ragionevole appare essere quella che àncora il tasso di cambio all'inizio del giorno della scadenza, avuto riguardo al valore stimato dalle piattaforme site nel *locus solutionis*[53].

---

una influenza sul contratto».

[50] Sulla possibilità di applicare l'istituto alla inflazione monetaria E. Betti, *Teoria generale del negozio giuridico*, cit., 489 s., spec. nota 12; A. Riccio, *Dell'eccessiva onerosità*, in *Comm. c.c.* Scialoja e Branca, Bologna-Roma, 2010, 135; R. Franceschelli, *La svalutazione monetaria come causa di risoluzione dei contratti per eccessiva onerosità*, in *Temi*, 1949, 130; E. Favara, *Svalutazione monetaria ed eccessiva onerosità*, in *Giur. compl. cass. civ.*, 6, 1953, 278; R. Granata, *Brevi cenni in tema di eccessiva onerosità dipendente da eventi di portata generale e in specie da svalutazione monetaria*, ivi, 2, 1954, 58; E. Quadri, *Congiuntura economica e svalutazione monetaria: osservazioni in tema di risoluzione per eccesiva onerosità*, in *Dir. giur.*, 1975, 809; Id., *Le obbligazioni pecuniarie*, cit., 464 ss. (con particolare riferimento alla possibilità di ricorrere ad ulteriori strumenti quali la buona fede o l'arricchimento senza causa); M. Lipari, *La risoluzione del contratto per eccessiva onerosità: la struttura del giudizio di prevedibilità e la rilevanza dell'inflazione* (nota a Cass., 15 dicembre 1984, n. 6574), in *Giust. civ.*, I, 1985, 2795; F. Macario, *Inflazione, fluttuazione del mercato ed eccessiva onerosità* (nota a Cass., 13 febbraio 1995, n. 1159), in *Corr. giur.*, 1995, 595 ss.; O. Cagnasso, *Appunti in tema di sopravvenienza contrattuale e svalutazione monetaria (nota a Trib. Torino, 14 dicembre 1979)*, in *Giur. it.*, I, 1980, 416 ss.; N. Irti, *Inflazione e rapporti tra privati*, in *Giust. civ.*, II, 1981, 310 ss.; P. Greco, *Debito pecuniario, debito di valore e svalutazione monetaria*, in *Riv. dir. comm.*, II, 1947, 108 ss.; R. Pardolesi, *Indicizzazione contrattuale e risoluzione per eccessiva onerosità*, in *Foro it.*, I, 1981, 2147 ss.; A. di Majo, *Il controllo giudiziale del principio nominalistico (profili comparatistici)*, in C.M Mazzoni - A. Nigro (a cura di), *Credito e moneta*, Milano, 1982, 773 ss.

[51] In Francia, ad esempio, tale principio è codificato all'art. 1343 del Code Civil.

[52] T. Ascarelli, *Obbligazioni pecuniarie*, cit., 384, nota 6.

[53] Cfr. Cass. civ., sez. VI, 25 settembre 2015, n. 1908, che ha applicato il «cambio vigente alla scadenza dell'obbligazione, cioè all'epoca [...] in cui il credito è maturato e *divenuto esigibile*, con conseguente tendenziale irrilevanza delle successive fluttuazioni del rapporto di cambio».

6. Rilievi conclusivi

L'innovazione tecnologica, nella sua pervasività economica, oramai da tempo pone i regolatori dinnanzi a sfide normative la cui soluzione fatica a trovare una soluzione univoca e tempestiva. Ciò è ancora più vero in tema di valute virtuali a motivo della estrema eterogeneità e dinamicità del fenomeno. Dal 2008 ad oggi, infatti, le crittovalute si sono esponenzialmente moltiplicate in qualità e quantità, offrendo, sicuramente, numerose opportunità di sviluppo dei mercati finanziari, ma al contempo introducendo rischi inediti nello scenario economico. Se alcuni gettoni, riproponendo in forma digitale strumenti già noti alla prassi dei commerci, non destano particolari problemi, i token autoreferenziali, qual è bitcoin, sembrano contraddire un postulato che fino a qualche anno fa vigeva incontrastato: la moneta è solo quella battuta dallo Stato.
La diffusione di questi strumenti di pagamento convenzionale ha così rinnovato la riflessione giuridica sulla natura giuridica del denaro, un dibattito invero mai sopito e soggetto a continue rivisitazioni rispetto al quale le elaborazioni teoriche sono state profondamente influenzate dalla forma che la moneta ha di volta in volta assunto nel corso della storia. Se si accetta la definizione che noi proponiamo, secondo cui moneta è il bene prescelto da una data collettività per veicolare un credito duraturo spendibile nei confronti della stessa, è di intuitiva evidenza come possa inscriversi nella categoria anche bitcoin. Bitcoin ha assunto credibilità come strumento di pagamento, non ultimo l'annuncio di Paypal di accettare, a decorrere dal 2021, pagamenti anche in bitcoin. Applicando l'ipotesi che bitcoin sia una moneta, tra l'altro, si riesce a elaborare, nelle more di una regolazione ufficiale, un quadro classificatorio il piú possibile esauriente, non tanto a fini puramente speculativi, quanto per gli importanti riflessi applicativi che ne possono conseguire. L'auspicio per il futuro è che la disciplina del mercato delle valute virtuali venga condotta in modo razionale e proporzionale, nel rispetto della duttilità che caratterizza la moneta *peer to peer*, cosí da rafforzare la stabilità dei prezzi delle valute virtuali e la fiducia che gli utilizzatori ripongono in esse[54].

[54] G. Lemme, *Criptomoneta e distacco dalla moneta legale: il caso bitcoin*, cit., 39, sostiene che con l'*imprimatur* statale la valuta virtuale potrebbe essere moneta a tutti gli effetti.

Data protection e contratto nei data-driven business model*

Silvia Martinelli

Abstract

La diffusione delle nuove tecnologie, di Internet e dei Big Data ha portato ad una rivoluzione dell'identità che ha reso necessaria l'introduzione di nuove norme a tutela della privacy e della personalità. La disciplina per la protezione dei dati personali ha introdotto forme di tutela dell'identità dinamica, attraverso i diritti dell'interessato, che tuttavia con l'accrescersi dell'attività algoritmica e dei *data-driven business model* basati su dati e algoritmi, si mostrano insufficienti. Si affianca una disciplina contrattuale sull'utilizzo dei dati, che ricalca l'importanza economica ch'essi rivestono e che inizia ad ottenere prime forme di regolazione (ad es. rispetto ai reputational feedback system, alla platform economy e nella *digital content directive*), ma necessiterebbe di una disciplina più organica.

New technologies, Internet and Big Data has led to an identity revolution which has required the introduction of new rules to protect privacy and personality. The discipline for the protection of personal data has created new forms of protection for the "dynamic identity", through the rights of the data subject. However, with the growth of algorithmic activity and data-driven business models based on data and algorithms, it appears insufficient. The contract became an instrument to discipline the use of data, which traces the economic importance that they cover. It begins to obtain the first forms of regulation (e.g. with respect to reputational feedback systems, platform economy and digital content directive), but it would need a more organic discipline.

Sommario

Keywords

privacy - platform - reputational feedback system - digital content - contratto.

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

1. La tutela della persona e i diritti degli interessati tra identità dinamica e dinamicità algoritmica

Con la diffusione delle nuove tecnologie, e in particolare di Internet, dei social network e dei Big Data, si sono moltiplicati i luoghi nei quali sono custodite le informazioni che ci riguardano e che dicono agli altri chi siamo e si è amplificato quell'effetto che Rodotà denominava "frazionamento dell'identità"[1]. Ciò è avvenuto sia in ragione dell'aumento delle relazioni, anche pubbliche, che ciascuna persona intrattiene, sia poiché, alla visione che gli altri soggetti hanno di noi, s'è aggiunta l'immagine che i nostri dati, diffusi sui social network o raccolti da soggetti terzi, riflettono, verso chiunque voglia e possa consultarli. Le informazioni sulla persona sono, inoltre, raccolte in più luoghi diversi e per differenti finalità, il che portava Rodotà ad osservare che, in ambito digitale la persona sembra dispersa e frammentata e, se ricondotta all'unica persona che ha generato tutte le rappresentazioni, reali o virtuali, estremamente dilatata e instabile, in quanto alla mercé degli interessi di chi, di volta in volta, raccoglie i dati ad essa relativi[2]. Si aggiunga, che il dato, riferito o riferibile alla persona, è offerto a chi vi ha accesso in forma "bruta", ovvero senza contestualizzazione, estrapolato in sé e per sé. Al contempo, la cristallizzazione dell'identità nei dati ha alterato la temporalità tradizionalmente connessa al concetto di identità, poiché in Internet, rispetto agli archivi tradizionali, i dati tendono ad essere presentati senza riferimento al criterio temporale. Abbiamo vissuto «una vera rivoluzione dell'identità»[3], tale che non poteva che assumere rilevanza anche sotto il profilo del diritto, richiedendo un necessario riconoscimento di forme di tutela della persona anche in ambito digitale. I diritti della personalità concernenti le informazioni sulla persona hanno così conosciuto una nuova stagione e, in particolare, il diritto alla riservatezza, disciplinato dal Legislatore europeo con la direttiva 95/46/CE e ora nel regolamento 679/2016, il GDPR.

Citando nuovamente Rodotà, «il riconoscimento del diritto alla protezione dei dati come diritto fondamentale realizza […] l'obiettivo di mantenere il rapporto tra la persona ed il suo corpo, non più racchiuso nei confini della fisicità e nel segreto della psiche, ma davvero sconfinato, affidato alle infinite banche dati che dicono al mondo chi siamo. Il fatto che altri legittimamente possieda una quota maggiore o minore di nostri dati non gli attribuisce il potere di disporne liberamente. La sovranità sul corpo si concreta nel diritto di accedere ai propri dati ovunque si trovino, di esigere un loro trattamento conforme ad alcuni principi (necessità, finalità, pertinenza, proporzionali-

[1] Cfr. S. Rodotà, *Il diritto di avere diritti,* Roma-Bari, 2012, 173, ove afferma che siamo in presenza di un'identità "dispersa" in quanto "le informazioni riguardanti la stessa persona sono contenute in banche dati diverse, ciascuna delle quali restituisce soltanto una parte o un frammento dell'identità complessiva". Cfr. anche R. Bodei, *Memoria e costruzione della persona*, in *Iride*, 23, 60, 2010, 339ss.; M. B. Ligorio-H. Hermans, *Identità dialogiche nell'era digitale*, Centro Studi Erickson, Milano, 2005, 190 ss.; S. Niger, *Diritto all'informazione, diritti della persona e archivi giornalistici online*, in *federalismi.it*, 11, 2013, 1 ss., che osserva come nel ciberspazio la persona sia "spezzata", dislocata in luoghi diversificati e moltiplicata, sottolineando come tale moltiplicazione non trovi origine nelle scelte dell'individuo, bensì negli interessi che spingono alla raccolta delle informazioni, i quali portano ad una moltiplicazione del *Sé* in funzione delle necessità del mercato.

[2] Cfr. S. Rodotà, ivi, 173 e 319.

[3] Cfr. ivi, 139.

tà), di poterne ottenere la rettifica, la cancellazione, l'integrazione. Il corpo elettronico e la sua gestione rimangono nella sfera giuridica della persona[4]».

La protezione dei dati personali diviene, quindi, con i diritti degli interessati, strumento di controllo del "Sé" digitale e il diritto all'oblio e alla cancellazione dei dati il più importante a disposizione della persona per riottenere riservatezza e dimenticanza[5].

Tali strumenti, tuttavia, si sono rivelati spesso inadeguati a garantire un'effettiva tutela degli interessati, la capacità del consenso al trattamento dei dati di garantire un'effettiva autodeterminazione informativa è stata posta in dubbio e il nuovo GDPR ha adottato un approccio più garantista e pubblicista, facendo dell'accountability e della valutazione del rischio il perno centrale del sistema di protezione[6].

Al contempo, il diritto all'oblio si è rilevato più complesso rispetto alla mera alternativa tra cancellazione e mantenimento dell'informazione[7]. I motori di ricerca e l'indicizzazione hanno consentito un più facile reperimento dell'informazione e, pertanto, sono stati considerati come maggiormente pregiudizievoli per l'interessato, anche determinando pronunce che imponevano la de-indicizzazione ma non anche la cancellazione dal sito ove l'informazione era stata pubblicata in origine, proprio in ragione della maggior invasività nella sfera individuale permessa da queste tipologie di ricerca abilitate dagli algoritmi.

Si pensi già alla sentenza della Cassazione n. 5525 del 5 aprile 2012[8] - nella quale la Cassazione affermava il «passaggio da una concezione statica a una concezione dinamica della tutela della riservatezza, tesa al controllo dell'utilizzo e del destino dei dati» fornendo ad ogni persona il diritto a mantenere il controllo sulle proprie informazioni – ove la domanda concerneva lo «spostamento di un articolo pubblicato molti anni prima in un'area di un sito Web non indicizzabile dai motori di ricerca» ovvero l'integrazione dello stesso «con le notizie inerenti gli sviluppi successivi della vicenda narrata».

Anche la più recente giurisprudenza della Corte di Giustizia del 24 settembre 2019, C-136/17 apre la strada a una visione meno rigida. Nella pronuncia, infatti, la Corte non soltanto ribadisce i variabili elementi da valutare nella decisione sulla richiesta di cancellazione (la natura e la gravità dell'infrazione di cui trattasi, lo svolgimento e l'esito di tale procedura, il tempo trascorso, il ruolo rivestito da tale persona nella vita pubblica e il suo comportamento in passato, l'interesse del pubblico al momento della richiesta, il contenuto e la forma della pubblicazione nonché le ripercussioni della

---

4 Cfr. ivi, 159.

5 Sia consentito un rinvio a S. Martinelli, *Diritto all'oblio e motori di ricerca. Memoria e oblio nell'era digitale*, Milano, 2017.

6 Cfr. *ex multis* F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il regolamento europeo 2016/679*, Torino, 2016; U. Pagallo-P. Casanovas-R. Madelin, *The middle-out approach: assessing models of legal governance in protection, artificial intelligence, and the web of data*, in *The Theory and Practice of Legislation*, 7, 1, 2019, 1 ss.

7 Sia consentito un rinvio a Cfr. S. Martinelli, *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in Internet e le problematiche poste dalla de-indicizzazione*, in *Il Diritto dell'Informazione e dell'Informatica,* 3, 2017, 565 ss. Cfr. anche S. Bonavita, *Deindicizzazione: tecnologie abilitanti ed evoluzione del rapporto tecnologia e diritto*, in *Danno e Responsabilità*, I, 2019, 127 ss.

8 Cfr. *ex multis* F. Di Ciommo-R. Pardolesi, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!,* in *Danno e Responsabilità*, 7, 2012, 701 ss.

pubblicazione per tale persona), che rendono l'oblio un diritto "mobile", da valutarsi sempre caso per caso, ma giunge anche ad affermare che, quand'anche il motore di ricerca ritenga necessario il mantenimento dell'informazione «è in ogni caso tenuto, al più tardi al momento della richiesta di deindicizzazione, a sistemare l'elenco dei risultati in modo tale che l'immagine globale che ne risulta per l'utente di Internet rifletta la situazione giudiziaria attuale, il che necessita, in particolare, che compaiano per primi, nel suddetto elenco, i link verso pagine web contenenti informazioni a tal proposito». L'algoritmo attua, quindi, un nuova rivoluzione, non rilevando più soltanto il mantenimento o la cancellazione, ma anche il peso attribuito all'informazione, la rilevanza che a tale peso viene attribuita e l'effetto che ne consegue, che nel caso del motore di ricerca si concreta nella posizione tra i risultati e nella rappresentazione d'insieme emergente dai risultati forniti.

I dati hanno rivoluzionato l'identità personale e, con essa i diritti della personalità, moltiplicando e disperdendo le informazioni che ci riguardano, ma si potrebbe ora evidenziare una seconda fase di questa rivoluzione che i dati hanno portato, nella quale essi divengono non soltanto informazioni più diffuse e accessibili, bensì anche intensamente rielaborate ad opera degli algoritmi per la creazione di beni e di servizi che si basano e si fondano su di essi.

In questa nuova fase, la "protezione" dei dati personali appare inidonea a regolare la complessità esistente, ove la necessità e la capacità di utilizzare e sfruttare i dati pare divenire centrale per lo sviluppo economico e nella quale all'interrogativo circa la possibilità di trattare o meno determinati dati occorre affiancare una più ampia riflessione su come tali dati possano essere utilizzati e scambiati e su quale sia la disciplina ad essi applicabile in un'ottica più dinamica.

2. I reputational feedback system e il ranking

Particolarmente rappresentativo nell'ottica della "dinamica dei dati" e nell'ambito dei nuovi servizi e delle nuove forme di organizzazione che su di essi si basano è il caso dei reputational feedback system e del ranking. Su di essi si fondano i sistemi di comparazione e di intermediazione online[9] e al loro funzionamento è affidata la reputazione dei soggetti recensiti.

Così come avviene anche per i like e le condivisioni sui social network, i reputational feedback system e il ranking, si basano sui dati forniti e generati dagli utenti nell'utilizzo del servizio e, organizzati e rielaborati dall'algoritmo, sono posti al centro dei nuovi modelli di business della platform economy quali elemento fondamentale per determinare e favorire l'incontro e lo scambio tra gli utenti all'interno della piattaforma.

I reputational feedback system sono generalmente costituiti da combinazioni tra punteggi e commenti testuali e possono riguardare il bene o servizio nel suo insieme o

[9] Cfr. C. Busch, *Crowdsourcing Consumer Confidence: How to Regulate Online Rating and Review Systems in the Collaborative Economy*, in A. De Franceschi (a cura di), *European Contract Law and the Digital Single Market*, Cambridge, 2016, 223 ss.; G. Smorto, *Reputazione, fiducia e mercati*, in *Europa e diritto privato*, 1, 2016, 199; A. Thierer, *How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the "Lemons Problem"*, in *University of Miami Law Review*, 70, 2016, 830.

presentare voci differenti (ad es. pulizia, comfort, posizione, etc.). Sono valutazioni individuali e personali che vengono aggregate e mostrate in aggiunta alle informazioni fornite da colui che, sulla piattaforma, offre il bene o servizio. L'aggregazione di queste informazioni e di più valutazioni individuali e personali può essere paragonata a una votazione, in quanto rappresentazione aggregata delle espressioni di singole valutazioni.

Il "rank", che determina l'indicizzazione del bene o servizio, è il risultato di un sistema di classificazione, basato sull'identificazione di alcuni parametri rilevanti per far sì che l'utente che effettua una ricerca possa raggiungere l'informazione, il bene o il servizio desiderato. Per la sua determinazione rilevano i reputational feedback system, ma ad essi si affiancano le analisi sui dati generati dagli utenti nell'utilizzo del servizio (come il numero di visualizzazioni o di processi di acquisto effettivamente conclusi), i criteri inseriti dai programmatori nell'algoritmo (come il mostrare prima i venditori "gold" che, per meriti o maggiori esborsi, hanno acquisito tale status), quelli suggeriti dall'algoritmo stesso (ad esempio, in relazione all'acquisto di prodotti di categorie diverse, ma che spesso vengono acquistati dalle medesime persone), quelli basati sulla storia dello specifico utente (quando Silvia viaggia preferisce la posizione centrale, piuttosto che il comfort), etc.

Ranking e algoritmo, assieme ai reputational feedback system, caratterizzano il servizio, sono alla base del suo funzionamento, determinano il successo o l'insuccesso della piattaforma stessa, ma anche gli acquisti, le vendite, i guadagni dei soggetti che operano a vario titolo al suo interno.

Il Legislatore europeo è intervenuto al riguardo introducendo da un lato alcune norme per la protezione del consumatore, con le modifiche introdotte dalla direttiva 2161/2019, dall'altro con il regolamento 1150/2019 per tutelare i "business users". Si tratta, quindi, di interventi che toccano i rapporti tra le due diverse categorie di utenti e la piattaforma. Per il caso dei motori di ricerca e dei loro rapporti con i "business users" ovvero i «titolari di siti web», in ragione della loro rilevanza anche in assenza di un rapporto contrattuale tra i due soggetti, sono introdotti obblighi di trasparenza mediante pubblicazione di informazioni sul sito web del motore di ricerca[10].

Il nuovo art. 6-*bis*, introdotto dalla direttiva 2161/2019 alla direttiva 83/2011, prevede, tra i nuovi obblighi informativi introdotti per i marketplaces, alla lett. a, che siano indicati «i principali parametri che determinano la classificazione delle offerte presentate al consumatore come risultato della sua ricerca sul mercato online». Per "parametri" s'intende «qualsiasi criterio generale, processo, segnale specifico integrato negli algoritmi o qualsiasi altro meccanismo di aggiustamento o di retrocessione utilizzato in connessione con la classificazione»[11].

Alla direttiva 29/2005, all'art. 7, «Omissioni Ingannevoli», sono aggiunti i commi 4-*bis* e 6, relativi al *ranking* e alle recensioni. Il primo, prevede che, nel caso in cui sia fornita ai consumatori «la possibilità di cercare prodotti offerti da professionisti diversi o da consumatori sulla base di una ricerca sotto forma di parola chiave, frase o altri dati, indipendentemente dal luogo in cui le operazioni siano poi effettivamente concluse,

[10] Cfr. art. 5, parr. 2 ss., del regolamento 1150/2019.

[11] Cfr. Considerando 22 della direttiva 2161/2019.

sono considerate rilevanti le informazioni generali, rese disponibili in un'apposita sezione dell'interfaccia online che sia direttamente e facilmente accessibile dalla pagina in cui sono presentati i risultati della ricerca, in merito ai parametri principali che determinano la classificazione dei prodotti presentati al consumatore come risultato della sua ricerca e all'importanza relativa di tali parametri rispetto ad altri parametri»; il secondo, che ove sia fornito accesso alle recensioni dei consumatori sui prodotti, «sono considerate rilevanti le informazioni che indicano se e in che modo il professionista garantisce che le recensioni pubblicate provengano da consumatori che hanno effettivamente acquistato o utilizzato il prodotto».

Il regolamento 1150/2019 dedica l'art. 5 al ranking o "posizionamento", introducendo obblighi informativi per i servizi di intermediazione online e per i motori di ricerca[12]. Per i servizi di intermediazioni online, nelle condizioni generali di contratto tra la piattaforma e il business user, devono essere indicati «i principali parametri che determinano il posizionamento e i motivi dell'importanza relativa di tali parametri principali rispetto ad altri parametri»[13]. Per i fornitori di motori di ricerca, è introdotto l'obbligo di pubblicare online una loro descrizione «facilmente e pubblicamente accessibile», redatta in un linguaggio semplice e comprensibile e aggiornata[14]. Essa deve indicare i «principali parametri che, individualmente o collettivamente, sono i più significativi per determinare il posizionamento», specificandone «l'importanza relativa». Per entrambe le categorie di servizi considerate, è previsto un onere di trasparenza relativo all'esistenza/possibilità di corrispettivi diretti o indiretti corrisposti dal business user che possano influire sul posizionamento[15].

Tutte le informazioni sopramenzionate devono essere tali da consentire ai business users di «comprendere chiaramente se, come e in quale misura» il meccanismo di posizionamento tiene conto di alcuni elementi dalla norma elencati. In particolare, si prevede l'obbligo di indicare se il ranking tiene conto: a) delle caratteristiche dei beni e dei servizi offerti; b) della «pertinenza di tali caratteristiche» per i «consumatori», ovvero della profilazione; c) (per i motori di ricerca) delle «caratteristiche grafiche del sito web», nella versione in inglese «design characteristics», che parrebbe riferirsi agli elementi tecnici e grafici, di web design, che possono incidere sull'indicizzazione[16].

L'assolvimento di tali oneri informativi non implica l'obbligo di rivelare l'algoritmo[17]. Inoltre, al fine di evitare che una spiegazione troppo dettagliata o la rivelazione di

[12] Cfr. art. 2, c. 1, n. 5, del regolamento 1150/2019, che definisce "online search engine" o "motore di ricerca online" un servizio digitale che «consente all'utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto». Per il caso dei motori di ricerca e dei loro rapporti con i business users ovvero i "titolari di siti web", in assenza di un rapporto contrattuale tra i due soggetti, e sono introdotti obblighi di trasparenza mediante pubblicazione di informazioni sul sito web del motore di ricerca.

[13] Cfr. art. 5, par. 1, del regolamento.

[14] Cfr. art. 5, par. 2.

[15] Cfr. art. 5, par. 3.

[16] Cfr. art. 5, par. 5.

[17] Cfr. art. 5, par. 6.

alcune caratteristiche relative al funzionamento del ranking possano essere utilizzate dagli utenti per manipolare il sistema e falsare il rank (con danno per il mercato, la concorrenza e i consumatori) viene specificato che i fornitori di tali servizi non sono tenuti a rivelare «informazioni che, con ragionevole certezza, si tradurrebbero nella possibilità di trarre in inganno i consumatori o di arrecare loro danno attraverso la manipolazione dei risultati di ricerca». É precisato, altresì, che resta impregiudicata la direttiva 943/2016. Si prevede, inoltre, che la Commissione elabori orientamenti in materia di trasparenza per precisare ulteriormente gli obblighi informativi[18].

Infine, si rinviene, al quarto comma, un ulteriore obbligo informativo per il motore di ricerca, per il caso di rimozione o modifica del posizionamento effettuata a seguito di una segnalazione ricevuta da parte di terzi. In tal caso, è prevista la possibilità per il titolare del sito web di «prendere visione del contenuto della segnalazione». Non è chiaro se tale previsione implichi altresì un obbligo di notifica o comunicazione della rimozione o modifica nel posizionamento al titolare del sito web. Non è chiaro, inoltre, come tale previsione vada coordinata con le norme in materia di gestione dei contenuti illeciti da parte delle piattaforme (data protection, copyright, hate speech, terrorismo, etc.).

Lo stesso regolamento introduce all'art. 7, obblighi informativi concernenti i trattamenti differenziati eventualmente posti in essere rispetto ad alcune categorie di utenti, in relazione all'accesso e ai servizi forniti, ai corrispettivi diretti e indiretti, alle condizioni e al posizionamento, indicando anche le «principali considerazioni di ordine economico, commerciale o giuridico per tale trattamento differenziato».

Gli interventi del Legislatore europeo recepiscono un'esigenza di trasparenza, cui viene dato riscontro con l'introduzione di obblighi informativi nelle condizioni generali di contratto, mediante interventi e normative differenziate per i consumatori e i "business users", nonché con obblighi di informazione più generali, in assenza del contratto, rispetto ai motori di ricerca. Il regolamento 1150/2019 recepisce l'esigenza di porre dei contrappesi al potere delle piattaforme e dei limiti all'autonomia privata con riguardo a tali soggetti, tutelando un utente che, pur non essendo consumatore né lavoratore, si trova in una condizione di debolezza.

Un diverso approccio è stato prospettato nel "Discussion Draft of a Directive on Online Intermediary Platforms", elaborato dal Research Group on the Law of Digital Services dell'European Law Institute[19], che ha proposto un intervento normativo volto a regolare le "online intermediary platforms" nel loro insieme, successivamente

[18] Cfr. art. 5, par. 7. Infine, si rinviene, al quarto comma, un ulteriore obbligo informativo per il motore di ricerca, ma non anche per il servizio di intermediazione, per il caso di rimozione o modifica del posizionamento effettuata a seguito di una segnalazione ricevuta da parte di terzi. In tal caso, è prevista la possibilità per il titolare del sito web di «prendere visione del contenuto della segnalazione». Non è chiaro se tale previsione implichi altresì un obbligo di notifica o comunicazione della rimozione o modifica nel posizionamento al titolare del sito web. Non è chiaro, inoltre, come tale previsione vada coordinata con le norme in materia di gestione dei contenuti illeciti da parte delle piattaforme (data protection, copyright, hate speech, terrorismo, etc.). Non è chiaro, infine, perché una simile disposizione, ove ritenuta necessaria, non debba applicarsi anche al servizio di intermediazione online.

[19] Cfr. C. Busch et al. (a cura di), *Discussion Draft of a Directive on Online Intermediary Platforms. Commentary, Jagiellonian University Press*, Krakow, 2019; Research group on the Law of Digital Services, *Discussion Draft of a Directive on Online Intermediary Platforms, in European Consumer and Market Law*, 4, 2016, 164–169. Si

rielaborato nelle "Model Rules on Online Platforms"[20] che hanno recepito stimoli e commenti, proponendo un insieme di disposizioni volte a regolare la platform economy, non più nella forma della direttiva ma come model rules che possano fungere da modello per legislatori nazionali, europeo e internazionali, o da fonte d'ispirazione per l'autoregolamentazione e la standardizzazione.

Nelle Model Rules, cui si limita l'analisi poiché più complete, sono dedicati ai reputation system tre articoli: Article 5, General Requirements for Reputation Systems; Article 6, Criteria of Professional Diligence for Reputation Systems; Article 7, Portability of Reviews.

L'art. 5 prevede che la piattaforma che fornisca un reputation system sia tenuta a fornire informazioni «*about how the relevant information is collected, processed and published as reviews*», nonché che il reputational feedback system debba essere conforme agli standard di diligenza professionale («*must comply with the requirements of professional diligence*»).

Il riferimento alla diligenza professionale, da affiancare agli obblighi informativi, ha il pregio di consentire graduazione, flessibilità e adattabilità in relazione al potere economico della piattaforma considerata, alle specificità del modello di business e alla tecnologia utilizzata, con adeguamento alle sue evoluzioni, avendo quale riferimento lo stato dell'arte. In tal modo, sistemi di certificazione, norme ISO[21] e standard tecnici di settore potranno svilupparsi per la sua specificazione e concretizzazione.

Il terzo comma dell'art. 5 prevede, inoltre, una regola al riguardo: la presunzione di soddisfazione dello standard della diligenza professionale («*A reputation system is presumed to comply with the requirements of professional diligence*») ove siano adottati e soddisfatti gli standard richiesti da standardisation organisation nazionali, europee o internazionali o ove siano soddisfatti i criteri di cui all'articolo 6.

All'art. 6 sono elencati i seguenti criteri di valutazione dell'operato delle piattaforme:

a) se la piattaforma afferma che le recensioni sono redatte da veri consumatori è tenuta a adottare misure ragionevoli e proporzionate per verificare che le recensioni siano basate su uno scambio effettivamente avvenuto;

b) se la piattaforma afferma che le revisioni si basano su una transazione verificata, deve assicurarsi che la recensione sia stata redatta da una delle parti partecipanti allo scambio;

c) se la piattaforma è a conoscenza o dovrebbe essere a conoscenza del fatto che l'autore della recensione ha ricevuto dei benefici per redigerla, deve indicarlo; se il beneficio concerne il merito della recensione, positiva o negativa, la piattaforma è tenuta ad assicurarsi che la recensione non venga pubblicata o venga cancellata;

d) le recensioni possono essere rifiutate o rimosse solo per un motivo legittimo, informando l'autore del rifiuto o della rimozione e specificandone i motivi[22];

e) le recensioni devono essere pubblicate senza indebito ritardo;

---

vedano, in particolare, l'art. 6, "Transparency of Listing", e all'art. 8, "Reputational Feedback Systems".

[20] C. Busch et al., *The ELI Model Rules on Online Platforms*, in *European Consumer and Market Law*, 9, 2, 2020, 61 ss.; European Law Institute, *Model Rules on Online Platforms, Report of the European Law Institute*,

[21] Cfr. ISO 20488:2018, *Online customer reviews. Principles and requirements for their collection, moderation and publication.*

[22] Viene, altresì, specificato che l'obbligo di motivazione non deve essere considerato tale da indurre la

f) le recensioni devono indicare la data del giorno in cui sono state redatte; l'ordine o nel quale le recensioni sono presentate per impostazione predefinita e l'importanza relativa attribuita non devono essere fuorvianti; la piattaforma deve fornire agli utenti informazioni facilmente accessibili sui parametri principali che determinano l'ordine, in cui vengono presentate le recensioni o l'importanza relativa attribuita, nonché offrire la possibilità di visualizzare le recensioni in ordine cronologico;
g) se il reputation system mostra le recensioni relative ad un periodo determinato, la piattaforma deve indicare il periodo di riferimento, il quale deve essere ragionevole e comunque non inferiore agli ultimi 12 mesi;
h) se le singole revisioni vengono combinate in un punteggio consolidato, il metodo di calcolo utilizzato non deve portare a risultati fuorvianti e deve essere indicato il numero delle recensioni totali; se la valutazione consolidata viene calcolata sulla base di fattori diversi dalla media numerica delle recensioni, la piattaforma deve informare gli utenti su tali fattori; se le recensioni vengono visualizzate solo per un periodo di tempo fisso, le recensioni che non vengono mostrate non devono essere utilizzate neanche per il calcolo della valutazione consolidata;
i) la piattaforma deve fornire gratuitamente meccanismi che consentano di rispondere alla recensioni e segnalare eventuali abusi.
Infine, l'articolo 7 delle Model Rules introduce un diritto alla portabilità delle recensioni e, quindi, del patrimonio reputazionale acquisito. Se le recensioni e il ranking acquisiscono, nei nuovi ecosistemi, tale centrale importanza, è evidente che, ove la reputazione acquisita non possa essere trasferita o convertita nel passaggio da una piattaforma ad un'altra, si determina un nuovo effetto lock-in, in mercati nei quali, come si è detto, già esistono importanti effetti network. Lo sviluppo di meccanismi che consentano la portabilità della reputazione da una piattaforma ad un'altra, anche mediante l'utilizzo di terze parti di fiducia, diviene, quindi, fondamentale per tutelare la concorrenza[23].
Il caso dei reputational feedback system e del ranking, la prima forma di regolazione sopradescritta e quella prospettata nella Model Rules, evidenziano chiaramente la maggiore complessità ormai esistente, che va ben al di là della mera alternativa tra cancellazione e mantenimento dell'informazione.

piattaforma a divulgare informazioni che potrebbero essere utilizzate per manipolare il *reputation system*.

[23] Le Model Rules prevedono che la piattaforma debba a predisporre "facilities" che consentano il trasferimento delle recensioni in un formato che sia «structured, commonly used and machine-readable». Tale possibilità deve essere offerta almeno ogni mese e al termine del contratto. La piattaforma è tenuta ad informare l'utente, prima della conclusione del contratto, in merito ai processi, ai requisiti tecnici, alle tempistiche e ai costi applicabili necessari per l'esercizio della portabilità. Con riguardo alla piattaforma ricevente, si prevede un obbligo di verifica delle recensioni, volto a controllare che siano state raccolte secondo la diligenza professionale, nonché l'obbligo di indicare che quelle recensioni sono state generate su una piattaforma diversa. La circolazione delle recensioni e dei ranking tra piattaforme comporta il rischio di utilizzi distorti del diritto alla portabilità, volti a falsare la concorrenza introducendo recensioni false. L'adozione di standard il più possibile omogenei per i reputation systems, anche mediante l'utilizzo della standardizzazione, dovrebbe diminuire i rischi e favorire l'affidabilità dei sistemi reputazionali nel loro complesso. Cfr. European Parliament, Resolution of 15 June 2017 on a European Agenda for the collaborative economy, 2017/2003(INI), che evidenzia l'importanza della portabilità del rating e delle recensioni, che costituiscono un "digital market value", da effettuarsi nel rispetto della privacy e della protezione dei dati di tutti i soggetti coinvolti.

Tali sistemi reputazionali e di indicizzazione, basati su dati e algoritmi, hanno superato il mero intento informazionale, andando a costituire la base portante di nuovi modelli di business e di nuovi mercati.
Si tratta, inoltre, di norme volte alla regolazione di sistemi informativi basati su algoritmi che vengono regolati nell'ambito del diritto contrattuale.

3. Data protection e contratto nei data-driven business model

Alcuni studiosi hanno evidenziato come «La commercializzazione dei dati personali ha accelerato il processo di mercificazione degli individui, che sono visti sempre più come una massa di informazioni da raggruppare o dividere a seconda dell'uso commerciale che si intende farne»[24]. Altri, denominando tale fenomeno come "svendita della privacy" – ove non addirittura come "fine della privacy" – si sono mostrati preoccupati per la facilità con la quale gli utenti tendono ad acconsentire al trattamento dei propri dati personali, senza comprenderne la reale importanza[25]. Tuttavia, è ormai innegabile che i dati hanno assunto un valore economico rilevante, che sono scambiati come controprestazione in cambio di servizi, nonché sono posti alla base del funzionamento di interi modelli di business, ben rappresentati ma non limitati ai social networks, alla platform economy e ai business model basati su ranking e reputational feedback system[26].
Ove i dati rientrino nell'ambito della definizione di dati personali si applicherà il regolamento 679/2016 per la protezione dei dati personali delle persone fisiche e la libera circolazione dei dati, cosiddetto GDPR[27]. Tuttavia, anche nell'ambito contrattuale (e anche con riguardo al trattamento di dati non personali), rivestono una centrale importanza le questioni concernenti quali dati siano raccolti, come siano utilizzati, chi può accedervi e chi può scaricarli e utilizzarli; anche qualora non si tratti di dati personali.
In quest'ottica, i diritti più rilevanti concernenti i dati, sono il diritto di accesso e il diritto alla portabilità del dato, mentre il diritto all'oblio diviene un limite nell'utilizzo dei dati, un diritto di recesso dalla prestazione della fornitura dei dati sempre esercitabile

[24] S. Niger, *Sorveglianza e nuovi diritti di libertà*, in G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in F. Galgano (diretto da), *Trattato di diritto commerciale e di diritti pubblico dell'economia*, XLVIII, Padova, 2008.

[25] Per una ricostruzione delle principali voci su questo tema si veda G. Ziccardi, *Internet controllo e libertà*, Milano, 2015, 143 ss.

[26] Nella platform economy, ad esempio, i dati rilevano per la realizzazione dei match, la descrizione di prodotti e servizi, la profilazione dei customers, il ranking e i reputational feedback system. Cfr. S. P. Choudary, *Platform Scale*, Platform Thinking Labs, 2015; G. G. Parker et al., *Platform Revolution. How networked markets are transforming the economy and how to make them work for you*, New York, 2016; M. E. Stucker-A. P. Grunes, *Big Data and Competition Policy*, Oxford, 2016; M. Zeng, *Smart Business. I segreti del successo di Alibaba*, Milano, 2018.

[27] Sia consentito un rinvio a S. Martinelli, *Commento all'art. 4 del GDPR (Definizioni),* in E. Gabrielli (diretto da), A. Barba-S. Pagliantini (a cura di), *Commentario del Codice Civile*, Modulo Delle Persone, II, Milano, 2019.

dall'interessato[28].

Il diritto alla portabilità dei dati, in particolare, di cui all'art. 20 del GDPR e che consiste nel diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento[29], è ancora uno dei diritti degli interessati meno utilizzato, sviluppato e sfruttato, ma costituisce una delle sfide più urgenti per ridurre gli effetti lock-in e favorire la concorrenza in un mercato fortemente accentrato e potrebbe trovare estensione anche oltre la definizione di dato personale.

Alcune normative europee di nuova introduzione sono intervenute per regolare i dati anche in ambito contrattuale. Essi sono oggetto di alcune disposizioni della Digital Content Directive (direttiva 770/2019), nell'ambito della tutela dei consumatori, nonché del regolamento 1150/2019, per la protezione dei business users[30].

Al Considerando 24 della Digital Content Directive, in particolare, è evidenziato che spesso il consumatore non paga un prezzo per il servizio fornendo, invece, i suoi dati; nonché che i dati, pur non potendo essere considerati una merce, essendo la protezione dei dati personali un diritto fondamentale, possono essere oggetto di rimedi contrattuali. Viene per la prima volta affermato, quindi, che la direttiva dovrebbe applicarsi «ai contratti in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o servizi digitali al consumatore e in cui il consumatore fornisce, o si impegna a fornire, dati personali» quale controprestazione[31].

All'art. 16 della direttiva, dedicato agli obblighi dell'operatore economico verso il consumatore in caso di risoluzione, sono, inoltre, previste disposizioni relative al destino dei dati e dei contenuti digitali[32].

L'operatore economico è tenuto ad astenersi «dall'utilizzare qualsiasi contenuto diverso dai dati personali che sia stato fornito o creato dal consumatore nell'ambito dell'utilizzo del contenuto digitale o del servizio digitale fornito dall'operatore economico, fatto salvo il caso in cui tale contenuto:

a)sia privo di utilità al di fuori del contesto del contenuto digitale o del servizio digitale fornito dall'operatore;

b)si riferisca solamente all'attività del consumatore nell'utilizzo del contenuto digitale

---

[28] Cfr. S. Thobani, *Diritti della personalità e contratto*, Torino, 2018, 171 ss; C. Bedir, *Contract Law in the Age of Big Data*, in *European Review of Contract Law*, 16, 3, 2020.

[29] Cfr. M. E. Stucker - A. P. Grunes, *Big Data and Competition Policy*, Oxford, 2016; I. Graef-M. Husovec-N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, in *German Law Journal*, 19, 6, 2018, 1359 ss.; I. Graef-J. Verschakelen-P. Valcke, *Putting the right to data portability into a competition law perspective*, in *The Journal of the Higher School of Economics*, Annual Review, 53 ss., 2013; S. Martinelli, Sharing *Data and Privacy in the Platform Economy: The Right to Data Portability and «Porting Rights»,* in L. Reins (a cura di), *Regulating New Technologies in Uncertain Times*, The Hague, 2019, 113 ss.

[30] Cfr. C. Cauffman, *New EU rules on business-to-consumer and platform-to-business relationships*, in *Maastricht Journal of European and Comparative Law*, 26, 4, 2019, 469 ss.; A. Palmieri, *Profili giuridici delle piattaforme digitali*, Torino, 2019; C. Twigg-Flesner, *The EU's Proposals for Regulating B2B Relationships on online platforms – Transparency, Fairness and Beyond*, in *European Consumer and Market Law*, 7, 6, 2018, 222 ss.

[31] Cfr. S. Lohsse . R. Schulze, D. Staudenmayer (a cura di), *Data as Counter-Performance* – Contract Law 2.0? Münster Colloquia on EU Law and the Digital Economy, Oxford, 2020; S. Thobani, *Diritti della personalità e contratto*, Torino, 2018.

[32] Il secondo comma dell'articolo fa comunque salva l'applicazione del regolamento 679/2016.

o del servizio digitale fornito dall'operatore;
c)sia stato aggregato dall'operatore economico ad altri dati e non possa essere disaggregato o comunque non senza uno sforzo sproporzionato; o
d) sia stato generato congiuntamente dal consumatore e altre persone, e altri consumatori possano continuare a utilizzare il contenuto»[33].
Escluse le ipotesi di cui alle lettere a, b e c, l'operatore economico è tenuto a mettere a disposizione del consumatore, su richiesta dello stesso, gratuitamente e senza impedimenti, entro un lasso di tempo ragionevole e in un formato di uso comune e leggibile da dispositivo automatico, «i contenuti diversi dai dati personali, che sono stati forniti o creati dal consumatore durante l'utilizzo del contenuto digitale o del servizio digitale fornito dall'operatore economico»[34].
Il regolamento 1150/2019 dedica ai dati l'articolo 9, imponendo obblighi informativi, sia rispetto ai dati trattati e ai dati ai quali il business user può avere accesso.
Le piattaforme sono tenute a inserire nelle condizioni generali di contratto «una descrizione relativa all'accesso tecnico e contrattuale» ai dati personali o non personali forniti dai business users o dai consumatori forniti o generati nell'utilizzo del servizio; oppure, ove non venga fornita la possibilità di eseguire tale accesso, una dichiarazione in tal senso[35]. La descrizione deve informare il business user in merito:
a) alla possibilità per la piattaforma di intermediazione di accedere ai dati, personali e non personali forniti o generati dai consumatori e dai business users per l'utilizzo dei servizi di intermediazione online, specificando le categorie di dati interessate e le condizioni;
b) alla possibilità per il business user di accedere ai medesimi dati, specificando le categorie e le condizioni;
c) la possibilità di accedere a tali dati in forma aggregata («forniti o generati mediante la fornitura di servizi di intermediazione online a tutti gli utenti commerciali e ai relativi consumatori»), con specificazione;
d) alla fornitura a terzi dei dati di cui alla lett. a specificando al contempo, ove tale fornitura a soggetti terzi non sia necessaria per l'esecuzione del contratto, la finalità di tale condivisione e le possibilità di cui i business users dispongono «per esimersi da tale condivisione dei dati»[36].
Entrambe le disposizioni citate, art. 16 della direttiva e art. 9 del regolamento forniscono dettagliate discipline in relazione ai dati. Rispetto al consumatore, con riguardo al momento della conclusione del rapporto, prevedendo l'astensione dall'utilizzo ulteriore dei dati da parte del provider, con ampie esclusioni, nonché il diritto del consumatore di ricevere i dati, anch'esso correlato da esclusioni. Rispetto al business users, invece, la regolazione si è incentrata sulla trasparenza in relazione ai dati trattati e sui diritti di accesso a tali dati.
L'attenzione all'accesso per i business user e all'interruzione del rapporto rispetto ai consumatori ricalca quelli che sono i preminenti interessi delle due categorie e risente

[33] Cfr. art. 16, par. 4, della direttiva..

[34] Cfr. art. 16, par. 4-5, della direttiva.

[35] Cfr. art. 9, par. 1, del regolamento.

[36] Cfr. art. 9, par. 2, del regolamento.

del fatto che per il consumatore, essendo egli necessariamente anche interessato, è già destinatario dell'informativa sul trattamento in relazione ai dati personali trattati, tuttavia pare che vi sia, ad avviso di chi scrive, la necessità di una regolamentazione più ampia e uniforme tra le due categorie di soggetti, entrambi utenti della piattaforma o servizio digitale.

4. Qualche conclusione

Alla luce del quadro descritto, pur mantenendo distinte le due discipline (quella relativa al trattamento dei dati personali e quella relativa alla disciplina contrattuale del rapporto)[37], si immagina un'espansione della regolazione contrattuale concernente i dati, personali e non personali, strumento principe per la gestione del valore del dato dal punto di vista economico, e si ipotizza, de iure condendo, una più completa e dettagliata disciplina dei diritti e dei rapporti concernenti dati, in particolare a tutela degli utenti, contraenti deboli in un rapporto contrattuale sbilanciato.
Tale disciplina dovrebbe dialogare con la protezione dei dati personali e distinguere tra le ipotesi di dati personali e non personali e, in ogni caso, ricomprendere:

- un obbligo di informativa sui dati, personali e non personali, che il fornitore del servizio tratta, con specificazione delle categorie e delle finalità;
- un obbligo di informativa relativo ai soggetti terzi che hanno accesso a tali dati, con specificazione delle categorie di dati e delle finalità della condivisione e delle possibilità di cui gli utenti dispongono per esimersi da tale condivisione dei dati;
- un obbligo di informativa sulla possibilità di accedere a tali dati in forma aggregata;
- i diritti di accesso dell'utente a tali dati, personali e non personali, con possibilità di introdurre diritti di accesso garantiti e non modificabili in pejus contrattualmente;
- il diritto alla portabilità dei dati, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, da dettagliarsi con riguardo alla tipologia di dati oggetto del diritto e alle modalità tecniche, e da rendere non modificabile contrattualmente, almeno con riguardo ad alcune categorie di dati, al fine di favorire la concorrenza e diminuire il lock-in;
- le conseguenze del diritto alla revoca del consenso e dell'esercizio del diritto alla cancellazione dei dati personali, da regolarsi in conformità alla disciplina per la tutela dei dati personali, facendo pienamente salvo il diritto all'autodeterminazione informativa e il potere di disporre dei dati che ci riguardano[38];
- un obbligo informativo relativo all'utilizzo dei dati al termine del rapporto concernente: la possibilità di accedervi e il tempo del mantenimento del diritto di accesso e alla portabilità;
- nullità delle disposizioni contrattuali volte ad impedire l'utilizzo dei dati oggetto del diritto alla portabilità, con esclusioni;
- definizione di strumenti e misure sanzionatorie efficaci per garantire il rispetto delle norme sopradescritte anche in un contesto di forte squilibrio contrattuale.

[37] S. Thobani, *Diritti della personalità e contratto*, Torino, 2018, 159.

[38] Ivi, 153 ss.

Lungi dal trarre conclusioni definitive rispetto alla regolazione di un mercato ancora poco studiato e in veloce divenire, s'intende contribuire all'animare una più ampia riflessione sulla disciplina applicabile ai dati nel loro utilizzo, che pur trovando i suoi limiti nella tutela della persona e della sua personalità, necessita di adeguate forme di tutela che non possono prescindere dal riconoscimento del loro valore economico.
Una possibile disciplina contrattuale dell'utilizzo dei dati così abbozzata dovrebbe poi essere affiancata da una diversa disciplina concernente l'algoritmo e, quindi, l'utilizzo del dato, in una dimensione dinamica[39], fondata sui principi dell'accountability e dalla valutazione del rischio[40], affiancate da dettagliati normativi relativi ad alcune applicazioni specifiche, rispetto ai quali la normativa sopradescritta in materia di reputational feedback system può costituire un primo esempio.

[39] Cfr. P. Palka*, Data Management Law for the 2020s: the Lost Origins and the New Needs,* in *Buffalo Law Review*, 2, 68, 2020, 559 ss.

[40] Cfr. A. Koene et al., *A governance framework for algorithmic accountability and transparency*, EPRS, 2019; C. Busch, *Algorithmic Regulation and (Im)Perfect Enforcement in the Personalized Economy*, in C. Busch-A. De Franceschi, *Handbook on Personalized Law*, Oxford, 2020.

La relazione di cura nell'era della comunicazione digitale*

Massimo Foglia

Abstract

Nell'era della comunicazione digitale e dei social network, accade con frequenza sempre maggiore che la comunicazione medico-paziente avvenga anche a distanza, con l'ausilio di strumenti quali e-mail, social network, sms, messaggi WhatsApp e via dicendo. Il presente contributo si sofferma sul problema della spersonalizzazione del rapporto medico-paziente, nonché sull'emergere di nuovi scenari di responsabilità sanitaria connessi appunto all'impiego di mezzi di comunicazione digitali.

In the age of digital communication and social networks, the doctor-patient communication is increasingly performed via remote, using means like e-mails, SMS, WhatsApp messages and so on. This article deals with the issue of the depersonalization of the doctor-patient relationship, as well as on the emergence of new basis of medical liability related to the use of digital communication means.

Keywords

relazione di cura – comunicazione digitale – responsabilità medica

1. Introduzione

Nell'era della comunicazione digitale e dei social media, accade con frequenza sempre maggiore che la relazione di cura sia condotta anche a distanza, con l'ausilio di strumenti quali e-mail, social network, sms, messaggi WhatsApp e via dicendo[1]; nuovi

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

[1] V., di recente, A. Spina, *La medicina degli algoritmi: Intelligenza Artificiale, medicina digitale e regolazione dei dati personali*, in F. Pizzetti (a cura di), *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 319 ss.; L. Rufo, *Social media e consulto medico: tra opportunità e rischi per i pazienti*, in *Inform. e dir.*, 2017, 1-2, 383 ss.; G. Pascuzzi - U. Izzo, *Le problematiche giuridiche connesse all'utilizzo delle nuove tecnologie in sanità,* in *psychiatryonline.it* (3 novembre 2012); M. De Angelis, *Alcune questioni giuridiche sulla regolamentazione del progresso tecnologico in sanità*, in *Diritto & questioni pubbliche*, 2017, 31; E. Pietrafesa - R. Di Leo - M.

canali telematici per mezzo dei quali il paziente comunica a distanza con il medico curante, al fine di metterlo a parte dei sintomi di una malattia o per trasmettergli i risultati di analisi, oppure ancora per formulare richieste di vario tipo.

L'odierno impiego dei mezzi di comunicazione digitale può essere visto come un contemporaneo simbolo di separazione che allontana il medico dal paziente, come accaduto in passato con l'invenzione dello stetoscopio[2]: un tempo lontano, il gesto che vedeva il medico accostare l'orecchio al torace di un malato, quasi nell'atto di cingerlo tra le braccia, colmava una distanza, un vuoto.

Due, in particolare, sono le conseguenze del processo di allontanamento del medico dal paziente che il presente contributo si propone di affrontare.

La prima concerne la spersonalizzazione del rapporto medico-paziente ed i riflessi negativi che la privazione di una relazione di cura individuale provoca nell'accompagnamento del malato: il dialogo ed il confronto tra questi ed i curanti sono presupposti di una vera consensualità; l'aspetto relazionale e comunicativo della prestazione sanitaria costituisce il momento di saldatura di un dovere giuridico oltre che etico[3], e rappresenta l'espressione di un generale principio di solidarietà sociale, in grado di dare concretezza al ruolo del consenso nell'ambito del rapporto terapeutico, che impone al professionista di agire nell'ottica dell'interesse altrui a prescindere dall'esistenza di specifici obblighi contrattuali o di quanto espressamente stabilito da singole norme di legge[4].

Il secondo aspetto, invece, riguarda l'emergere di nuovi scenari di responsabilità sanitaria connessi all'impiego di mezzi di comunicazione digitali. Dal tema della comunicazione discendono problematiche che si riallacciano ai profili della responsabilità medica[5]. La comunicazione è infatti il veicolo dell'informazione, che a sua volta è il presupposto del consenso all'atto medico. Da qui si può cogliere chiaramente il *filo rosso* fra la dinamica del rapporto medico-paziente e il discorso giuridico sul consenso informato nelle sue varie declinazioni[6].

Castriotta, *ICT [Tecnologie dell'informazione e della comunicazione] e mercato tra nuove professioni e rischi emergenti*, in *Rivista degli infortuni e delle malattie professionali*, I, 2014, 405 ss.

[2] In questi termini S.B. Nuland, *How We Die: Reflections on Life's Final Chapter* (1993), trad. it. *Come moriamo. Riflessioni sull'ultimo capitolo della vita*, Milano, 1994, 297: «Questo ruolo assunto dagli strumenti fu considerato positivamente già dalla comunità medica del tempo: pochi clinici si sentivano (e si sentono tuttora) a proprio agio dovendo accostare l'orecchio al torace di un malato. A tale ragione e alla sua immagine, rappresentativa di un particolare status, questo strumento [lo stetoscopio, ndr] deve la sua popolarità; basta trascorrere qualche ora seguendo un giovane medico interno mentre fa il giro del reparto per osservare i diversi ruoli che assume questo simbolo di autorità e di separazione».

[3] Da ultimo con la legge 22 dicembre 2017, n. 219 ("Norme in materia di consenso informato e disposizione anticipate di trattamento"). V., in part., l'art. 1, c. 8, ove si legge che «Il tempo della comunicazione tra medico e paziente costituisce tempo di cura».

[4] Anche sotto questo profilo si avverte l'esigenza di un ripensamento del rapporto medico-paziente. In questi termini R. Pucella, *È tempo per un ripensamento del rapporto medico-paziente?*, in *Resp. medica*, 2017, 3 ss. Il consenso alle cure non è un elemento stabile e risente di innumerevoli fattori personali, psicologici, familiari, sociali, culturali e religiosi. Cfr. *Raccomandazioni della SICP: Informazioni e consenso progressivo in cure palliative: un processo evolutivo condiviso* (ottobre 2015).

[5] In tale prospettiva v., per tutti, R. Pucella, *Autodeterminazione e responsabilità nella relazione di cura*, Milano, 2010, spec. 153 ss.

[6] Per un approfondimento sia consentito il rinvio a M. Foglia, *Consenso e cura. La solidarietà nel rapporto*

Prima di affrontare le singole questioni suddette, è utile delineare lo sfondo sul quale esse si innestano, descrivendo talune peculiarità della realtà sanitaria che incidono inevitabilmente sul presente discorso.

2. Comuni-*care*: tempi e luoghi del consenso alle cure

La questione del consenso del paziente all'atto medico è molto antica. Per secoli il principio del consenso al trattamento è rimasto estraneo al rapporto medico-paziente. Un mondo "silenzioso"[7], caratterizzato da un forte paternalismo, in cui il malato è stato sostanzialmente privato della sua competenza e della sua libertà di decidere[8]. Nello scenario odierno, di contro, si può affermare che il credo paternalistico del "*doctor knows best*" abbia forse raggiunto il punto più avanzato della sua fase discendente, verso quel progressivo cambiamento culturale che ha portato nella pratica sanitaria ad un nuovo e diverso modo di pensare, favorevole ad un *empowerment* del paziente[9], specialmente sotto il profilo del suo diritto ad essere informato e posto nelle condizioni di assumere scelte terapeutiche consapevoli[10].
Lo ha ribadito, di recente, la *Supreme Court* inglese sottolineando con parole efficaci come il dovere del medico non possa dirsi assolto «bombardando il paziente di informazioni tecniche»; informazioni che probabilmente egli non sarà neppure in grado di comprendere[11].
Ebbene, in Italia, la legge n. 219/2017, in materia di consenso informato e disposizioni anticipate di trattamento, ha lanciato una sfida culturale al mondo della sanità, e in particolare ai medici chiamati ad abbandonare la postura mentale della medicina paternalistica. Tra questi principi giuridici vi è quello secondo il quale «il tempo della comunicazione tra medico e paziente costituisce tempo di cura» (art. 1, c. 8) ed il con-

terapeutico, Torino, 2018.

7 Parla di "mondo silenzioso" il medico americano J. Katz nel suo libro Id., *The Silent World of Doctor and Patient*, New York, 1984, 1 ss., in cui l'A. ripercorre le tappe storiche del rapporto medico-paziente.

8 I documenti storici testimoniano come siano mutati tanto il comportamento del paziente nei confronti del medico quanto la natura dei loro reciproci rapporti. Cfr. P. Ariès, *Essais sur l'histoire de la mort en Occident* (1975), trad it. *Storia della morte in occidente*, Milano, 1998, 69. Sul tema attuale dell'isolamento del morente, v. N. Elias, *Über die Einsamkeit der Sternbenden in unseren Tagen* (1982), trad. it. *La solitudine del morente*, Bologna, 1985.

9 Cfr. F.D. Busnelli, *Il fattore "potenziamento": salute, medicina e deontologia al vaglio delle nuove tecnologie*, in *Resp. medica*, 2017, 315 ss.

10 Da un modello centrato sulla malattia ("*disease centred*"), il cui obiettivo è semplicemente raggiungere una diagnosi corretta e intervenire attraverso strategie terapeutiche adeguate, si è progressivamente passati, a partire dagli anni '80, ad una "*patient-centred medicine*", un modello centrato sul paziente: scopi della visita medica sono il raggiungimento di una diagnosi corretta, la comprensione del vissuto/prospettiva del paziente e l'intervento attraverso strategie terapeutiche adeguate.

11 *Montgomery v. Lanarkshire Health Board* [2015] UKSC 11, par. 90: «*…the doctor's advisory role involves dialogue, the aim of which is to ensure that the patient understands the seriousness of her condition, and the anticipated benefits and risks of the proposed treatment and any reasonable alternatives, so that she is then in a position to make an informed decision. This role will only be performed effectively if the information provided is comprehensible. The doctor's duty is not therefore fulfilled by bombarding the patient with technical information which she cannot reasonably be expected to grasp, let alone by routinely demanding her signature on a consent form*».

senso informato è l'«incontro» – e dunque il confronto – tra «l'autonomia decisionale del paziente e la competenza, l'autonomia professionale e la responsabilità del medico» (art. 1, c. 2).

Eppure, le caratteristiche dell'attività sanitaria, come la velocità dei ritmi lavorativi o la mancanza di tempo e di spazio dedicati al dialogo con i pazienti[12], contribuiscono ancora oggi all'idea fallace secondo la quale il consenso alle cure si riduce alla compilazione di un modulo, quando invece il momento comunicativo consente al paziente di conoscere tutte le informazioni necessarie al fine di operare scelte di cura consapevoli e serve nel contempo al medico affinché questi non sia estraneo alla decisione che matura nella sfera del malato[13].

È probabile che il medico in cuor suo sappia che il consenso del paziente è molto più di una pratica modulistica. La sensazione è che gli operatori della salute stiano iniziando a vedere le regole del consenso informato sotto un'altra luce, e a riconoscere in esse un utile strumento della relazione di cura[14].

La regola, anche di natura deontologica[15], postula una vera e propria interazione tra il medico e il paziente, ponendosi l'obiettivo di colmare quel *deficit* di partenza che caratterizza la relazione di cura, allo scopo di riequilibrare il rapporto con il soggetto

---

[12] V., ad esempio, la testimonianza di L. Fontanella, *La comunicazione diseguale. Ricordi di ospedale e riflessioni linguistiche,* Roma, 2011.

[13] R. Pucella, *Autodeterminazione e responsabilità nella relazione di cura*, cit., 84 s.: «È il medico che conosce le malattie, che ne ha chiare le cause e di rimedi; di fronte a lui vi sono il malato ed il suo vissuto. [...] Nessuno dei due possiede la verità, che sgorga, invece, dal riconoscimento del vissuto del malato come storia. Lo strumento attraverso il quale questo obbiettivo si realizza è il dialogo, per mezzo del quale il paziente è sollecitato a far riaffiorare il vissuto alla coscienza; non si tratta, però, di ricorrere alla semplice anamnesi, intesa come interrogatorio guidato dell'ammalato, diretta a far risalire alla sua memoria un vissuto che consente al medico di pronunciare la diagnosi. […] Se, dunque, il medico non può rinunciare alla funzione cognitiva del malato, quest'ultimo ha bisogno dell'aiuto del medico nel perseguire la sua miglior salute».

[14] V. P. Borsellino, *Consenso informato. Una riflessione filosofico-giuridica sul tema*, in *Salute e società*, 3, 2012, 17 ss. Lo testimonia anche il fatto che vengono organizzati molti convegni al riguardo e che in letteratura sono sempre più numerosi i riferimenti alla centralità della relazione di cura. Ma l'attuale, complessa realtà sanitaria presenta ancora forti criticità. Ciò può essere dovuto ad un insieme di fattori che il giurista non può ignorare. In medicina, come in qualunque professione, bisogna infatti fare i conti con le risorse, con i sistemi e con gli assetti organizzativi consolidati. Sul passaggio «dall'ospedale all'azienda» v. R. Lusardi - S. Tomelleri, *Non è solo retorica. Le immagini della collaborazione in sanità*, in *Rass. it. sociologia*, 2016, 55 ss., spec. 62. L'attuale funzionamento dell'organizzazione ospedaliera è riconducibile al modello industriale, risponde a logiche di mercato e mira al raggiungimento di determinati obiettivi di produzione. Maggiore è il numero di pazienti assistiti ogni anno, più alta è la redditività delle aziende ospedaliere, anche del settore pubblico, che ottengono finanziamenti in proporzione al numero delle prestazioni offerte ai pazienti. Da ciò deriva un'esigenza di velocizzare le prestazioni sanitarie: fenomeno che avvicina i luoghi dello spazio ospedaliero, come gli ambulatori, le sale operatorie e le sale parto, a «luoghi il cui funzionamento ricorda per molti aspetti quello di una *catena di montaggio*» (C. Quagliariello - C. Fin, *Il consenso informato in ambito medico. Un'indagine antropologica e giuridica*, Bologna, 2016, 77 ss., corsivo dell'A.). A ciò si aggiunga il progressivo aumento dei pazienti accolti nelle strutture sanitarie e, come conseguenza, il sovraffollamento dello spazio ospedaliero, accentuato dalla carenza di personale medico.

[15] Il Codice di deontologica medica (2014) dispone che, nell'informare il paziente, «il medico adegua la comunicazione alla capacità di comprensione della persona assistita o del suo rappresentante legale, corrispondendo a ogni richiesta di chiarimento, tenendo conto della sensibilità e reattività emotiva dei medesimi, in particolare in caso di prognosi gravi o infauste, senza escludere elementi di speranza» (art. 33, c. 2).

professionista che detiene il bagaglio informativo[16]. Se il paziente non fosse in grado di comprendere "realmente" ciò che il medico gli comunica, il consenso espresso dal malato non potrebbe dirsi effettivo né la sua volontà autentica, poiché mancherebbe una vera conoscenza e comprensione delle informazioni comunicategli su cui fondare la scelta terapeutica.

In altre parole, il processo comunicativo include quello informativo[17], ma si svolge nell'ambito del rapporto interpersonale di cui il malato è parte attiva[18]. Una delle esigenze principali dei malati e dei familiari è infatti quella di relazionarsi con i professionisti. Essi chiedono il dialogo con il personale sanitario, e desiderano risposte, spiegazioni[19].

Molti medici ammettono che "parlare" con il malato è quasi sempre d'aiuto ma spesso non viene fatto; che per migliorare le cure, specialmente quelle di fine vita, «ogni medico dovrebbe essere un esperto di comunicazione»[20]. Tutto ciò è ancor più vero se si pensa che a volte la medicina non può fare alcunché per vincere la malattia: «quando non c'è posto per il bisturi, le parole sono l'unico strumento del chirurgo»[21].

La parola allora "guarisce" [22], acquista il senso di una cura in grado, entro lo spazio

---

[16] «L'uno sa e l'altro ignora», come osserva M. Portigliatti Barbos, *Il modulo medico di consenso informato: adempimento giuridico, retorica, finzione burocratica?*, in *Dir. pen. proc.*, 1998, 894. È sempre nell'ottica di questo rapporto dialogico che il Codice di deontologia prevede che «ogni ulteriore richiesta di informazione da parte del paziente deve essere soddisfatta» (art. 33, c. 3), disponendo che sul medico incombe l'obbligo di fornire «le informazioni riguardanti prognosi gravi o infauste o tali da poter procurare preoccupazione e sofferenza alla persona», ma con la cautela – dice il Codice – di informare «con prudenza, usando terminologie non traumatizzanti e senza escludere elementi di speranza» (art. 33, c. 5).

[17] È solo attraverso il dialogo medico-paziente che si possono individuare le quattro dimensioni che caratterizzano il malato nella difficile convivenza con la malattia: i.) la dimensione delle *idee di malattia*; ii.) la dimensione dei *sentimenti*; iii.) la dimensione delle *aspettative*; iv.) la dimensione del *contesto*. L'insieme di queste quattro dimensioni viene identificato nella letteratura medica con l'efficace espressione «agenda del paziente», che, a differenza del più ristretto concetto di "vissuto del paziente", implica una «dimensione relazionale», poiché sta ad indicare «il vissuto della malattia *portato* al medico» (così E.A. Moja - P. Poletti, *Comunicazione e performance professionale: metodi e strumenti*, II, *La comunicazione medico-paziente e tra operatori sanitari* (Aprile 2016), Ministero della Salute, Direzione Generale della Programmazione Sanitaria, 10, reperibile nel sito internet del Ministero.

[18] Com'è stato ben descritto da un medico palliativista: «Comunicare la diagnosi non è semplicemente fornire un'informazione. […] Informazione e comunicazione non sono la stessa cosa […] La comunicazione integra l'informazione all'interno di un processo relazionale, usa la continuità della relazione come strumento» (così G. Lonati, *L'ultima cosa bella. Dignità e libertà alla fine della vita*, Milano, 2017, 21).

[19] Cfr. A. Gawande, *The Heroism of Incremental Care*, The New Yorker, January 23, 2017, trad. it. *Il medico che ti può salvare la vita*, in *Internazionale*, 10 novembre 2017, n. 1230, 43 ss.: «Ho cominciato a capire […] quando mi sono accorto che i dottori, gli infermieri e il personale che lavorava all'accoglienza chiamavano per nome quasi tutti i pazienti che entravano. Spesso li conoscevano da anni e avrebbero continuato a vederli per anni. Osservandolo mentre si occupava di un paziente che era arrivato con dolori all'addome, Asaf non mi sembrava un dottore speciale. Ma quando mi sono reso conto che medico e paziente si conoscevano sul serio […] ho cominciato a capire l'importanza di quella familiarità».

[20] *The Economist*, A Better Way to Care for the Dying, April 29, 2017, trad. it. *Verso la fine*, in *Internazionale*, 16 giugno 2017, n. 1209, 42 ss., dove si apprende, per esempio, che gli oncologi statunitensi devono sostenere una media di 35 colloqui al mese sul fine vita.

[21] P. Kalanithi, *When Breath Becomes Air* (2016), trad. it. *Quando il respiro si fa aria*, Milano, 2016, 57.

[22] Cfr. M. Graziadei, *Il consenso informato e i suoi limiti*, in *Trattato di biodiritto*, diretto da Rodotà e Zatti, *I diritti in medicina*, a cura Lenti, Palermo Fabris, Zatti, Milano, 2011, 220. Nella letteratura medica v., di recente, R. Milanese - S. Milanese, *Il tocco, il rimedio, la parola. La comunicazione tra paziente e medico come*

di relazione col malato, di restituire dignità e significato all'esperienza della malattia e della morte.
Non stupisce, dunque, che una delle cause più comuni dello stress tra i medici sia proprio l'incapacità di parlare della morte con i pazienti. Quasi tutti gli oncologi che visitano malati terminali ammettono che nessuno mai ha insegnato loro a parlare con questo tipo di pazienti[23].
Non va infine dimenticato che la comunicazione può incidere anche sullo stato d'animo dei familiari o delle persone vicine al malato. Dai racconti dei medici si ha conferma che all'arrivo di un paziente in gravi condizioni, la prima conversazione con il medico potrebbe segnare per sempre il ricordo che la famiglia crea di quella morte[24]. I familiari possono accoglierla pacificamente e accettare che sia giunta l'ora di una fine ineluttabile, oppure rifiutarla dolorosamente e magari accusare i medici di non aver fatto tutto il possibile per salvare la vita del proprio caro.
È dunque chiara la ragione per la quale nella relazione tra il medico e il paziente è essenziale la comunicazione, quale momento strutturale del rapporto medico-paziente. Da tali considerazioni appare evidente come la "digitalizzazione" della comunicazione nella relazione di cura abbia provocato un vuoto, di fatto un'assenza di dialogo che innegabilmente produce effetti negativi sul rapporto medico-paziente e sull'accompagnamento del malato.

3. Una relazione "a distanza"

L'atto medico presuppone sempre l'"incontro" tra due persone. Sin dalla medicina antica si insegna che alla base di tutto c'è un contatto «umano» tra il medico ed il paziente, quel contatto umano che il progresso tecnologico e l'inevitabile burocratizzazione della pratica medica rischia di spersonalizzare, di inibire, di raffreddare.
È accaduto di recente negli Stati Uniti che un familiare venisse informato del decesso del proprio caro da un robot entrato nella stanza in cui egli si trovava in attesa di notizie. In un mondo dominato dalle macchine, tale fatto non stupisce ma deve sollecitare una riflessione.

strumento terapeutico, Firenze, 2015, in cui è svolta un'analisi estesa sull'influenza della comunicazione sull'agire terapeutico.

[23] *The Economist*, April 29, 2017, cit. Per colmare questo vuoto l'*Ariadne Labs*, un gruppo di ricerca fondato dal noto medico statunitense Atul Gawande, ha compilato una "*Guida alle conversazioni con i malati gravi*", una lista molto semplice degli argomenti che i medici dovrebbero affrontare con i malati terminali (il materiale è consultabile nel sito web*ariadnelabs.org*). Da questa guida emerge, ad esempio, che i medici dovrebbero chiedere al paziente quanto sa della sua malattia, verificare quanto vuole sapere, fare una prognosi sincera, domandargli quali siano i suoi desideri e quali compromessi è disposto a fare. Un testo fondamentale sulla comunicazione tra medico e malato terminale è della psichiatra E. Kübler-Ross, *On Death and Dying* (1969), trad. it. *La morte e il morire*, Assisi, 2013.

[24] P. Kalanithi, *Quando il respiro si fa aria*, cit., 57. Sul punto v. anche M. Marzano, *Scelte finali. Morire di cancro in Italia*, Bologna, 2004, 67: «Le decisioni comunicative adottate nella prima fase della malattia condizionano pesantemente tutti gli eventi successivi, secondo una sorta di effetto "imprinting" per cui la "prima mossa è quella che conta". La ragione di questo effetto è legata all'azione dei dispositivi fiduciari, e cioè relativi al "contesto di aspettative aventi una valenza positiva per l'attore sociale e formulate in condizioni di incertezza"» (corsivo dell'A.).

Nell'era tecnologica viviamo e interagiamo con i robot e gli agenti artificiali in generale, così la scena della realtà ci costringe una volta di più a ripensare la scena del diritto. Dagli innovativi studi sulla c.d. mente incorporata (*embodied mind*), dove è riconosciuto un ruolo fondamentale, nella conoscenza umana, al corpo e alle emozioni, emerge che il progresso nella conoscenza della nostra "socialità" è fondamentale se si vuole elaborare un «programma che permetta ad un agente robotico di partecipare in modo convincente e moralmente accettabile a un'interazione sociale». Su tale premessa, al fine di introdurre un robot come partner sociale in una casa di riposo, una scuola, un ospedale o un supermercato, occorre implementare nei robot sociali forme di "empatia artificiale"; e per far questo è necessario comprendere a fondo come funziona l'emozionalità umana, apprendere i meccanismi fisiologici che stanno alla base dell'arrossire, del piangere o del suicidarsi[25].

Tali considerazioni si riallacciano al tema della comunicazione digitale, della relazione "a distanza" tra il medico e il malato o comunque al tema della relazione "mediata" dalla macchina. In questo scenario, infatti, l'introduzione della tecnologia nelle strutture sanitarie ha per certi versi acuito, nello specifico, il problema comunicativo[26]. Da un lato la tecnologia ha certamente contribuito ad accorciare i tempi della prestazione sanitaria e ad incrementare la qualità del servizio ma, per altro verso, il problema comunicativo, ora traslato anche nella dimensione digitale, ha determinato, come già sottolineato, un allontanamento del medico dal paziente. Non sembra infatti che il tempo "risparmiato" grazie ad una più agevole erogazione dei servizi sanitari sia andato a vantaggio del tempo dedicato alla relazione e al dialogo con il paziente.

Ad ulteriore conferma di questa tendenza alla separazione del medico dal paziente si pensi al diffuso impiego della "telemedicina", in virtù della quale per la realizzazione di talune pratiche mediche, per lo più diagnostiche, non vi è la necessaria compresenza nel medesimo luogo del paziente o dell'operatore sanitario, operando quest'ultimo sulla esclusiva base di dati a lui pervenuti attraverso tecnologie informatiche il cui utilizzo, appunto, consente lo svolgimento di atti medici anche "fra assenti"[27].

Va però osservato, per completezza, che la comunicazione mediata dalla tecnologia offre nuove potenzialità di interazione e di cura. L'uso della tecnologia in medicina non va certamente osteggiato, ma accolto e governato. Una medicina fortemente tecnologizzata, le cui potenzialità si concentrano quasi esclusivamente sul corpo inteso come organismo, richiede d'altro canto un maggior investimento nella umanizzazione delle cure nella prospettiva più sopra delineata.

---

[25] Per approfondimenti v. P. Dumouchel - L. Damiano, *Vivere con i robot. Saggio sull'empatia artificiale*, Milano, 2019, spec. 60.

[26] Nell'ambito del rapporto professionale si parla ormai da tempo anche di "deontologia digitale": v. A. Graziani, *La deontologia digitale*, in *Arch. civ.*, 2002, 429 ss.

[27] Così Cass. pen., sez. III, 17 settembre 2019, n. 38485, in *Riv. pen.*, 2019, 1036. Per ulteriori approfondimenti v. C. Leanza, *La telemedicina: profili civilistici di responsabilità*, in *Rass. dir. farm.*, 2020, 531 ss.; C. Botrugno, *La diffusione dei modelli di cura a distanza: verso un "diritto alla telesalute"?*, in *Rivista di Biodiritto*, 2014, 17 ss.; Id., *Un diritto per la telemedicina: analisi di un complesso normativo in formazione*, in *Pol. dir.*, 2014, 639 ss.; C. Filauro, *Telemedicina, cartella clinica elettronica e tutela della privacy*, in *Danno resp.*, 2011, 472 ss.; R. D'Angiolella, *Responsabilità e telemedicina*, in *Rass. dir. civ.*, 2009, 921 ss.

4. Nuovi scenari di responsabilità medica

Da altra prospettiva è interessante osservare come l'ingresso della tecnologia nelle strutture sanitarie, e in particolare la digitalizzazione della comunicazione medico-paziente, abbia inciso anche sotto il profilo della responsabilità professionale del medico. Va detto, a mo' di premessa, che l'impatto della rivoluzione digitale nel mondo delle professioni intellettuali è notevole, sotto molti e diversi punti di vista: dall'estensione del perimetro e del contenuto dell'obbligazione professionale in ragione dell'avanzamento delle nuove tecnologie, all'affacciarsi di nuovi profili e nuove competenze che la legge o il mercato impone al moderno professionista.

Il professionista, oggi, è chiamato ad affrontare nuovi e più numerosi obblighi[28], nonché ad acquisire competenze un tempo non richieste: basti pensare, su tutte, alle ormai fondamentali e ineludibili competenze informatiche essenziali per lo svolgimento delle quotidiane attività del professionista.

A fronte di un aumento delle pretese e delle aspettative dell'utente[29], sempre più esigente ed avvertito[30], si potrebbe discorrere, parafrasando il passo di un recente saggio,

[28] Obblighi che vanno da quelli di informazione e di trasparenza, a quelli di riservatezza e trattamento dei dati personali; dal dovere di formazione professionale continua, imposto a talune categorie professionali, ad un dovere di "protezione" nei confronti dei destinatari finali del servizio. Del resto la tendenza oggi è di considerare superata la concezione monolitica del rapporto obbligatorio, riconoscendo la presenza di obblighi "altri", quali i cosiddetti "obblighi o doveri di protezione" (*Schutzpflichten*), che, a differenza dell'obbligo principale (di prestazione), sono suscettibili di gravare su ambedue le parti del rapporto – sul debitore e sul creditore – posto che essi si distinguono tanto dagli obblighi positivi di prestazione, quanto dagli obblighi di carattere meramente accessorio. Sull'argomento si possono consultare, C. Castronovo, voce *Obblighi di protezione*, in *Enc. giur. Treccani*, XXI, Roma, 1990, 1 ss.; C. Scognamiglio, *Il danno al patrimonio tra contratto e torto*, in *Resp. civ. prev.*, 2007, 1255 ss.; C.W. Canaris, *Norme di protezione, obblighi del traffico, doveri di protezione*, in *Riv. crit. dir. priv.*, 1983, 793 ss.: «I primi [doveri di prestazione, ndr] sono finalizzati alla realizzazione ed alla promozione dell'interesse alla prestazione, i secondi [doveri di protezione, ndr] alla protezione dei restanti beni della controparte. La peculiarità decisiva dei "doveri di protezione" e, nel contempo, la loro differenza sostanziale con gli "obblighi del traffico", sta nel fatto che la loro violazione determina una responsabilità alla stregua dei principi contrattuali».

[29] L'utente oggi si identifica con la figura del «consumatore» o «contraente debole». La letteratura sul punto è vastissima. Si possono consultare, tra gli altri, V. Roppo, *Protezione del consumatore e teoria delle classi*, in *Pol. dir.*, 1975, 701 ss.; C.M. Mazzoni, *Contro una falsa categoria: i consumatori*, in *Giur. comm.*, I, 1976, 624 ss.; M. Bessone, *Interesse collettivo dei consumatori e regolazione giuridica del mercato. I lineamenti di una politica del diritto*, in *Giur. it.*, IV, 1986, 296 ss.; Id., *«Consumerism» e tutela dei consumatori. I percorsi obbligati dì una politica del diritto*, in *Pol. dir.*, 1987, 615; V. Zeno-Zencovich, voce «Consumatore (tutela del)», in *Enc. giur.*, VIII, Roma, 1988, 1 ss.; V. Buonocore, *Contratti del consumatore e contratti d'impresa*, in *Riv. dir. civ.*, I, 1995, 6 ss.; R. Pardolesi, *Clausole abusive (nei contratti dei consumatori): una direttiva abusata?*, in *Foro it.*, V, 1994, 138 s; G. Benedetti, *Tutela del consumatore e autonomia contrattuale*, *Riv. trim. dir. proc. civ.*, 1998, 21 ss.; N. Irti, *L'ordine giuridico del mercato*, Roma-Bari, 1998, 49 s.; E. Gabrielli - A. Orestano, voce *Contratti del consumatore*, in *Digesto civ.*, 2000, 1 ss.; A.P. Scarso, *Il contraente debole*, Torino, 2006. Più di recente, v. V. Cuffaro, *Nuovi diritti per i consumatori: note a margine del d.lgs. 21 febbraio 2014, n. 21*, in *Corr. giur.*, 2014, 745 ss.; P. Trimarchi, *Il diritto protegge gli ingenui?*, in *Studi in onore di Giovanni Iudica*, Milano, 2014, 1387; A. Fici, *Sulla nozione di "contratto del consumatore"*, in *Riv. dir. priv.*, 2018, 435 ss.

[30] Nell'epoca di una società veloce, liquida e complessa, il comune cittadino, privo di specifiche competenze, è indotto a credere di poter fare a meno dell'intermediario, del mediatore, dell'esperto, del professionista, poiché la rivoluzione digitale ha consentito l'accesso ad una massa enorme di informazioni, permettendo così la realizzazione di esperienze immateriali e l'acquisizione di presunti "saperi".

di una "professionalità aumentata"[31]. Lo si vede con solare evidenza nel campo sanitario, dove il paziente di oggi, informato e navigatore di siti internet, può raccogliere una moltitudine di informazioni, più o meno attendibili, riguardanti la propria malattia e i suoi sintomi; dunque il peso dell'informazione si sposta sul piatto della bilancia del paziente e provoca un insolito capovolgimento nell'agire del medico, costretto ad integrare e correggere informazioni già acquisite, accertandosi anzitutto di cosa sa, o crede di sapere, il malato della sua condizione[32].

In tale scenario l'attività medico-sanitaria è chiamata a conformarsi a standard qualitativi sempre più elevati. La complessità ed evoluzione della scienza medica hanno contribuito al processo di specializzazione della medicina e del medico, e così alla scomposizione della prestazione sanitaria in capo ad una pluralità di soggetti che compongono l'*équipe*[33].

È in tale direzione che si registra una significativa espansione del concetto di diligenza professionale[34]. Maggiori sono le possibilità tecniche offerte dal progresso scientifico e tecnologico nel campo delle professioni intellettuali, più elevato è lo standard di diligenza richiesto al professionista.

Sotto il profilo della diligenza richiesta, si ricava infatti, dall'art. 1176 c.c., c. 2, un concetto "elastico" che va rapportato al singolo caso concreto, anche in relazione all'evoluzione della dotazione tecnologica del singolo professionista in virtù della quale crescono le aspettative del creditore, al punto da segnare il passaggio, in taluni casi, da un'obbligazione di mezzi ad una di risultato[35]. Sicché in definitiva si è indotti ad affer-

---

[31] A. Baricco, *The Game*, Torino, 2018, spec. 80 ss.

[32] Cfr. G. Lonati, *L'ultima cosa bella. Dignità e libertà alla fine della vita*, cit., 66: «Partiamo da quello che sa lei: che cosa ha trovato in internet sulla malattia?».

[33] La relazione medico-paziente costituisce un rapporto obbligatorio «complesso», che si realizza nell'arco di tutte le fasi dell'intervento medico e non si limita all'aspetto strettamente terapeutico della prestazione professionale. La condotta medica è volta alla «protezione» del paziente sin dal primo contatto con il medesimo e in tutte le fasi dell'intervento medico, tra cui quello informativo e diagnostico. Più di recente, l'art. 5 della legge n. 24/2017 (legge Gelli) ha imposto agli esercenti le professioni sanitarie l'osservanza di c.d. linee-guida, oggetto di raccomandazioni specifiche, che facciano capo ad associazioni tecnico-scientifiche delle professioni sanitarie, iscritte in appositi elenchi istituiti con decreto del Ministero della Salute. E, in ogni caso, in mancanza di tali linee-guida, è fatto obbligo ai medici di attenersi «alle buone pratiche clinico-assistenziali» (art. 5 della legge Gelli). L'obbligo del medico di attenersi a quanto stabilito dalle linee guida o dalle pratiche assistenziali ha rilevanza tanto in sede penale, quanto in sede civile, nella valutazione della colpa professionale del medico e nella determinazione del risarcimento del danno (art. 7, c. 3, legge Gelli). Sul punto è di recente intervenuta Cass. pen., sez. un., 21 dicembre 2017, n. 8770, in *Foro it.*, II, 2018, 217; in *Giur. it.*, 2018, 841 (m), con nota di A. Di Majo: «In tema di responsabilità dell'esercente la professione sanitaria, le raccomandazioni contenute nelle linee guida definite e pubblicate ai sensi dell'art. 5 l. 8 marzo 2017, n. 24 - pur rappresentando i parametri precostituiti a cui il giudice deve tendenzialmente attenersi nel valutare l'osservanza degli obblighi di diligenza, prudenza, perizia - non integrano veri e propri precetti cautelari vincolanti, capaci di integrare, in caso di violazione rimproverabile, ipotesi di colpa specifica, data la necessaria elasticità del loro adattamento al caso concreto; ne consegue che, nel caso in cui tali raccomandazioni non siano adeguate rispetto all'obiettivo della migliore cura per lo specifico caso del paziente, l'esercente la professione sanitaria ha il dovere di discostarsene».

[34] Il concetto di diligenza, come espressamente dichiarato nella Relazione (n. 559) al codice civile, «riassume in sé quel complesso di cure e di cautele che ogni debitore deve normalmente impiegare nel soddisfare la propria obbligazione, avuto riguardo alla natura del particolare rapporto ed a tutte le circostanze di fatto che concorrono a determinarlo».

[35] Si pensi all'avanzamento della medicina ed a quelle operazioni medico-chirurgiche diventate nel

mare che «il professionista è sempre meno *magister*, quindi è sempre meno mago, per scimmiottare il filologo, ed è sempre più fornitore di servizi, anche se di alta qualità, per i quali è impegnato al pari di qualsiasi altro debitore»[36].

Ebbene, in tale contesto, la digitalizzazione della comunicazione medico-paziente incide sulla responsabilità professionale del medico, allorché questi, ad esempio, autorizzi il (o anche solo consenta al) proprio paziente di comunicare proprio a mezzo degli strumenti informatici di cui sopra; in tal caso, a mio avviso, egli poi non può ignorare le informazioni ricevute adducendo a sua discolpa l'inadeguatezza o l'irritualità del canale comunicativo impiegato. Una volta provato che il medico abbia effettivamente ricevuto e negligentemente ignorato il contenuto del messaggio (si pensi, in ipotesi, agli esiti di un esame radiografico che richiedano un tempestivo intervento), appare difficile sostenere che il professionista non fosse tenuto a considerare tali informazioni in ragione della pretesa straordinarietà del mezzo di comunicazione usato. Quantomeno egli avrebbe dovuto prontamente invitare il mittente a comunicare attraverso i canali più tradizionali, ed avvisarlo del fatto che mezzi di comunicazione alternativi non potessero garantire un pronto ed attendibile riscontro.

Diversamente, il medico è chiamato a valutare e ponderare tutte le informazioni a lui pervenute, secondo i canoni di diligenza professionale, e così ad attivarsi tempestivamente ogni qual volta risulti necessario invitare il paziente a sottoporsi agli opportuni accertamenti del caso.

A titolo esemplificativo, nella giurisprudenza si registrano vicende di responsabilità professionale connesse alla mancata tempestiva diagnosi di una patologia imputabile alla negligenza del medico che abbia trascurato i segnali di pericolo lanciati dal paziente per telefono[37].

Con riguardo all'"idoneità" del mezzo di comunicazione impiegato dal paziente per comunicare con il proprio medico, occorre poi rammentare che, sul piano probatorio, la giurisprudenza ammette la rilevanza, almeno in astratto, dei mezzi tecnologici più moderni.

Il messaggio WhatsApp o sms, ad esempio, può essere assimilato ad una comunicazione e-mail, ai sensi dell'art. 20, c. 1-*bis*, del d.lgs. 7 marzo 2005, n. 82 (*codice dell'ammini-*

tempo interventi cosiddetti di routine.

[36] M. Franzoni, Dalla colpa grave alla responsabilità professionale, 2ª ed., Torino, 2016, 6.

[37] V. Cass. civ., sez. III, 29 novembre 2010, n. 24143, in *Nuova giur. civ. comm.*, I, 2011, 449, con nota di M. Foglia, *Errata diagnosi del medico, il problema causale e la* chance *perduta.* Sul tema più di recente, Cass. civ., sez. III, 20 agosto 2015, n. 16993, in *Riv. nel diritto*, 2015, 1759: «L'omissione o la tardiva diagnosi di una patologia terminale cagiona al paziente un danno, nonostante l'esito ineluttabile della malattia, con conseguente responsabilità medica dello specialista e necessità di risarcire il danno morale terminale patito agli eredi della vittima, in conseguenza della grave negligenza professionale e del nesso causale che sussiste fra l'esercizio negligente della propria attività e la perdita della chance di procrastinare l'evento infausto e di diminuire il dolore»; Cass. civ., sez. III, 14 giugno 2011, n. 12961, in *Danno e resp.*, 2013, 639, con nota di B. Tassone: «In tema di danno alla persona, conseguente a responsabilità medica, integra l'esistenza di un danno risarcibile l'omissione della diagnosi di un processo morboso terminale, allorché abbia determinato la tardiva esecuzione di un intervento chirurgico, che normalmente sia da praticare per evitare che l'esito definitivo del processo morboso si verifichi prima del suo normale decorso, e risulti inoltre che, per effetto del ritardo, sia andata perduta dal paziente la chance di conservare, durante quel decorso, una migliore qualità della vita nonché la chance di vivere alcune settimane od alcuni mesi in più, rispetto a quelli poi effettivamente vissuti».

strazione digitale), secondo il quale «l'inidoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità».

La giurisprudenza più recente afferma che, in mancanza di contestazione, da parte del destinatario, sul fatto che il messaggio non fosse integro, completo ed adeguatamente leggibile, o che non desse certezza di provenire dalla persona fisica quale mittente, la modalità informatica di comunicazione di una qualsivoglia dichiarazione o volontà può in concreto ritenersi validamente munita del requisito della forma scritta[38].

In ambito penale, ad esempio, è ormai pacifico che i dati informatici già acquisiti dalla memoria del telefono in uso all'indagato (Sms, messaggi WhatsApp, messaggi di posta «scaricati») siano idonei a costituire prove documentali, in quanto non rientranti né nel concetto di corrispondenza, la cui nozione implica un'attività di spedizione dal mittente mediante consegna a terzi per il recapito, né in quello di intercettazione, che postula la captazione di un flusso di comunicazioni in corso[39].

Analogamente, è interessante ricordare che, nella giurisprudenza giuslavoristica, il licenziamento intimato per sms è stato ritenuto validamente munito di forma scritta, qualora non ne sia contestata la provenienza dal mittente[40].

Simili considerazioni potrebbero valere per il telegramma dettato per telefono, riguardo al quale la giurisprudenza non si pone più un problema astratto di esistenza in sé della forma scritta, bensì un problema concreto relativo a come - a fronte di contestazioni svolte dal destinatario - risolvere la questione relativa alla certezza della sua provenienza dal mittente. Ma ogni volta che tali contestazioni non vengono poste, ne discende che la forma scritta esiste.

5. Conclusioni

Le peculiarità dei singoli scenari di cura e la valorizzazione dei concetti di dignità e identità del malato impongono di ripensare all'idea di salute e di medicina, ancor più in un'epoca caratterizzata dalla superiorità della tecnica sull'uomo.

È stato osservato che sullo sfondo dell'interazione medico-paziente, anche nell'ottica dell'acquisizione del consenso informato, campeggia il principio di tutela della dignità della persona e della sua identità. Un valido consenso all'atto medico, anche quando acquisito per ogni singolo atto diagnostico-terapeutico nelle forme previste dalla

[38] In tal senso v. App. Firenze, 5 luglio 2016, in *Argomenti dir. lav.*, 2017, 189, con nota di C. Lazzari; *Riv. it. dir. lav.*, 2017, II, 120, con nota di A. Rota.

[39] Così Cass. pen., sez. V, 21 novembre 2017, n. 1822, in *Foro it.*, 2018, II, 252, con nota di Minafra.

[40] App. Firenze, 5 luglio 2016, cit. In fatto, tale comunicazione — letta prima sul display del telefono e poi stampata come documento da produrre in giudizio — fu intesa dal destinatario come l'effettiva comunicazione di un licenziamento ed in tali termini fu quindi oggetto della relativa impugnazione stragiudiziale. Infatti, il lavoratore non metteva in discussione la legittimazione della persona fisica (i.e. il proprio datore di lavoro) da cui proveniva la manifestazione di volontà. Piuttosto, in giudizio negava l'idoneità in sé del messaggio sms ad integrare il requisito della forma scritta necessario per intimare un recesso efficace.

legge, si può realizzare solo in un più ampio e autentico contesto relazionale, in cui il consenso, inteso come processo relazionale di decisione, si articola in un percorso che coinvolge i sanitari, il malato e i suoi familiari, sviluppandosi nella dimensione umana delle interazioni tra gli attori coinvolti.

Il dialogo talvolta risulta faticoso, ma serve a cambiare prospettiva, a vestire i panni dell'altro – il malato – ed a metterlo nel proprio orizzonte. Il bravo medico, nel tempo della medicina tecnologica, è colui che non sovrappone la sua concezione di vita a quella del paziente, ma sa individuare il limite del suo potere, raggiunto il quale egli si fa garante della dignità del malato, guidandolo, dopo averlo informato, nelle decisioni; e accompagnandolo, quando la morte diventa inevitabile, nell'ultimo tratto della sua esistenza.

Queste, credo, dovrebbero essere le condizioni per una vera consensualità, i presupposti di scelte terapeutiche meditate e consapevoli nel rispetto della persona umana, nella sua unicità. Il compito del giurista è quello di aiutare il medico a mettere a fuoco tali condizioni: ma occorre una lettura operosa della realtà dell'uomo che vive l'esperienza della malattia e della sofferenza[41].

[41] Per spiegare la condizione del malato e della malattia, ho trovato efficace la metafora dell'acquario: M. Foglia, *Nell'acquario. Contributo della medicina narrativa al discorso giuridico sulla relazione di cura*, in *Resp. medica*, 2018, 373 ss.

"*Do Algorithms dream about Electric Sheep?*" Percorsi di studio in tema di discriminazione e processi decisori algoritmici tra le due sponde dell'Atlantico*

Giacomo Capuzzo

Abstract

Questo studio si propone di descrivere il panorama giuridico che relaziona la discriminazione al mondo dell'intelligenza artificiale, con particolare riferimento all'impiego degli algoritmi. L'autore analizza il funzionamento di queste macchine automatiche nell'ambito dei processi decisori di attori privati e pubblici sottolineando i potenziali effetti discriminatori derivanti da tale impiego. Il testo approfondisce i vari aspetti della tutela discriminatoria tra gli ordinamenti multilivello europeo e statunitense approfondendo le discipline normative e la trattazione di alcuni casi pratici per fornire una mappa introduttiva alla tematica.

This study aims at describing the legal framework that relates discrimination to the world of artificial intelligence, with particular reference to the use of algorithms. The author analyzes the operation of these automatic machines within the decision-making processes of private and public actors, emphasizing the potential discriminatory effects resulting from such use. The paper explores the various aspects of discriminatory protection between the European and US multilevel legal systems, deepening the regulatory disciplines and dealing with some practical cases to provide an introductory map to the issue.

Sommario

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

sul trattamento dei dati personali – 2.5 La tutela antidiscriminatoria negli Stati Uniti d'America nel campo dei processi decisori algoritmici – 3. La discriminazione algoritmica in pratica: una serie di casi sostanziali – 4. A mo' di conclusione.

Keywords

intelligenza artificiale - algoritmi - tutela antidiscriminatoria - privacy - controllo sociale

1. Alcuni cenni introduttivi

Il crescente impiego dell'intelligenza artificiale all'interno dei settori produttivi e dell'amministrazione pubblica ha contraddistinto i primi decenni del nuovo secolo. Lo sviluppo tecnologico ha consentito l'utilizzo sempre maggiore di elaboratori elettronici in grado di eseguire compiti di supporto e talvolta in sostituzione dell'attività umana[1].

Un passaggio fondamentale ha riguardato la possibilità di raccogliere e processare masse di dati mediante i quali elaborare informazioni capaci di consentire un funzionamento intelligente da parte delle macchine stesse. Attraverso questo percorso si può concepire un processo decisorio automatico affidato a degli elaboratori che, sulla base dei dati inseriti, consente l'individuazione di una specifica soluzione ad un determinato problema. Queste nuove applicazioni hanno favorito l'introduzione dell'intelligenza artificiale in molti ambiti delle attività produttive e della pubblica amministrazione. In particolare, è aumentato l'impiego di algoritmi, sequenze di istruzioni informatiche ben definite che sono impiegate per risolvere una serie di problemi o per eseguire un determinato calcolo[2].

L'algoritmo è quindi una delle diverse applicazioni dell'intelligenza artificiale e comprende un'ampia gamma di strumenti, che a loro volta influenzano una varietà di operazioni. Si tratta di un tipo di decisione che viene presa miliardi di volte all'anno in

[1] In tema di nuove tecnologie in generale ed intelligenza artificiale, a carattere introduttivo, si veda S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; F. Pasquale, *The black Box Society: The Secret algorithms that Control Money And Information*, Cambridge, 2015, 5 ss.; S. Barocas - A. D. Selbst*, Big Data's Disparate Impact*, in 104 *Calif. L. Rev.* 671, 674 N.10, 2016; I. Ajunwa, *Algorithms At Work: Productivity Monitoring Platforms And Wearable Technology As The New Data-Centric Research Agenda For Employment And Labor Law*, in 63 *St. Louis U. L.J.* 2019; I. Ajunwa, *Genetic Testing Meets Big Data: Tort And Contract Law issues*, in 75 *Ohio St. L.J.* 1225, 2014; D. K. Citron - F. Pasquale, *The Scored Society: Due Process For Automated Predictions,* in 89 *Wash. L. Rev.* 1, 2014; K. Crawford - J. Schultz, *Big Data And Due Process: Toward A Framework To Redress Predictive Privacy Harms*, in 55 *B.C. L. Rev.* 93, 2014; L. Edwards-M. Veale, *Slave To The Algorithm? Why A 'Right to an explanation' Is Probably Not The Remedy You Are Looking For,* in 16 *Duke L. & Tech. Rev.* 18, 2017; G. Resta-V. Zeno Zencovich (a cura di), *La protezione transnazionale dei dati personali,* Roma, 2016; G. Resta, *Diritti esclusivi e nuovi beni immateriali*, Torino, 2011; G. Pitruzzella, *Big Data, Competition and Privacy: A Look from the Antitrust Perspective*, in *Concorrenza e Mercato*, 2016, 15 ss.; F. Pizzetti, *Privacy e diritto europeo nella protezione dei dati personali*, Torino, 2016; G. Pascuzzi*, Il diritto nell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2002. A. D. Selbst-S. Barocas, *The Intuitive Appeal Of Explainable Machines*, in 87 *Fordham L. Rev.* 2018.

[2] S. Barocas-S. Hood-M. Ziewitz, *Governing Algorithms: A Provocation Piece, Governing Algorithms*, 29 Mar. 29, 2013.

svariati settori come quello creditizio, concorsuale o diagnostico in ambito medico[3]. Questa tipologia di intelligenze artificiali è sviluppata utilizzando metodi di apprendimento automatico (*machine learning*). Si tratta di tipologie di algoritmi che costruiscono funzioni di previsione sulla base di una serie di dati allo scopo di realizzare tali predizioni; una volta consolidata tale funzione, l'algoritmo riceve un particolare "input" (come le caratteristiche di un candidato ad una particolare posizione lavorativa) e predice alcuni risultati (come la sua performance in specifici ambiti)[4].

L'utilità di queste macchine è tale che sono molteplici ormai gli ambiti in cui viene sfruttata e le sue implicazioni sociali sono del tutto evidenti. Molte delle decisioni che sono prese all'interno della società si basano o sono influenzate dagli esiti di queste elaborazioni algoritmiche. Per tali ragioni, i giuristi hanno cominciato ad interessarsi alle ripercussioni nel mondo giuridico di queste nuove tecnologie[5].

Il loro impiego è rilevante per il diritto[6], sia perché le regole dell'ordinamento si estendono al funzionamento dell'algoritmo quando è impiegato in relazione a particolari attività umane, sia perché il diritto stesso ha cominciato ad impiegare algoritmi nell'ambito della sua applicazione, come ad esempio nei contratti di appalto o nel calcolo dell'assegno di mantenimento. In particolare i principali ambiti di interesse hanno riguardato finora la tutela della privacy e il trattamento dei dati personali e in ambito di protezione antidiscriminatoria. Quest'ultimo aspetto ha attirato di recente le attenzioni degli studiosi perché l'impiego degli algoritmi nel contesto di diversi processi decisionali, sia nel comparto privato, che in quello pubblico, li ha spinti a chiedersi se non vi potessero essere possibili ambiti di discriminazione connessi con questa tipologia di intelligenze artificiali[7].

Tali rilievi si fondano su due serie di considerazioni che hanno entrambe origine nei

---

[3] A. Mantelero, *I Big Data nel quadro della disciplina europea della tutela dei dati personali*, in *Il Corriere giuridico - Speciali Digitali 2018*, 2018, 46 ss.; V. Morabito, *Big Data and Analytics. Strategic and Organizational Impacts,* New York, 2015, 23 ss; P. T. Kim, *Auditing Algorithms for Discrimination*, in 166 *U. Pa. L. Rev. Online* 189, 2017; Id., *Data-Driven Discrimination At Work,* in 58 *Wm. & Mary L. Rev.* 857, 2017; P. Kim-S. Scott, *Discrimination In Online Employment Recruiting*, in 63 *St. Louis U. L.J.*, 2019; C. A. Sullivan, *Employing*, 2018 (Seton Hall Public Law Research Paper); J. A. Kroll et al., *Accountable Algorithms*, in 165 *U. Pa. L. Rev.* 633, 2017.

[4] C. Angelopoulos, et al., *Study of fundamental rights limitations for online enforcement through self regulation*, report IViR Institute for Information Law, University of Amsterdam, 2016; J. Angwin et al., *Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks*, in *ProPublica*, 23 maggio 2016 J. R. Bambauer-T. Zarsky, *The algorithm game*, in *Notre Dame Law Review,* 2018.

[5] R. Avraham, *Discrimination and Insurance*, in K. Lippert-Rasmussen (a cura di), *The Routledge handbook of the ethics of discrimination*, New York, 2017; K. Charles-J. Guryan, *Prejudice and wages: An empirical assessment of Becker's the Economics of Discrimination*, in *J. Polit. Econ.,* 116, 2008, 773 ; M. Turner et al., *All other things being equal: A paired testing study of mortgage lending institutions–final report*, Tech. Rep., US Department of Housing and Urban Development Office of Policy Development and Research, Washington, 2002. M. Bertrand-S. Mullainathan, *Are Emily and Greg more employable than Lakisha and Jamal? A field experiment on labor market discrimination, in Am. Econ. Rev.* 94, 2004, 991 ; V. Zeno-Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *questa Rivista,* 2, 2018, 5-6.

[6] Su questo punto il rimando è a S. Rodotà, *Elaboratori elettronici e controllo sociale*, cit.; Id. *Tecnologie e diritti*, Bologna, 1995.

[7] S. Barocas-A. Selbst, *Big data's disparate impact*, in *Calif. Law Rev.* 104, 2016, 671 ss. S. Bornstein, *Antidiscriminatory algorithms*, in *Ala. Law Rev*. 70, 2018, 519 ss.; J. Kleinberg-J. Ludwig-S. Mullainathan-C. Sunstein, *Discrimination in the age of algorithms*, in *J. Legal Anal.* 10, 2018, 113 ss.; L. Sweeney, *Discrimination in online ad delivery*, in *Queue*, 2013, 10 ss..

discorsi e nelle elaborazioni che hanno accompagnato l'impiego di questi strumenti, secondo la prima, sebbene gli algoritmi consentano di ridurre la discrezionalità legata ai processi decisori gestiti dagli esseri umani, si ritiene altamente probabile che gli stessi riproducano le disuguaglianze già esistenti. Rispetto alla seconda linea argomentativa, l'idea che i calcoli algoritmici siano percepiti come neutrali, nella convinzione che la tecnologia sia sempre un aiuto, semplifichi le cose e che quindi il funzionamento di queste macchine ad apprendimento automatico non possa essere ricostruito o alterato dall'esterno (*black box*), rendendo di fatto il settore immune alla regolamentazione di natura giuridica[8].

2. L'antidiscriminazione alla prova dei processi decisori algoritmici: l'approccio *ex post*

Se le questioni principali relative all'utilizzo degli algoritmi risultano condivise dalla dottrina prevalente negli ordinamenti occidentali, per quanto concerne le soluzioni, le opinioni sono piuttosto diverse e non solo per la presenza di normative e tutele differenti tra le due sponde dell'Atlantico in tema di discriminazioni. In particolare, sono stati evidenziati due diversi approcci alla protezione antidiscriminatoria nell'ambito dei processi decisori algoritmici. Il primo preferisce una tutela *ex post* attraverso l'estensione dell'attuale regolamentazione in materia antidiscriminatoria anche ai casi relativi all'impiego degli algoritmi[9]. Tale approccio punta ad informare la creazione dell'algoritmo ai principi di trasparenza e di responsabilità in modo da prevenire la possibilità di produrre un esito discriminatorio[10]. In questo modo è possibile operare una verifica di un particolare algoritmo, attraverso l'accesso alle informazioni che lo riguardano e agli schemi della sua elaborazione, identificare difetti, errori intenzionali e forse scovare risultati indesiderati e possibilmente non intenzionali come la discriminazione. Questo approccio consente quindi uno stretto controllo di tutte le componenti dell'algoritmo allo scopo di escludere ogni possibile risultanza che possa condurre a discriminazioni o ad altri esiti non in linea con le normative vigenti nel

[8] Su questo punto si veda F. Pasquale, *The Black Box Society: The Secret Algorithms that control Money and Information,* cit., 34-35; I. Bogost, *The Cathedral of Computation,* cit; K. Fink , *Opening the government's black boxes: freedom of information and algorithmic accountability*, in *Information, Communication & Society*, 21(10), 2018, 1453.

[9] Sui rischi e le problematiche sollevate dall'impiego massivo dell'intelligenza artificiale, A. G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York, 2017; A. Danna-O.H. Gandy Jr., *All that glitters is not gold: Digging beneath the surface of data mining*, in *J Bus Ethics*, 40(4), 2002, 373; J. Burrell, *How the machine 'thinks': understanding opacity in machine learning algorithms*, in *Big Data & Society* 3(1), 2016,1 ss.; D. M. Boyd-K. Crawford, *Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon*, in *Information, Communication & Society*, 15(5), 2012, 662.

[10] T. Khaitan, *A theory of discrimination law*, Oxford, 2015; P. Hacker, *Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law Common Market Law Review*, 4, 55, 2018, 1143 ss.; M. Hardt, *How big data is unfair. Understanding sources of unfairness in data driven decision making*, 2014; R. Gellert-K.De Vries-P. De Hert-S. Gutwirth, *A comparative analysis of anti-discrimination and data protection legislations,* in *Discrimination and privacy in the information society,* Berlin, Heidelberg, 2013, 61-89.

campo di applicazione dell'algoritmo[11]. Una simile condizione difficilmente può verificarsi con rispetto agli algoritmi, se si fa riferimento, ad esempio, a quei casi che hanno destato maggiori perplessità nel campo della tutela antidiscriminatoria.
La principale problematica dell'approccio *ex post* per regolare l'automazione risiede nel fatto che anche con tutte le informazioni relative ad uno specifico algoritmo, elaborare una mappa di tutte le possibili variabili intervenute all'interno del processo decisorio è molto spesso alquanto complicato[12]. Al contrario una protezione *ex ante* che tiene conto dell'elaborazione dell'algoritmo attraverso le procedure tecniche impiegate per realizzarlo e predispone una regolamentazione giuridica puntuale rispetto alle casistiche previste dal funzionamento dei processi decisori algoritmici[13]. proibire quei risultati che possono comportare discriminazioni, vietare gli usi inappropriati e fino a richiedere che il software sia costruito secondo determinate specifiche che possono essere testate o controllate[14].

2.1 *segue* L'approccio *ex ante*

Sulla base di quanto appena esposto, è necessario quindi soffermarsi sugli interrogativi connessi con un approccio *ex ante* alla protezione antidiscriminatoria rispetto all'impiego degli algoritmi. I contorni di una tutela *ex post* come quella fondata sull'applicazione dei principi neoliberali di trasparenza e responsabilità sono stati delineati nel precedente paragrafo, svelando una concezione che, sebbene consenta una tutela generale per tutti i casi nei quali emerga una decisione al termine di un processo decisorio algoritmico che possa essere considerata discriminatoria, rimane su di un piano meramente formale per la difficoltà di mappare il funzionamento dell'algoritmo e di reperire prove effettive che possano attribuire il risultato in questione ad uno o più responsabili[15].
L'approccio *ex ante* si basa invece su un'opera di classificazione e analisi di questi sistemi automatici per comprendere la tipologia di danno che possono comportare, le soluzioni che possono essere prodotte e gli impieghi consentiti di questi software. Per

[11] Il passaggio si può ritrovare approfondito in P. T. Kim, *Data-Driven Discrimination at Work*, cit., 857; D. J. Weitzner et al., *Information Accountability*, cit., 86.

[12] Per l'argomento in generale, si veda, M. Kaminski, *Binary governance: A two-part approach to accountable algorithms* (2018), in 92 *S. Calif. L. Rev.* 2019. Per gli esempi, A. Datta et al., *Discrimination in online advertising: A multidisciplinary inquiry* (Conference on Fairness, Accountability and Transparency 2018) 20; A. Datta-M.C. Tschantz, *Automated experiments on ad privacy settings*, in 1 *Proceedings on Privacy Enhancing Technologies*, 2015, 92.

[13] Su di un approccio all'antidiscriminazione che si fondi su alcuni principi generali si veda J.H. Gerards, *Discrimination grounds*, in M. Bell-D. Schiek (a cura di), *Ius commune case books for a common law of Europe – Non-discrimination*, Oxford, 2007, 33 ss.. Federal Trade Commission, *Big data: A tool for inclusion or exclusion? Understanding the issues* (Gennaio 2016); C. Dwork et al., *Fairness through awareness*, in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference ACM*, 2012, 214.

[14] Su questi punti programmatici si veda European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, Marzo 2018.

[15] Sul punto si richiama la trattazione di D. R. Desai-JA. Kroll, *Trust but Verify: A guide to Algorithms and the Law*, cit., 11 ss.

fare ciò è però necessario comprendere lo sviluppo di tali processi decisori, le componenti degli stessi, in quale modo questi sistemi algoritmici riescano a discriminare e come questo possa essere rilevato su di un piano strettamente giuridico[16].

In questo senso, si può iniziare ad approfondire questi temi specificando come, nonostante le persone spesso si riferiscano impropriamente a qualsiasi processo che rielabora dati e produce una previsione come ad un "algoritmo", è importante notare che ci sono effettivamente due processi algoritmici separati al lavoro nelle applicazioni di *screening* del tipo che stiamo considerando: 1) L'algoritmo di screening (o *screener*) prende semplicemente le caratteristiche di un individuo (come un candidato di lavoro) e restituisce una previsione del risultato di questo individuo. Questa previsione quindi informa una decisione. 2) L'algoritmo di formazione (o *trainer*) è ciò che produce l'algoritmo di screening[17].

La costruzione di questo secondo algoritmo implica (tra le altre cose) l'assemblaggio di istanze passate da utilizzare come dati di addestramento, la definizione del risultato da prevedere e la scelta di predittori candidati da considerare. L'algoritmo di screening è solo il risultato meccanico dell'applicazione dell'algoritmo di addestramento su un insieme di dati di addestramento. Quindi, mentre il primo può produrre decisioni distorte, il momento in cui si genera il trattamento discriminatorio è spesso la fase di addestramento che coinvolge il secondo[18].

2.2 Il potenziale discriminatorio degli algoritmi: una guida pratica

ll processo decisionale guidato dall'intelligenza artificiale può portare alla discriminazione in diversi modi. In un articolo fondamentale, Barocas e Selbst distinguono cinque modi in cui il processo decisionale algoritmico può portare alla discriminazione. I problemi riguardano (I) come vengono definite la *target variable* e le *class labels*; (II) l'etichettatura dei dati di addestramento; (III) la raccolta dei dati di addestramento; (IV) la selezione degli indicatori; (V) i *proxies* ed infine (VI) l'impiego degli algoritmi per fini discriminatori in modo volontario[19].

[16] S. Wachter, *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, in 34 *Computer Law & Security Review*, 3, 2018, 436 ss.; A.D.Selbst-S. Barocas, *The intuitive appeal of explainable machines*, in *Fordham Law Review*, 86, 2018; R. Swedloff , *Risk classification's Big Data (r) evolution*, in 21 *Connecticut Insurance Law Journal*, 2014, 339; A. Moretti, *Algoritmi e diritti fondamentali della persona. Il contributo del regolamento (UE) 2016/679* in *Dir. Inf.,* 4-5, 2018, 799 ss..

[17] Il funzionamento dell'algoritmo come procedura in due fasi è ben spiegata in: J. Kleinberg-J. Ludwig-S. Mullainathan-C. Sunstein, *Algorithms as discrimination detectors*, in *Proceedings of the National Academy of Sciences of the United States of America*, 28 luglio 2020.

[18] *Ibid.*

[19] La trattazione delle diverse ipotesi di distorsione discriminatoria del percorso decisorio algoritmico sono delineate in S. Barocas-A.D. Selbst, *Big Data's disparate impact*' cit., 671. Le stesse ipotesi sono riprese in F. Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making*, (Consiglio d'Europa) Strasburgo, 2018, 10 ss.

I) la definizione di target variable e class labels.

Come si è visto in precedenza l'algoritmo di screening lavora sulla base dell'algoritmo di addestramento, entrambi cercano correlazioni tra gruppi di dati, il secondo per fornire dati al primo, il primo per elaborare la soluzione richiesta. Ad esempio, quando un'azienda sviluppa un filtro antispam, l'algoritmo alla base viene allenato attraverso l'inserimento di una serie di messaggi di posta elettronica che sono etichettati dai programmatori come "spam" e "non spam". I messaggi etichettati sono i dati di addestramento[20].

L'algoritmo rileva quali caratteristiche dei messaggi sono correlate all'essere etichettati come spam, l'insieme di queste correlazioni individuate è spesso chiamato "modello predittivo". L'algoritmo viene addestrato a studiare i dati inseriti per capire quali caratteristiche possono essere prese in considerazione per ottenere i risultati richiesti, che vengono definiti come *target variable*[21]. Se la *target variable* definisce ciò che gli operatori stanno cercando, le *class labels* dividono in categorie mutualmente escludibili i risultati richiesti, nell'esempio riportato in precedenza del filtro spam, le persone concordano grosso modo sulle etichette delle classi: quali messaggi sono spam o meno. In altre situazioni, è meno ovvio quali dovrebbero essere le variabili di destinazione[22].

Questo punto fa riferimento ad uno degli aspetti più controversi relativi all'impiego degli algoritmi nonché una delle maggiori cause di trattamenti discriminatori attraverso processi decisionali algoritmici. Chiunque desideri servirsi di un algoritmo allo scopo di predire una soluzione ad una particolare questione, necessita di semplificare il quadro degli attributi ai quali vuole fare attenzione per consentire alla macchina di elaborarli. In altre parole, gli operatori, anche di fronte a dati non discriminatori e correttamente campionati, dovranno procedere ad un'attività interpretativa degli stessi per consentire il loro utilizzo da parte dell'algoritmo[23].

Si prenda, ad esempio, il caso di un'azienda che sia alla ricerca di una/o candidata/o per ricoprire una posizione al suo interno. L'idea è quindi quella di assumere un soggetto modello e per farlo sarà necessario indicarne le qualità: L'azienda potrebbe scegliere "essere raramente in ritardo" come etichetta di classe per valutare se un dipendente è considerato positivamente per l'assunzione. In questo caso i soggetti con redditi più bassi, che solitamente vivono più lontano dal luogo di lavoro, si troverebbero in una posizione di svantaggio, anche se superano gli altri dipendenti sotto altri aspetti[24].

II) e III) etichettatura (labelling) dei dati di addestramento e (III) raccolta dei dati di addestramento

Queste due operazioni si riferiscono a due tipologie di casi piuttosto simili, la discriminazione deriverebbe in queste ipotesi dai passaggi relativi al trattamento dei dati di

[20] F. Zuiderveen Borgesius, *Discrimination, artificial intelligence and algorithmic decision-making*, cit.

[21] P. Dourish, *Algorithms and their others: Algorithmic culture in context* in *Big Data & Society*, 3(2), 2016; F. Zuiderveen Borgesius, *Discrimination, artificial intelligence and algorithmic decision-making*, cit. C. O'Neil, *Weapons of math destruction: How big data increases inequality and threatens democracy*, cit.

[22] S. Barocas-A.D. Selbst, *Big Data's disparate impact*, cit., 678.

[23] Ivi, 679.

[24] F. Zuiderveen Borgesius, Ivi, 11.

addestramento dell'algoritmo[25].

Secondo il punto (II), i dati risultano discriminatori non perché introducano nuovi elementi o correlazioni che portino ad un simile risultato, ma perché riproducano un comportamento discriminatorio già presente nella società. L'esempio classico in questo caso è quello di una azienda sanitaria inglese che di fronte ad un numero rilevante di candidati per alcune posizioni nella sua struttura decide di utilizzare un programma per velocizzare le procedure di selezione. Il programma viene addestrato utilizzando i dati provenienti dalle precedenti assunzioni[26].

Il risultato è stato che il programma discriminava nei confronti di alcune categorie sociali come le donne e la popolazione non autoctona. In questo caso non è stato introdotto alcun elemento discriminante, semplicemente nelle precedenti procedure qualcuno aveva sistematicamente discriminato quelle particolari categorie sociali, di conseguenza i dati utilizzati per l'addestramento dell'algoritmo erano già di partenza alterati[27].

Al punto (III) invece si fa riferimento al momento precedente a quello appena trattato, al passaggio relativo al campionamento dei dati da utilizzare nell'addestramento dell'algoritmo[28]. Un esempio utile per questo caso riguarda l'app *Street Bump*, un'app che utilizza le informazioni GPS degli utenti per segnalare alle amministrazioni pubbliche quali sono le strade che devono ricevere manutenzione. In questo caso il campionamento risultava distorto dal fatto che le segnalazioni avvenivano per le strade dove il numero di smartphone era maggiore, perciò le strade dei quartieri più abbienti ricevevano maggiore assistenza rispetto a quelle di quelli meno abbienti, dove la percentuale di telefoni di nuova generazione era inferiore[29].

IV) la selezione degli indicatori

Questa operazione riprende alcuni aspetti del punto (II) sulla creazione delle *class labels*, classificazioni attraverso le quali i dati vengono trattati per consentire alla macchina di processarli, talvolta questo processo può essere troppo costoso o risultare troppo lungo, per questo motivo si scelgono delle particolari caratteristiche che fungono da indicatori per l'algoritmo, ad esempio un particolare tipo di educazione o qualche corso specialistico. Tali scelte però possono tradursi in comportamenti discriminanti nei confronti di alcune categorie sociali, se si addestra l'algoritmo a preferire candidati da università private particolarmente costose, automaticamente verranno esclusi gli individui meno abbienti e appartenenti alle minoranze che statisticamente sono meno presenti all'interno di quel tipo di istituti educativi[30].

---

25 S. Barocas - A.D. Selbst, Ivi, 680-1; F. Zuiderveen Borgesius, *Ibid.*

26 L'esempio è ampiamente illustrato in S. Lowry - G. Macpherson, *A blot on the profession*, in *Br Med J*, 296, 1988, 657.

27 F. Zuiderveen Borgesius, *Discrimination, artificial intelligence and algorithmic decision-making,* cit., 12.

28 S. Barocas-A.D. Selbst, *Big Data's disparate impact*, cit., 685; D. Robinson-L. Koepke. *Stuck in a pattern,* 2016.

29 Federal Trade Commission, *Big data: A tool for inclusion or exclusion? Understanding the issues*, cit, 27. Per un approfondimento su temi delle politiche di sorveglianza al tempo dell'AI, si veda A.G. Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*, New York, 2017.

30 S. Barocas-A.D. Selbst, Ivi, 689.

V) Proxies

Questo punto riguarda i cosiddetti *proxies*, quei dati che sono stati campionati per essere utilizzati come addestramento per l'algoritmo, ma che sono indirettamente collegati a particolari categorie sociali e possono quindi comportare un comportamento discriminatorio da parte della macchina. I dati sono, in questo caso, perfettamente neutrali e non comportano come al punto precedente una scelta a monte da parte degli operatori, si tratta di dati che possono ricollegarsi a determinate situazioni e quindi sono denominati *proxies*, perché il risultato discriminatorio non si determina per effetto dei dati immessi nella macchina, ma le caratteristiche ad essi ricollegate[31].

VI) discriminazione algoritmica volontaria

Infine l'ultimo caso contempla l'ipotesi più diretta nella quale gli operatori abbiano un positivo intento discriminatorio alla base dell'impiego dell'algoritmo, in questi casi di solito si servono di *proxies* ovvero di campionature di dati non corrette per consentire gli esiti discriminatori che si vogliono ottenere[32].

Il quadro che si presenta è piuttosto complicato, la tipologia di funzionamento dell'algoritmo e la complessità del processo decisorio che lo coinvolge complica non poco la regolamentazione giuridica dell'utilizzo di questo tipo di software. In questo senso, appare difficile seguire un approccio *ex post* sul tema perché l'utilizzo di principi generali come quelli esposti in precedenza non consentirebbe una tutela efficace nei diversi tipi di casi appena trattati[33].

2.3 La tutela antidiscriminatoria multilivello

La normativa in materia antidiscriminatoria, nei diversi ordinamenti occidentali, si serve di strumenti diversi in particolare nei sistemi giuridici che si prenderanno in considerazione: quello statunitense e quello europeo. In entrambi questi contesti si parla di tutele multilivello delle situazioni giuridiche soggettive che si integrano nella protezione di taluni interessi come quelli relativi all'eguaglianza sostanziale degli individui. Nello specifico a livello europeo si possono distinguere due diverse fonti del diritto, da una parte c'è la Convezione Europea dei Diritti dell'Uomo e dall'altra la Carta dei diritti fondamentali, la direttiva in tema di antidiscriminazione e il regolamento GDPR[34]. La convenzione disciplina la tutela antidiscriminatoria all'art. 14 della Convezione, che tutela in via generale il godimento dei diritti senza discriminazioni di sesso, razza,

[31] Ivi, 692.

[32] Sulla discrimazione intenzionale si veda P. T. Kim, *Data-driven discrimination at work*, cit., 857 J. Bryson, *Three very different sources of bias in AI, and how to fix them,* in *Adventures in NI*, 13 July 2017; B. Friedman-H. Nissenbaum, *Bias in computer systems,* in *ACM Transactions on Information Systems* (TOIS), 14(3), 1996, 330.

[33] J. A. Kroll et al., *Accountable algorithms*, in 165 *University of Pennsylvania Law Review*, 2016, 633 ss.

[34] P. Hacker, *Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law*, 55 *Common Market Law Review*, 4, 2018 1143 ss.; N. Helberger-F. Zuiderveen Borgesius-A. Reyna, *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, in *Common Market Law Review*, 54, 2017, 1427 ss.

colore, la lingua, la religione, le opinioni politiche o quelle di altro genere, l'origine nazionale o sociale, l'appartenenza a una minoranza nazionale, la ricchezza, la nascita od ogni altra condizione. Tale disposizione è ulteriormente rafforzata dalla previsione del protocollo 12 alla Convezione che riafferma una tutela omnicomprensiva in ambito antidiscriminatorio, oltre l'elenco contenuto all'art. 14[35].

La giurisprudenza della Corte Edu si è successivamente assunta il compito di definire le due tipologie principali di discriminazione, quella diretta che fonda la differenza di trattamento in analoghe o similari situazioni basata su caratteristiche identificabili. Al contrario la discriminazione indiretta si pone in essere attraverso un'azione che è all'apparenza neutrale, ma si risolve in un atto discriminatorio nei confronti di una particolare categoria sociale. Uno studio delle sentenze della Corte sul tema ha evidenziato come la regolamentazione a tutela della discriminazione indiretta non sia lineare come nel caso di quella diretta[36].

Una disciplina molto simile è quella prevista dall'ordinamento UE, la Carta fondamentale di Nizza prevede una disciplina che riprende quella della CEDU, all'art. 21, c. 1 si legge «é vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale»[37].

Tale prescrizione è stata successivamente positivizzata anche in una serie di direttive a partire dalla n. 43 del 2000. Il regime disposto è sostanzialmente speculare a quello instaurato dalla CEDU; anche in questo caso viene delineata una discriminazione diretta di semplice interpretazione e una indiretta, che si distingue per una disciplina maggiormente discrezionale[38].

La normativa predispone, come si è visto in precedenza rispetto alla giurisprudenza della Corte Edu, la possibilità di liberarsi da parte del convenuto dimostrando che la presunta condotta discriminatoria è avvenuta allo scopo di ottenere un risultato legittimo e che gli strumenti utilizzati per raggiungere tale obiettivo sono necessari e proporzionati; il principio di proporzionalità è impiegato anche nella legislazione EU come strumento per contemperare la tutela antidiscriminatoria con altri interessi[39].

---

[35] Sono diversi i trattati e le convezioni che predispongono una tutela antidiscrimatoria, la Dichiarazione universale dei Diritti d'uomo dell'ONU all'art. 7, la Convezione Europea dei diritti dell'uomo all'art. 14 e al protocollo 12 che non è ancora stato ratificato da tutti i membri, la Carta fondamentale dei diritti dell'Unione Europea all'art. 21 che verrà trattato in questo paragrafo e l'art. 26 della Convenzione Internazionale dei diritti civili e politici all'art. 26.

[36] Su questo punto nella giurisprudenza della Corte Edu si vedano le sentenze, *Biao v. Denmark* (Grand Chamber), ric. 38590/10 (2016), § 89; *D.H. and Others v. Czech Republic*, ric. 57325/00 (2007), §§ 187-188.

[37] Carta fondamentale dei diritti dell'Unione Europea, art. 21, 2002.

[38] La distinzione è rinvenibile nella normativa europea in tema di antidisciminazione, la 2000/43/CE che attua la parità di trattamento tra gli individui indipendemente dalla razza e dall'origine etnica, la 2000/78/CE che stabilisce una disciplina in materia di parità di trattamento in materia di occupazione, la 2004/113/CE che disciplina la parità di trattamento nell'ambito dell'accesso a beni e servizi e la 2006/54/CE che regola le pari opportunità e la parità di trattamento tra uomini e donne in materia di occupazione e impiego.

[39] Su questa eccezione si veda l'art. 2, par. 2, lett. *b)*, della direttiva 2000/43/EC: «…a meno che

2.4 La discriminazione algoritmica attraverso la normativa sul trattamento dei dati personali

Nel contesto dell'Intelligenza artificiale, una regolamentazione che può rivelarsi particolarmente utile nell'ambito dell'ordinamento UE al trattamento dei dati personali. In questo campo, la tutela approntata è meno legata a principi generali e più imperniata su singole regole che disciplinano in modo chiaro la protezione accordata dal diritto alla privacy. La normativa promossa in ambito europeo sul tema enuclea alcuni principi come la trasparenza, l'integrità, la responsabilità e la confidenzialità, ma fonda la propria disciplina su prescrizioni che regolano ogni passaggio della gestione dei dati personali: dalla raccolta all'archiviazione, dallo scopo al controllo del trattamento[40].
Il regolamento adottato dall'UE in questo campo, il *General Data Protection Regulation* offre una serie di disposizioni che vanno proprio in questa direzione, stabilendo che le autorità garanti dei Paesi membri possono richiedere informazioni e l'accesso al sistema di elaborazione dei dati ai responsabili del trattamento, possono accedere ai luoghi fisici dove avviene la gestione dei dati e condurre audit su un particolare utilizzo di intelligenze artificiali[41]. In tema di processi decisori algoritmici, il GDPR ha predisposto una serie di regole a cominciare dall'art. 22, che si occupa di quelle decisioni prese con il solo ausilio degli algoritmi e per il quale: *«The data subject shall have the right not to be subject to a decision based solely on automated processing including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her»* (c.1)[42].
Il diniego di prestazioni assistenziali o pensionistiche, ovvero una pronuncia di un organo giurisprudenziale o di una pubblica amministrazione che fondino la propria decisione esclusivamente su di un processo algoritmico fanno nascere in capo ai soggetti coinvolti un diritto a ricorrere contro la stessa. Per la trattazione in oggetto è interessante notare come questa tutela si applica anche nei casi di *profiling*[43].

---

tale disposizione, criterio o prassi siano oggettivamente giustificati da una finalità legittima e i mezzi impiegati per il suo conseguimento siano appropriati e necessari.» che è ripreso specularmente nella sentenza della Corte Edu *Biao v. Denmark* cit., § 91-2.

[40] Sulla normativa dell'UE in tema di privacy con particolare riferimento all'intelligenza artificiale e ai Big Data si veda European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, Marzo 2014; G. Buttarelli, *Towards a New Digital Ethics: Data, Dignity and Technology, Speech before the Institute of International and European Affairs*, Dublino, 2015, 1-4; F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione,* cit.

[41] Sulla relazione tra GDPR e tutela antidiscriminatoria, si veda W. Schreurs-M. Hildebrandt-E Kindt-M. Vanfleteren, *Cogitas, ergo sum. The role of data protection law and non-discrimination law in group profiling in the private sector*' in M. Hildebrandt-S. Gutwirth, (a cura di) *Profiling the European citizen*, Heidelberg, Berlino, 2008; P. Hacker, *Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law*, cit., 1143 ss.; F. Zuiderveen Borgesius, *Discrimination, artificial intelligence and algorithmic decision-making*, cit., 21.

[42] Art. 21 GDPR. In questo ambito si rimanda a I.. Mendoza-L. A. Bygrave *The right not to be subject to automated decisions based on profiling*, University of Oslo, in Research paper no. 20 (2017). Sia sul tema in generale, che con specifico riferimento alla discriminazione in tema di online *pricing*, si veda F. Zuiderveen Borgesius - J. Poort, *Online price discrimination and EU data privacy law*, in *Journal of Consumer Policy*, 2017,1 ss.

[43] L'art. 4, par. 4, del GDPR definisce il profiling come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali

L'art. 22 stabilisce delle eccezioni alla regola enunciata al c.1, il divieto non si applica se la decisione automatizzata (i) è basata sul consenso esplicito dell'interessato; (ii) è necessaria per un contratto tra la persona fisica e il titolare del trattamento; o (iii) questo è autorizzato dalla legge. I primi due casi però fanno scattare l'applicazione di un'altra disciplina per la quale il responsabile del trattamento è tenuto ad attuare misure adeguate per salvaguardare i diritti, le libertà e i legittimi interessi dell'interessato e almeno il diritto di ottenere l'intervento umano da parte del responsabile del trattamento e per contestare la decisione (art. 22, par. 3, GDPR)[44].

Questa previsione diviene estremamente interessante perché consente la possibilità di ricorrere nei confronti di decisioni espresse esclusivamente attraverso procedure algoritmiche che possono aver compresso i diritti dei soggetti coinvolti dalle stesse. In alcuni casi si è parlato di un *algorithmic due process* che tutela alcune libertà e diritti fondamentali degli individui nei confronti di tali processi decisionali[45].

Rimane ancora un argomento di discussione se queste obbligazioni diano vita ad un diritto di spiegazione in capo ai soggetti coinvolti dalla decisione in virtù del quale sia possibile richiedere un chiarimento rispetto a qualsiasi risultato individuato con l'ausilio dell'intelligenza artificiale. Questo obbligherebbe gli operatori a porre in essere quei passaggi richiesti dalla trasparenza informatica e consentirebbe ai soggetti coinvolti di avere informazioni tecniche attraverso le quali cercare di comprendere i passaggi del processo decisorio, come previsto dall' art. 9 *Data Protection Convention* 108 del Consiglio d'Europa del 2018. In generale però è spesso difficile spiegare la logica alla base di una decisione, come un algoritmo, analizzando grandi quantità di dati, arriva a quella decisione. In alcuni casi, non è chiaro quanto una spiegazione potrebbe aiutare i soggetti interessati, soprattutto nella misura in cui pone l'onere di comprendere la stessa decisione e la sua adeguatezza in capo a loro[46].

La normativa in tema di protezione dei dati personali offre una tutela più articolata nei confronti delle decisioni che coinvolgono l'intelligenza artificiale, la trattazione tende a reggersi non solo su principi generali, che sono più difficili da applicare alle diverse casistiche tecniche che possono verificarsi all'interno di un processo decisorio algoritmico, ma anche sul lavoro svolto dalle autorità garanti che possono sviluppare

relativi ad una persona fisica..» Su questo tema si veda, O. De Schutter-J. Ringelheim, *Ethnic profiling: A rising challenge for European human rights law*, cit., 358 ss.; B. E. Harcourt, *Against prediction: Profiling, policing, and punishing in an actuarial age*, Chicago, 2008.

44 Su questo aspetto si veda, F. Zuiderveen Borgesius, *Discrimination, artificial intelligence and algorithmic decision-making*, cit., 22. Sulla possibilità di regolamentare questo ambito, P. De Hert-S. Gutwirth, *Regulating profiling in a democratic constitutional state* in M. Hildebrandt - M.S. Gutwirth (a cura di), *Profiling the European Citizen*, cit.

45 Sull'individuazione di un *algorithmic due process* si rimanda a M. Kaminski, *Binary governance: A two-part approach to accountable algorithms*, in *S. Calif. L. Rev.* (2018) 92. Sullo stesso punto, si parla più in generale di *technological due process*, K. Citron, *Technological due process*, in 85 *Wash.UL Rev.*, 2007, 1249.

46 Sul tema del *right of explanation* si veda, L. Edwards-M. Veale, *Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for*, in 16 *Duke L.& Tech.Rev.*, 2017, 18; Id., *Enslaving the algorithm: from a "right to an explanation" to a "right to better decisions"?*, in *IEEE Security & Privacy*, 16(3), 2018, 46 ss.; M. Kaminski, *The right to explanation, explained,* 2018; G. Malgieri, *Right to explanation and algorithm legibility in the EU Member States legislations*, 17 Agosto 2018; cfr. S. Wachter-B. Mittelstadt-L. Floridi, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, in *International Data Privacy Law*, 2017, 2.

regolamentazioni di settore o codici di condotta in specifici ambiti che consentono una maggiore versatilità delle regole approntate, che sono così in grado di rapportarsi in modo sostanziale con le caratteristiche informatiche proprie di ogni algoritmo[47].
Questi aspetti positivi sono però attenuati da una serie di obiezioni che la dottrina in materia ha posto in essere rispetto alla tutela antidiscriminatoria attraverso la protezione dei dati personali. In primo luogo, la disciplina in esame può essere utilizzata solo nel caso in cui il processo decisorio algoritmico gestisca dati personali, nel caso in cui non siano coinvolti dati classificati come tali, non è possibile ricorrere all'autorità garante o fare affidamento sulla normativa. Ad esempio molti dei dati a cui abbiamo fatto riferimento nei casi esposti nel precedente paragrafo, il CAP, il percorso di studi, ma soprattutto perché l'algoritmo di addestramento che crea il modello predittivo non si serve di dati personali, elabora un percorso decisorio sulla base di dati generali[48].

2.5 La tutela antidiscriminatoria negli Stati Uniti d'America nel campo dei processi decisori algoritmici

L'antidiscriminazione nel mondo giuridico americano è uno strumento particolarmente sviluppato capace di adattarsi nel corso degli anni ai vari ambiti di applicazione. A livello costituzionale federale, il fulcro della tutela ruota attorno alla *equal protection clause* contenuta all'interno del XIV emendamento, che garantisce uguale protezione a tutti gli individui da parte del diritto. Questa prescrizione mirava a tutelare i diritti dei soggetti nei confronti degli stati federati, a livello federale, è garantita dalla giurisprudenza della Corte Suprema un'uguale tutela dal quinto emendamento alla costituzione. Tale prescrizione a livello costituzionale a consentito l'introduzione di una serie di strumenti normativi sia a livello nazionale che statale a tutela delle categorie sociali maggiormente esposte a trattamenti discriminatori. In particolare è bene ricordare il *Civil Right Act* del 1964 che riconosce una tutela generale nei confronti di ogni tipo di discriminazione, con particolare riferimento al tema di questo scritto, il titolo VII prevede una garanzia risarcitoria nei confronti di tutte le forme di discriminazione indiretta (*disparate treatment*)[49].
L'ordinamento statunitense, nonostante la posizione di avanguardia dell'industria nazionale nell'ambito dell'intelligenza artificiale, non possiede una legislazione generale sul tema. La produzione normativa ha riguardato principalmente un paio di ordini esecutivi delle amministrazioni Obama e Trump che hanno delineato i piani industriali nel campo dell'intelligenza artificiale, alcune regolamentazioni di determinati settori come quella relativa alle automobili senza conducente e una serie di proposte di legge

[47] Su questo punto si veda S. Bornstein, *Antidiscriminatory algorithms*, cit., 522 ss.; J. Kleinberg-J. Ludwig-S. Mullainathan-C. Sunstein, *Discrimination in the age of algorithms*, cit., 5.

[48] Sui limiti della normativa sul trattamento dei dati: S. Wachter-B. Mittelstadt, *A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI*, cit., 81 ss; M. Ananny-M K. Crawford, *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*, in *New Media & Society* 20(3), 2018, 973.

[49] Su questo punto in relazione con i processi decisori algoritmici si veda, S. Bornstein, *Antidiscriminatory algorithms*, cit., 525 ss.

presentate davanti al Congresso e in attesa di essere votate[50].
Di queste ultime, gli esempi più importanti sono stati i progetti di legge presentati al Senato e alla Camera relativi all'*Algorithmic Accountability Act* (S. 1108, H.R.2231) che sono stati introdotti al Congresso il 10 aprile 2019, probabilmente in risposta ai rapporti recentemente pubblicizzati sui rischi dei risultati distorti prodotti dall'utilizzo dell'intelligenza artificiale[51]. Il disegno di legge mira a richiedere agli attori privati e alle entità pubbliche di condurre delle valutazioni d'impatto sui loro sistemi decisionali automatizzati considerati "ad alto rischio" al fine di verificare in quale modo il processo decisorio algoritmico si relaziona con i principi generali di accuratezza, correttezza, privacy e sicurezza[52]. La proposta prevede inoltre che tali valutazioni dovrebbero essere condotte da terze parti esterne, compresi revisori ed esperti tecnologici indipendenti[53]. Questa normativa richiede agli operatori privati e pubblici che impiegano intelligenze artificiali di condurre valutazioni di impatto del tutto simili a quelle proposte dal disegno di legge federali sui processi decisionali algoritmici e sui sistemi informativi. Tale verifica implica una valutazione del processo di sviluppo del sistema, compresa la componente relativa al suo *design and training data*, deve contenere una descrizione dettagliata delle migliori pratiche utilizzate per minimizzare i rischi e un'analisi costo-benefici[54].

3. La discriminazione algoritmica in pratica: una serie di casi sostanziali

Uno studio esaustivo di questo tema non può realizzarsi senza un approfondimento di alcuni casi sostanziali che hanno riguardato la tutela discriminatoria rispetto all'impiego degli algoritmi all'interno dei processi decisori elaborati dalla pubblica amministrazione o da attori privati. Come si è illustrato nella sezione precedente, la casistica è alquanto ampia e si è scelto quindi di concentrare l'attenzione su due categorie che riguardano la selezione di dipendenti e studenti, la pubblicità online. È ovvio che questa disamina esclude alcuni ambiti molto rilevanti quali la pubblica sicurezza, le traduzioni automatiche, la ricerca di immagini nella rete e la discriminazione di prezzo.

Selezione e valutazione dipendenti pubblici
Si è già visto come l'intelligenza artificiale possa essere utilizzata per selezionare po-

[50] Executive Office of the President National Science and Technology Council, Committee on Technology, *Preparing for the Future of Artificial Intelligence*, Ottobre 2016. Questo primo documento dell'Amministazione Obama è stato seguito da un ordine esecutivo dell'amministrazione Trump, Exec. Order No. 13,859, 3 C.F.R. 396, 2019.

[51] Algorithmic Accountability Act of 2019, S. 1108, H.R. 2231, 116th Cong. (2019). Sulla proposta di legge si veda S. Revanur, *In a Historic Step Toward Safer AI, Democratic Lawmakers Propose Algorithmic Accountability Act*, in *Medium* (20 aprile 2019).

[52] Algorithmic Accountability Act (2019) par. 2 c. 2 e 3 lett. (b).

[53] Algorithmic Accountability Act (2019) par. 3 lett. (b)(1)(C).

[54] E. J. Tail et al., *Proposed Algorithmic Accountability Act Targets Bias in Artificial Intelligence*, in *JD Supra*, 27 giugno 2019.

tenziali dipendenti o studenti. Un caso di questo genere ha riguardato Amazon[55], che impiegava un sistema di intelligenza artificiale per la selezione dei candidati alle posizioni di lavoro nell'azienda, i programmatori l'avevano addestrato a trovare modelli nei curriculum inviati per tecnici informatici nei dieci anni precedenti, la maggior parte dei quali, a causa della demografia di chi detiene quei posti di lavoro, proveniva da candidati uomini. Di conseguenza l'algoritmo aveva sviluppato un modello che lo portava a preferire i candidati maschi, perciò qualsiasi frase che includesse la parola "donna" o sue derivazioni, come in "capitano del club di scacchi femminile" comportava l'automatica esclusione del curriculum della candidata[56].

Nel caso di Amazon, l'azienda ha posto rimedio accantonando il software nella impossibilità di escludere ogni possibile esito discriminatorio del processo decisorio algoritmico, in altri casi distinguere la portata di alcuni dati è molto più difficile, di conseguenza provare eventuali effetti discriminatori diventa complicato. In questo senso è emblematico il caso *McKinzy v. Union Pacific*[57], nel quale l'attore, un candidato ad una posizione lavorativa ha citato in giudizio il potenziale datore di lavoro, sulla base di una supposta discriminazione razziale da parte dell'algoritmo[58]. Il procedimento ha stabilito che l'azienda aveva utilizzato un algoritmo per valutare il curriculum dell'attore, il quale ha affermato di essere stato escluso in ragione della sua origine etnica, la difesa della Union Pacific ha fornito i dati relativi all'esperienza lavorativa dell'attore, sottolineando come McKinzy non fosse qualificato per la posizione aperta secondo dati che non tenevano conto dell'appartenenza etnica. La corte si è pronunciata a favore della Union Pacific proprio per la sua capacità di motivare sulla base di criteri neutri il rigetto del candidato[59]. Si è visto in precedenza come simili criteri possano comunque comportare un risultato discriminatorio indiretto se sono collegati (*proxies*) con caratteristiche relative a determinate categorie sociali. Rispetto alla discriminazione indiretta si è già avuto modo di parlare di come sia la Corte Edu, che le direttive UE[60] consentano l'eccezione del perseguimento di un obiettivo legittimo e necessario. In questo senso la Corte Suprema degli Stati Uniti[61] aveva già tracciato la strada con la teoria della "*business necessity*", per la quale, se un datore di lavoro può dimostrare che una particolare misura o politica aziendale è necessaria per la conduzione dell'impresa anche se questa comporta il verificarsi di una discriminazione indiretta. Con riferimento ai casi di discriminazione algoritmica, questa difesa potrebbe applicarsi se il datore di lavoro può

---

55 Il caso è raccontato in J. Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, in *Reuters*, 9 ottobre, 2018.

56 La rilevanza giuridica del caso è esposta in S. Bornstein, *Antidiscriminatory algorithms,* cit., 521.

57 *McKinzy v. Union Pac. R.R.,*2010WL3700546(2010).

58 *Ibid.*

59 *Ibid.*

60 Si rimanda alla sentenza Corte Edu, *D.H. and Others v. Czech Republic*, ric. 57325/00, (2007), §§ 187-188; art. 2 , par. 2, direttiva 2000/43/EC.

61 La teoria della *business necessity* è stata elaborata nel precedente *Griggs v. Duke Power Co.*, 401 U.S. 424 (1971).Si veda sulla questione I. Ajunwa, *Automated Hiring*, cit., 41-2. L'utilizzo del dato statistico per provare la *business necessity* è richiamato sia da Ajunwa per quanto riguarda la Corte Suprema, sia da F. Zuiderveen Borgesius, *Discrimination, artificial intelligence and algorithmic decision-making*, cit., 19 per quanto concerne la Corte Edu e la normativa UE.

dimostrare che i dati su cui fa affidamento un algoritmo sono una "necessità aziendale" o, in altre parole, sono statisticamente correlati ad una corretta gestione dell'azienda.

Pubblicità online

L'intelligenza artificiale è impiegata per la pubblicità online mirata, in questo campo, l'algoritmo rielabora i dati forniti dagli utenti attraverso le loro interazioni per proporre segnalazioni pubblicitarie su misura. Questo impiego dell'intelligenza artificiale è stato segnalato perché particolarmente esposto a pratiche discriminatorie, già nel 2013 si è dimostrato come le persone che cercassero nomi di provenienza afroamericana, venivano esposti dal motore di ricerca di Google ad annunci pubblicitari per soggetti destinatari di condanne penali o precedenti di polizia. Al contrario, se si digitavano nomi di provenienza caucasica, lo stesso motore di ricerca individuava un numero significativamente inferiore di annunci connessi ai precedenti giudiziari dei destinari[62].
Nel 2015 uno studio condotto da ricercatori ha elaborato una simulazione nella quale utenti del motore di ricerca di Google, che si sono auto-dichiarati maschi o femmine nelle impostazioni, effettuavano identiche ricerche online sulla piattaforma. I ricercatori hanno quindi analizzato gli annunci presentati dall'algoritmo. Google ha mostrato annunci pubblicitari agli utenti simulati maschili da una certa agenzia di consulenza che prometteva salari elevati con frequenza significativamente maggiore rispetto a quelli proposti alle utenti simulate donne con effetti discriminatori. Lo studio ha inoltre notato come non sia possibile individuare il motivo per il quale alle utenti simulate donne è stato mostrato un numero inferiore di annunci pubblicitari per impieghi a salari elevati, a causa dell'opacità del sistema automatico che gestisce la piattaforma e elabora i diversi dati immessi dagli utenti[63].
Un altro caso interessante ha riguardato le modalità di inserzione degli annunci pubblicitari proposte dalla piattaforma Facebook. Il social network ha consentito agli inserzionisti di indirizzare gli annunci pubblicitari agli utenti sulla base di una serie di dati sensibili processati dal suo algoritmo come ad esempio, i dati relativi alle preferenze sessuali[64]. Il Garante per la protezione dei dati olandese ha posto in essere un'indagine in questo ambito e ha provveduto a registrare una serie di profili falsi sulla piattaforma indicanti, tra le varie informazioni richieste, la categoria "*men that are interested in other men*"[65]. La totalità dei profili registrati non ha posto in essere ulteriori interazioni sulla piattaforma ed è stata esposta a campagne pubblicitarie mirate per quella specifica categoria[66].

---

62 L. Sweeney, *Discrimination in online ad delivery*, in *Queue*, 2013, 11(3).

63 Lo studio empirico è descritto dagli autori in A. Datta - M. C. Tschantz - A. Datta, *Automated experiments on ad privacy settings*, in *Proceedings on Privacy Enhancing Technologies*, 2015, 92 A. Datta et al., *Discrimination in online advertising: A multidisciplinary inquiry,* (Conference on Fairness, Accountability and Transparency 2018) 20.

64 Autorità garante del trattamento dei dati olandese, *Dutch data protection authority: Facebook violates privacy law*, 16 maggio 2017.

65 Autorità garante del trattamento dei dati olandese, *Informal English translation of the conclusions of the Dutch Data Protection Authority in its final report of findings about its investigation into the processing of personal data by the Facebook group*, 23 febbraio 2017, 3.

66 *Ibid.*

Un ulteriore aspetto relativo alle inserzioni pubblicitarie sul social network Facebook è stato oggetto di un procedimento davanti ad una corte federale statunitense. La piattaforma consentiva agli inserzionisti, attraverso una serie di menù a scelta denominato "affinità etniche", di escludere una serie di categorie sociali come la popolazione di origine africana o ispanica dalla visualizzazione degli annunci[67]. La piattaforma consentiva anche l'esclusione di precisi gruppi di individui quali *"women in the workforce,", "moms of grade school kids,", "foreigners", "Puerto Rico Islanders"*; ovvero soggetti interessati a *"parenting," "accessibility," "service animal," "Hijab Fashion", "Hispanic Culture"* ovvero la pubblicizzazione di annunci di lavoro solo a persone di una determinata fascia di età[68]. Sulla base di queste risultanze una serie di organizzazioni no profit che operano nell'ambito del diritto all'abitazione e della tutela antidiscriminatoria nel mercato immobiliare hanno citato in giudizio[69] Facebook per la violazione del *Fair Housing Act* che prescrive come *«[t]o make, print, or publish, or cause to be made, printed, or published any notice, statement, or advertisement, with respect to the sale or rental of a dwelling that indicates any preference, limitation, or discrimination based on race, color, religion, sex, handicap, familial status, or national origin, or an intention to make any such preference, limitation, or discrimination»*[70]. Il ricorso lamentava essenzialmente tre condotte discriminatorie da parte della piattaforma: la possibilità per gli inserzionisti di includere o escludere gli utenti in base al loro sesso, età, interessi, comportamenti o dati demografici che si presume siano correlati o associati a razza, origine nazionale, disabilità o stato di famiglia; La possibilità per gli inserzionisti di definire un'area geografica ristretta per il pubblico degli annunci che potrebbe presumibilmente avere un impatto negativo in base alla razza o all'origine nazionale; 3) il possibile impiego dello strumento informatico *Lookalike Audience* da parte degli inserzionisti che avrebbe permesso di creare segmenti di pubblico tra gli utenti secondo dinamiche in grado di avere un impatto negativo su vari gruppi, anche in base a sesso, razza ed età[71]. Le parti hanno deciso di addivenire ad un accordo stragiudiziale[72] sulla base di una serie di comportamenti che il convenuto ha acconsentito di adottare per emendare le pratiche discriminatorie citate nel ricorso, tra le quali: a) la piattaforma creerà un portale pubblicitario separato per la creazione di annunci di alloggi, occupazione e credito ("HEC") che avrà opzioni di *targeting* limitate, per prevenire la discriminazione; b) Facebook elaborerà una pagina in cui gli utenti possano cercare e visualizzare tutti gli annunci che sono stati inseriti dagli inserzionisti per l'affitto e la vendita di alloggi indipendentemente dal fatto che gli utenti abbiano ricevuto tali annunci immobiliari sulla loro bacheca; c) la piattaforma richiederà agli inserzionisti di certificare il rispetto delle politiche di Facebook che vietano la discriminazione e tutte le leggi anti-discrimi-

---

67 Su questo punto si veda J. Angwin et al., *Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks*, in *ProPublica*, Maggio 2016; J. Angwin-A. Tobin-M. Varner, *Facebook (still) letting housing advertisers exclude users by race*, in *ProPublica*, Novembre 2017.

68 J. Angwin-N. Scheiber-A. Tobin, *Dozens of companies are using Facebook to exclude older workers from job ads*, in *ProPublica*, Dicembre 2017.

69 NFHA v. Facebook complaint, Caso 1:18-cv-02689, 25 giugno 2019.

70 42 U.S.C. § 3604(c).

71 NFHA v. Facebook complaint, Caso 1:18-cv-02689, cit.

72 NFHA v. Facebook settlement agreement, 18 marzo 2019.

nazione applicabili; d) Facebook consentirà ai querelanti di testare la sperimentazione della piattaforma pubblicitaria per garantire che le modifiche stabilite dall'accordo siano attuate in modo efficace[73].
Un ulteriore ricorso è stato presentato da parte del *Housing and Urban Development Department* degli Stati Uniti D'America sulla base delle stesse risultanze della causa appena riportata[74] Con un atto di citazione nell'estate del 2019 il Dipartimento federale conviene in giudizio la piattaforma Facebook per la violazione del *Fair Housing Act*. Non si conoscono ad oggi le sorti di questo contenzioso, le pratiche discriminatorie a cui si fa riferimento si estendono fino al primo trimestre dello scorso anno[75].

4. A mo' di conclusione

È difficile poter tracciare un quadro definitivo di una disciplina ancora in piena evoluzione. Lo sviluppo tecnologico nel campo dell'intelligenza artificiale è in rapida espansione e il diritto, per sua stessa natura, fatica a tenere il passo. I due approcci che sono stati utilizzati per presentare la disciplina antidiscriminatoria rispetto all'impiego degli algoritmi rappresentano le basi con cui si sta affrontando questo sforzo. Come si è detto l'approccio *ex ante* è spesso preferibile specie in quei contesti dove è possibile intervenire con autorità indipendenti come il Garante del trattamento dei dati che sono in grado di specificare il materiale regolamentare per adattarlo alle diverse realtà. In quegli ambiti nei quali tale cooperazione è più difficile, l'approccio *ex post* può sopperire ad eventuali lacune nella regolamentazione. Una sinergia tra questi due schemi di tutela sembra essere il modo migliore per estendere una tutela antidiscriminatoria effettiva ai processi decisori algoritmici.

[73] *Ibid.*

[74] La violazione del 42 U.S.C. § 3604(c).

[75] HUD v. Facebook complaint, FHEO No. 01-18-0323-8, 27 marzo 2019.

Smart assistant e dati personali: quali rischi per gli utenti?*

Lavinia Vizzoni

Abstract

Gli *smart assistant* sono programmi di assistenza vocale ormai molto diffusi. Il loro facile utilizzo e soprattutto la loro idoneità a rispondere a semplici richieste inoltrate dall'utente si accompagna però all'estrema pervasività degli stessi, che basano il loro funzionamento sulla raccolta di dati personali dell'utente (spesso di categorie particolari di dati) e si dimostrano idonei a captare pressoché ogni informazione rilasciata nell'ambiente circostante. Numerosi appaiono dunque i profili problematici che gli *assistant* presentano con riguardo alla disciplina del trattamento dei dati personali; i quali fanno emergere la necessità di ricercare una soluzione configurata in termini di "*design*" del programma stesso, all'interno di uno scenario in cui anche le certificazioni sono destinate ad assumere un ruolo sempre più di rilievo.

Smart assistants are now very popular voice assistance programs. Their easy use and above all their suitability to respond to simple requests sent by the user is though accompanied by the extreme pervasiveness of the assistants, which base their functioning on the extensive collection of the user's personal data (often special categories of data), and have proven to be capable of capturing almost any information released into the surrounding environment. Therefore, there are several challenging aspects that assistants show in comparison to the discipline of personal data processing, which reveal a need to seek a solution configured in terms of "design" of the program itself, within a scenario where even certification mechanisms are destined to assume an increasingly crucial role.

Sommario

Keywords

Smart assistant - *internet of Things* - intelligenza artificiale - *privacy by design* - certificazioni

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

1. Assistenti vocali, intelligenza artificiale e *Internet of Things*

Lo sviluppo delle tecnologie digitali applicate alla quotidianità ha condotto, negli ultimi anni, a una massiccia diffusione dei c.d. *smart assistant*. Si tratta di *software* che, grazie al c.d. *machine learning*, ossia a sistemi di apprendimento che utilizzano algoritmi di intelligenza artificiale, sono in grado di riconoscere il linguaggio naturale degli esseri umani e di interagire con gli stessi. Tale interazione può essere rivolta a soddisfare diversi tipi di richieste (ad esempio, fissare appuntamenti, impostare sveglie, *timer* e promemoria, riprodurre musica o notiziari, fornire previsioni meteo e di traffico) o a compiere determinate azioni, come accendere una luce, azionare un elettrodomestico o regolare la temperatura di un'abitazione.

Il loro costo contenuto, la frequente preinstallazione nei *device* e la semplicità di funzionamento ne hanno agevolato la diffusione e l'impiego. Gli assistenti in questione possono infatti essere installati in una pluralità di supporti: dagli *smart speaker* collocati all'interno delle abitazioni domestiche, ma anche di altri ambienti antropizzati, quali i luoghi di lavoro[1], se non anche le automobili, ai *device* che portiamo fisicamente con noi, i c.d. *wearable*, sino ai dispositivi più diffusi come gli *smartphone,* i *personal computer* e i *tablet*. In particolare, gli stessi si prestano anche ad agevolare lo svolgimento di attività quotidiane anche da parte di soggetti con autonomia ridotta.

Per fare questo, gli assistenti vocali raccolgono quasi ininterrottamente dati personali relativi sia all'utente diretto sia, più in generale, a coloro che si trovano nell'ambiente in cui gli stessi operano. Per di più, gli *smart assistant* si possono avvalere anche di soluzioni proprie del c.d. *Internet of Things* (*IoT*)[2], che offre la possibilità di sfruttare i vari oggetti, appunto, le "*things*" che incorporano i programmi di assistenza vocale "intelligente", per la raccolta di informazioni e l'attuazione di interventi finalizzati al miglioramento dei servizi offerti[3]. Gli *smart assistant* sono infatti capaci di "dialogare" con altri dispositivi *IoT*, come *smartwatch*, *smart* TV, sistemi di controllo da remoto o di videosorveglianza; il che amplifica la possibilità di raccolta, incrocio dei dati e diffusione di informazioni personali.

Se in passato l'*Internet of Things* si collocava in una rete di sensori in grado di restituire

[1] Con i conseguenti rilevanti interrogativi che si pongono in ordine alla sorveglianza dei lavoratori. Sulle intersezioni fra *data protection* e diritto del lavoro, v. precipuamente E. Dagnino, *Tecnologie e controlli a distanza*, in *Dir. rel. ind.*, 2015, 988 ss. e A. Stolfa, *La tutela della privacy sul luogo di lavoro: gli orientamenti della Corte Europea dei Diritti dell'Uomo*, in *Lav. giur*, 2018, 530 ss.

[2] Sulle applicazioni dell'*Iot*, con particolare riguardo proprio agli assistenti virtuali, cfr. le preoccupazioni espresse già da G. Ramaccioni *La protezione dei dati personali e il danno non patrimoniale. Studio sulla tutela della persona nella prospettiva risarcitoria*, Napoli, 2017, 16 ss. e 288 ss.

[3] Sulle potenzialità dell'*Iot* cfr. A. Santosuosso, *Intelligenza artificiale e diritto*, Milano, 2020, 180 ss., il quale evidenzia come l'Internet delle cose sia al centro dell'interesse della politica economica dell'Unione Europea. In tale prospettiva, esso diviene punto focale per la digitalizzazione della società, nel contesto dell'implementazione delle tecnologie 5G e nel perseguimento del più ampio obiettivo della realizzazione del *digital single market*. Sugli sviluppi dell'*IoT* e sui relativi impatti in tema di trattamento dei dati personali, cfr. E. Tosi, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice* Privacy, in Id. (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, Milano, 2019, 36 ss.

informazioni mediante tecnologie di RFID (*Radio Frequency IDentification*)[4], con l'avvento del Web si è passati ad un contesto più evoluto, in grado di catturare quantitativi ben maggiori di informazioni attraverso la connessione dei dispositivi. Le applicazioni dell'*IoT* investono oggi molteplici settori, a partire dall'industria 4.0[5], e si raccordano sempre di più all'uso di piattaforme, che permettono di connettere e controllare esternamente i dispositivi, di memorizzare e analizzare i dati raccolti, di monitorare e comandare gli oggetti connessi[6].

Rispetto ai dati personali raccolti dagli assistenti *smart* connessi diventa inoltre oggi cruciale la nozione non solo di interconnessione, ma anche di interoperabilità fra i sistemi informatici[7]: la tendenza in atto è infatti quella dello sviluppo di multipiattaforme che puntano al controllo di oggetti *smart* di fornitori e marche diverse da un unico punto di contatto. Particolarmente significativo appare l'accordo di recente stretto tra Amazon, Apple e Google, in genere non propensi ad alleanze, per la creazione di un protocollo unitario per la casa connessa, grazie al quale tutti i dispositivi potranno essere controllati con Alexa, Siri e Google Assistant[8].

Lungo tale versante, sono destinate ad imporsi all'attenzione degli studiosi proprio le implicazioni legate alla sicurezza e all'interoperabilità di architetture *IoT*, che assumono sembianze sempre più capillari[9].

---

[4] Cfr. F. Giovanella., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Milano, 2019, 1213.

[5] Nel contesto di quella che è una vera e propria *smart factory*, sono state sviluppate soluzioni che, per quanto futuristiche appaiano, sono già una realtà e vengono attualmente utilizzate in ambienti industriali tecnologicamente progrediti. Rientrano nel novero di siffatte soluzioni i dispositivi di robotica indossabile, quali gli esoscheletri per applicazioni industriali volti ad aumentare le capacità operative dei lavoratori che svolgono attività manuali e di movimentazione; o le *smart suit,* ossia tute realizzate anche tramite scansioni del corpo del lavoratore; così come le postazioni di lavoro auto-adattive, strutturate sulla base delle caratteristiche proprie di chi è chiamato ad utilizzare quelle postazioni, anche in termini di condizioni fisiche e di affaticamento. In proposito, v. l'analisi di L. Greco - A. Mantelero, *Industria 4.0, robotica e* privacy-by-design, in *Dir. informaz. informatica*, 2018, 883 ss.

[6] In generale, sulle piattaforme *online*, v. A. De Franceschi, *La vendita di beni con elementi digitali,* Napoli, 2019, 19 ss. In proposito, cfr. anche C. Busch, *Towards Fairness and Transparency in the Platform Economy? A First Look at the P2B Regulation*, in A. De Franceschi - R. Schulze (a cura di), *Digital Revolution – New Challenges for Law*, Baden-Baden, 2019, 57 ss.

[7] Sulla interoperabilità v. G.M. Riccio - F. Pezza, *Portabilità dei dati personali e interoperabilità*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 398 ss. Lo scritto (404 s.) si sofferma sulla interoperabilità, in relazione all'effettività del diritto alla portabilità nel settore della telefonia mobile, evidenziando la positività del modello inglese che pone gli obblighi relativi a carico del precedente gestore. Cfr. anche E. Battelli - G. D'Ippolito, *Il diritto alla portabilità dei dati personali*, in E. Tosi (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, cit., 202 ss.

[8] La notizia, datata 19 dicembre 2019, è tratta dal sito web www.corriere.it/tecnologia. Oltre ai citati Google, Amazon ed Apple, hanno aderito all'accordo in questione i produttori riuniti nella Zigbee Alliance, fra cui Ikea, Samsung SmartThings e Schneider Electric, a conferma del grande interesse che il mercato della domotica suscita. Il relativo protocollo sarà *open source* e tutti potranno realizzare prodotti compatibili con i tre noti assistenti vocali. Già rilevante era d'altronde apparso l'acquisto, da parte di Google, avvenuto nel 2014, di Nest Labs, azienda che aveva l'obiettivo di creare proprio dispositivi domotici, come i termostati e rilevatori di fumo.

[9] Qualche risultato nella direzione della interoperabilità sembra stia arrivando da ONEM2M (www.onem2m.org), un progetto congiunto di otto enti di standardizzazione mondiali, tra cui ETSI (Europa), ARIB (Giappone), CCIA (Cina), TIA (Nord America) e duecento partner, che si propone di definire

Da altra parte, l'implementazione dei programmi di assistenza vocale si lega strettamente ai progressi ottenuti nel campo dell'intelligenza artificiale. Lanciando ricerche vocali, l'utente inoltra segnali proprio ai sistemi di intelligenza artificiale utilizzati dagli *smart assistant*, che, tramite quegli *input* continuano a implementarsi così riuscendo a comprendere la domanda e a fornire risposte sempre migliori, riducendo progressivamente il margine di errore[10].

Più precisamente, l'intelligenza artificiale utilizza algoritmi sofisticati per ordinare enormi quantità di dati, tracciare schemi e fare previsioni: attività che sarebbero ripetitive e lunghe, se non praticamente impossibili, da eseguire manualmente. Le macchine "intelligenti" contribuiscono fortemente allo svolgimento di tali attività, avvalendosi anche della nota capacità di imparare da sé stesse, attraverso il c.d. *machine learning*, o addirittura di elaborare nuovi percorsi di apprendimento con il c.d. *deep learning*[11]. L'intelligenza artificiale pone però all'attenzione del giurista una serie di interrogativi che mettono alla prova le capacità di risposta dell'ordinamento giuridico e delle relative categorie concettuali[12]. Come osservato, l'idea che una macchina, per quanto "intelligente", possa assumere autonomamente decisioni che riverberano i loro effetti anche su diritti fondamentali della persona, suscita preoccupazione, e impone una riflessione approfondita che, in prospettiva, coinvolge anche le decisioni di politica del diritto da assumere[13].

La vera sfida — che già si profila con una certa chiarezza — dei meccanismi che sfruttano, per il loro funzionamento, algoritmi di intelligenza artificiale, sarà quella di conseguire soluzioni che garantiscano, anche sul versante etico, di soddisfare i criteri di spiegabilità, robustezza, correttezza e tracciabilità[14]. Non a caso, dalla Commissione Europea sono di recente giunte Linee Guida per uno sviluppo etico dell'intelligenza artificiale: si tratta di un documento, dal valore programmatico, che detta indicazioni per uno sviluppo di un'intelligenza artificiale a misura di essere umano[15], da ultimo

---

degli standard di riferimento (*framework* di interlavoro) per la costruzione di piattaforme di servizio interoperanti.

[10] V. G. D'Acquisto - M. Naldi, Big Data *e* Privacy by Design. *Anonimizzazione, Pseudonimizzazione, Sicurezza*, Torino, 2017, 9 ss.

[11] Cfr. F. Crisci, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm*., 2018, 1787 ss.

[12] V. U. Ruffolo - E. Gabrielli, *Introduzione*, in Id (a cura di), *Intelligenza artificiale e diritto,* in *Giur. it*., 2019, 1657 ss. Cfr. inoltre N. Zorzi Galgano, *Introduzione,* in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, 15 ss.

[13] Cfr. A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, 63 ss.

[14] Sul bilanciamento, in chiave etica, fra diffusione di soluzioni tecnologiche avanzate e impatto sui diritti e le libertà della persona, cfr. D. Wright, *A framework for the ethical impact assessment of information technology*, in *Ethics Inf. technol*., 2011, 199 ss.

[15] Sono i risultati diffusi dall'*High Level Group on Artificial Intelligence* della Commissione europea, reperibili nel sito web www.ec.europa.eu. La Commissione stessa, nelle sue comunicazioni del 25 aprile 2018 e del 7 dicembre 2018, ha diffuso la sua visione al riguardo, che sostiene un'AI «etica, sicura e all'avanguardia realizzata in Europa». Le linee guida della Commissione europea per un'intelligenza artificiale affidabile sono peraltro state aggiornate nel settembre 2019 dal centro studi del Parlamento europeo. Sul difficoltoso percorso orientato al pervenir ad un sistema europeo di *governance* dell'intelligenza artificiale, v. inoltre G. Mazzini, *A system of governance for Artificial Intelligence through the lens of emerging intersections between AI and EU law*, in A. De Franceschi R. Schulze (a cura di), *Digital Revolution – New Challenges for*

compendiate nel «Libro bianco sull'intelligenza artificiale — Un approccio europeo all'eccellenza e alla fiducia», datato 19 febbraio 2020.
A livello nazionale, è d'uopo quanto meno ricordare l'elaborazione dalle Proposte per una strategia italiana per l'intelligenza artificiale del Gruppo di esperti MISE[16], che, sulla stessa linea, indicano un percorso verso l'implementazione di un'intelligenza artificiale complementare — piuttosto che sostitutiva — all'intelligenza umana, tale da consentire di garantire il rispetto dei valori e dei principi fondamentali[17].

2. I relativi vantaggi e rischi

Proprio lo sviluppo di algoritmi evoluti di intelligenza artificiale, unitamente all'interconnessione degli oggetti *smart*, ha consentito dunque di creare soluzioni parzialmente o totalmente autonome, le cui capacità di apprendimento e monitoraggio delle abitudini degli utenti crescono esponenzialmente, di pari passo al tentativo, sempre più preciso, di adattare il livello di servizio offerto sulla base delle richieste effettuate dagli individui stessi. E a sua volta, la proficua convergenza fra *IoT* e *AI* dipende dalla disponibilità di dati personali.
In questo contesto, l'attenzione particolare che può essere riservata agli assistenti vocali "intelligenti" deriva da una duplice ragione: lo stretto legame del loro funzionamento con i dati personali, posto che l'operatività del dispositivo abbisogna, anzi, è dichiaratamente funzionale alla raccolta delle informazioni dall'utilizzatore e dal suo ambiente esistenziale, nonché il loro elevato grado di pervasività rispetto alla vita degli utenti.
Soprattutto, considerazioni inerenti all'ingente quantitativo di dati personali raccolti ed elaborati dai *device*, e correlative perplessità, sono state avanzate con riguardo agli *home speaker*, che trovano collocazione proprio nella casa, luogo dell'*habitat* domestico nel quale si svolge la personalità umana, da difendere gelosamente dalle intrusioni esterne, tanto da elevarsi, nella sua accezione di domicilio, ad area inviolabile al pari della stessa libertà personale[18].
Come osservato, gli *home speaker* rappresentano una sorta di *alter ego*[19], se non dei veri e propri «maggiordomi» dei proprietari[20], che raccolgono dati non solo sulle proprie

Law, cit., 245 ss.

[16] La prima versione delle Proposte per una strategia italiana per l'intelligenza artificiale è datata luglio 2019 ed è reperibile nel sito web del Ministero, www.mise.gov.it.

[17] É tuttavia rilevante segnalare che la versione finale di tali Proposte, formulata nel corrente anno dal Gruppo di esperti di alto livello del MISE, esprime apertamente una visuale non del tutto collimante con le indicazioni provenienti dall'Europa. In particolare, nelle Proposte nazionali si fa riferimento alla circostanza per cui l'Unione Europea manifesterebbe una visione del fenomeno eccessivamente orientata in chiave industriale e poco attenta ai profili di sostenibilità dello sviluppo.

[18] In sintesi, sul fondamentale rapporto di derivazione che lega il domicilio alla libertà personale, cfr. P. Scarlatti, *Libertà e inviolabilità del domicilio*, in *Diritto on line-Treccani*, 2016.

[19] Cfr. E. Palmerini, *Dalle* smart cities *allo* scoring *del cittadino*, in *I Confini del Digitale. Nuovi scenari per la protezione dei dati,* Convegno per la Giornata europea della protezione dei dati personali 2019 - 29 gennaio, Roma, 17 ss., spec. 23.

[20] Sono le considerazioni di F. Pizzetti., *Domotica. L'intelligenza artificiale che ci spia a casa: quali rischi e*

performance, quali prodotti, ma anche dati personali (scelte, preferenze, abitudini di consumo ...) degli utenti stessi; assistenti personali virtuali, dunque, che imparano a conoscere l'utente che interagisce con loro molto a fondo, e persino ad anticipare le relative richieste, eventualmente stipulando anche i relativi contratti[21].

Inoltre, gli assistenti vocali sono costantemente in attività grazie agli altri dispositivi ai quali sono connessi. Ciò può significare che, anche quando l'*assistant* non è in utilizzo, trasmette in continuazione ogni accadimento o variazione dell'ambiente che è in grado di percepire[22], con la realizzazione di un'operazione continua di monitoraggio dei comportamenti e di profilazione degli individui[23]. In effetti, il rapporto vocale tra le persone e lo *speaker*, così cruciale negli assistenti, appunto, vocali, demandati a rispondere alle richieste dell'utente, è possibile in quanto l'apparecchio è dotato della capacità di ascolto non solo del comando che gli venga di volta in volta impartito, ma di tutto ciò che accade nell'ambiente circostante[24]. D'altronde, i dispositivi in questione hanno dimostrato di registrare indifferentemente tutte le conversazioni che avvengano all'interno dell'ambiente domestico, ivi comprese, dunque, quelle in cui partecipino terzi che potrebbero addirittura ignorare l'esistenza di tali *device* o il relativo funzionamento. Gli utenti, così come i terzi inconsapevoli, potrebbero persino attivare l'*assistant* inavvertitamente, con comandi vocali impartiti involontariamente: studi pratici hanno infatti svelato che molti *speaker* non solo si accendono per effetto della pronunzia delle parole convenzionali, bensì rispondono anche ad una serie di stimoli vocali ulteriori.[25]

Il flusso di dati che i dispositivi generano è dunque costante e consistente: una situazione a cui fa, peraltro, da contraltare un profilo di particolare criticità, ossia la diffusa inconsapevolezza degli utenti[26], a maggior ragione particolarmente problematica pro-

soluzioni per la privacy, reperibileagendadigitale.eu, 4 aprile 2018, secondo il quale gli assistenti digitali intelligenti sono paragonabili a «moderni maggiordomi dell'era digitale, ma, esattamente come i maggiordomi vittoriani, sanno tutto di ciò che accade nella casa e tutto registrano e ritrasmettono».

21 È quanto osservato da E. Palmerini, *Dalle smart cities allo scoring del cittadino,* cit., 24.

22 V. ancora F. Pizzetti, *Domotica. L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la* privacy, cit.

23 In tema: A. Pierucci, *Elaborazione dei dati e profilazione delle persone*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 413 ss.

24 Nella scheda informativa dell'Autorità Garante per la protezione dei dati personali, su cui v. *infra*, par. 4, si fa espresso riferimento al fatto che «Quando è acceso ma non viene utilizzato, l'assistente digitale è in uno stato detto di *passive listening*, una sorta di "dormiveglia" da cui esce non appena sente la parola di attivazione che abbiamo scelto».

25 Soprattutto gli *home speaker* sembrano rispondere a molti più comandi vocali rispetto a quelle che sono le formule di accensione. Secondo quanto riportato dalla P*olicy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world* dello *European Consumer Consultative Group*, datata 16 maggio 2018, 13: «*In 2017, the Federation of German Consumer Organisations (vzbv) analysed the voice-controlled personal assistant 'Amazon Echo' and found that the device was recording far more conversation than the user intended as it reacted not only to the activating code word 'Alexa' but also to similar words. The same has been found to be true for Google Assistant*». Ancora, nella *Policy* si legge (9): «*Practical testing by the Digital Market Watch project of German consumer association has demonstrated that Google's Home Assistant that is supposed to be activated with the words 'OK Google' also awakens when conversations contain 'OK Kuchen' - meaning "OK cake" in German - and 'OK gut' – meaning 'OK fine'. The unwanted activation of the home assistant system entails that more private conversations are being transmitted and processed by Google than intended. Similar results were obtained for Amazon's Alexa*».

26 A proposito dell'inconsapevolezza dell'utente v. A. Mantelero, *Data protection, e-ticketing, and intelligent*

prio nei soggetti che da quelle soluzioni potrebbero trarre i vantaggi maggiori, ossia i soggetti più vulnerabili[27].

3. Assistenti vocali e trattamento dei dati personali

Già in siffatta esemplificazione si intravedono, a fianco delle molteplici opportunità, altrettanti rischi a carico dell'utente, soprattutto sul versante del trattamento dei dati personali[28]. Non è senza significato che ogni *Big Player* della Rete abbia creato un proprio *smart assistant,* strumento diretto per operare la profilazione dell'utente (i noti Siri di Apple, Alexa di Amazon, Cortana di Microsoft e Google Assistant di Google) e che proprio gli Internet Giants «*are leading the pack ... with no clear competitor in sight*»[29].
È in questa sede possibile soltanto accennare ai singoli profili che, dinanzi alla concreta operatività degli assistenti vocali intelligenti, svelano una particolare problematicità, senza poterli illustrare in dettaglio.
Già alcuni principi declamati dal regolamento si attagliano con difficoltà a scenari tecnologicamente evoluti, come quello in esame, specialmente laddove — e questo può senz'altro accadere — il trattamento dei dati raccolti dagli assistenti vocali si traduca in un'attività di *Big data analytics*, ossia in un procedimento di raccolta e analisi di grandi volumi di dati (*Big Data*)[30]. Fra questi, i tre principi tra loro strettamente connessi della minimizzazione dei dati trattati (art. 5, par. 1, lett. c) GDPR), della limitazione della loro conservazione (art. 5, par. 1, lett. e) GDPR) nonché della limitazione delle finalità del trattamento (art. 5, par. 1, lett. b) GDPR): non è infrequente che spesso si assista a raccolte di dati personali in notevoli quantità, sicuramente eccessive rispetto alle finalità del trattamento[31], con la frequente possibilità che questi vengano, peraltro, conservati oltre il necessario.

---

systems for public transport, in *International Data Privacy Law*, 2015, 309 ss.

[27] Fra questi, i minori. In proposito, cfr. le preoccupazioni espresse da E. Palmerini, *Dalle smart cities allo scoring del cittadino*, cit., 25. Sulla vulnerabilità della posizione dei minori in merito al trattamento dei loro dati personali operato anche da oggetti *smart*, v. inoltre A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019, spec. 5 ss. e 57 ss.

[28] Sulle profonde trasformazioni legislative vissute dal settore, *in primis* legate all'entrata in vigore del Reg. Ue 679/2016, c.d. GDPR, v. in generale G. Finocchiaro, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in Id. (a cura di), L*a protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2017, 5 ss.

[29] Lo riporta lo studio della Commissione europea, datato gennaio 2018, *The rise of Virtual Personal Assistants*, il cui testo è reperibile nel sito webec.europa.eu.

[30] Particolarmente significative, in materia, due relazioni del Garante della privacy inglese (Information Commissioner's Office, ICO), *Big data, artificial intelligence, machine learning and data protection, 2017,* e *Anonymisation: managing data protection risk, code of practice*, 2012, reperibili entrambe sul sito web dell'Autorità.

[31] Sulla problematicità delle situazioni — quali quelle qui in considerazione — in cui le informazioni sono inferite dai dati, tale che la finalità del trattamento non è chiara fin dal principio, ma si va definendo con il trattamento stesso e dunque non può essere comunicata all'interessato, v. G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, in U. Ruffolo - E. Gabrielli (a cura di), *Intelligenza artificiale e diritto*, cit., 1675.

Di fronte a siffatto contesto, neppure l'anonimizzazione[32], anch'essa prevista dal regolamento, e costituente una misura di protezione dei dati personali, a sua volta coerente con il principio di minimizzazione, dimostra particolare efficacia[33]. Premesso che l'anonimato del dato è di per sé un parametro relativo, in quanto correlato alla collegabilità del dato all'interessato, che a sua volta dipende da circostanze specifiche (il soggetto che opera il collegamento, il contesto in cui questi opera, le modalità con le quali il trattamento è eseguito ...)[34], proprio rispetto a grandi volumi di dati raccolti da una pluralità di fonti, le pratiche di anonimizzazione risultano particolarmente inadatte, dal momento che l'incrocio di dati consente un'alta possibilità di re-identificazione dell'interessato[35], vanificando l'anonimato stesso.

Va inoltre tenuta in debita considerazione la circostanza per cui gli *speaker* intelligenti sono idonei a raccogliere e trattare non solo dati che costituiscono caratteristiche personali dell'utilizzatore (sesso, età, ecc.), ma anche informazioni che rientrano fra le categorie particolari *ex* art. 9 GDPR[36], come i dati sanitari (si pensi a uno *smart assistant* istruito per ricordare l'orario di assunzione di farmaci) e soprattutto i dati biometrici[37]. L'attivazione e/o operatività dello *speaker* stesso dipende infatti dal comando vocale; se poi lo *smart assistant* è dotato anche di videocamera lo stesso raccoglierà dati quali la conformazione dell'iride e le espressioni del volto, dalle quali ricavare persino stati emozionali, e sarà in ogni caso capace di geolocalizzare l'utente.

Come noto, i dati biometrici sono una tipologia di dati personali connotata da peculiarità intrinseche, in cui si verifica quella sostanziale coincidenza fra persona e dato che rende il corpo del soggetto strumento per la sua identificazione, con le conseguenti possibili incidenze sull'identità stessa della persona[38]. Inoltre, i dati biometrici sono atti a rivelare caratteristiche uniche del soggetto, tanto da essere i soli dati personali a consentire un'identificazione univoca della persona[39]. Se in generale, le tecnologie bio-

---

[32] Sull'anonimizzazione in generale, e sulle incertezze relative al concetto di identificabilità dell'interessato, cfr. E. Pellecchia, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, 360 ss.

[33] Specificamente sull'anonimizzazione e i rischi di re-identificazione nel contesto dell'*IoT* e dei *Big Data*, v. F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), cit., 1222-23, A. Mantelero, *La* privacy *all'epoca dei* Big Data, ivi, 1190-91. Sulle difficoltà legate all'anonimizzazione nel contesto dei *Big Data* cfr. anche G. De Gregorio, R. Torino, Privacy, *protezione dei dati personali e* Big Data, in E. Tosi (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, cit., 474-5.

[34] G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, cit., 1675.

[35] F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., 1219.

[36] G. De Gregorio - R. Torino, Privacy, *protezione dei dati personali e* Big Data, cit., 470-1 evidenziano per vero come perda di significato anche la distinzione fra dati personali e categorie particolari di dati, in merito alla *Big Data Analytics*, laddove quindi vengano raccolti e trattati grandi volumi di dati, e laddove vi sia la possibilità di inferire dati personali da dati rientranti nelle categorie particolari e viceversa.

[37] Sui dati biometrici v. M. Pulice, *Sistemi di rilevazione di dati biometrici e* privacy, in *Lav. giur.*, 2009, 994 ss., e, da ultimo, le riflessioni di R. Ducato, *I dati biometrici*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 1285 ss. (sulla loro definizione e collocazione normativa, prima e dopo l'avvento del GDPR, cfr. in particolare 1294).

[38] Al riguardo, v. le riflessioni di S. Bisi, *Il corpo come* password*: alcune considerazioni in tema di sistemi di autenticazione biometrica*, in *Ciberspazio e dir.*, 2005, 3 ss.

[39] Cfr. L. Greco - A. Mantelero, *Industria 4.0, robotica e* privacy-by-design, cit., 883 ss.

metriche apportano consistenti vantaggi pratici, poiché consentono il riconoscimento automatizzato dei soggetti e incentivano la semplificazione di una pluralità di procedure, anche nell'esercizio delle attività quotidiane[40], dall'altro lato, i rischi che si profilano per l'interessato, connessi ad un utilizzo illegittimo o inappropriato dei dati biometrici, divengono particolarmente consistenti[41]: dai pericoli connessi al furto di identità[42] ai rischi correlati all'idoneità, propria delle tecniche biometriche, di consentire rilevazioni a distanza degli interessati, o di rappresentare la base per trattamenti discriminatori[43]. Ove l'obiettivo prioritario degli *smart assistant* sia la profilazione dell'utente a fini commerciali, per l'invio in particolare di pubblicità comportamentale, il trattamento dei dati sanitari e biometrici apre poi scenari molto più delicati. Il rischio che si prospetta è legato alla presenza di *bias*, per tale intendendo quelle distorsioni che gravano le decisioni assunte da sistemi informatici automatizzati che «discriminano sistematicamente e ingiustamente certi individui o gruppi di individui a favore di altri», negando opportunità o generando risultati indesiderati per motivi irragionevoli o inappropriati[44]. La profilazione è espressamente definita dall'art. 4 (4) e regolata nell'art. 22 del GDPR, mentre il principio di non discriminazione non è sancito esplicitamente dal GDPR. Tuttavia, a parte la sua valenza di principio generale a fondamento delle carte europee[45], come puntualmente osservato, a partire dal considerando n. 71 dello stesso — laddove si stabilisce che è opportuno che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate che tengano conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impediscano tra l'altro effetti discriminatori — si ricava l'esistenza di ulteriore principio fondamentale, definito «latente» nella trama normativa, di «non discriminazione algoritmica», da riferirsi non solo alla profilazione, ma anche a qualsiasi altra forma di algoritmo predittivo[46]. Si tratta di una problematica complessa da risolvere, rispetto alla quale anche le soluzioni avanzate si moltiplicano. Da un lato si propone il ricorso all'intervento normativo atto a regolare i processi decisionali in cui siano coinvolti algoritmi. Questo implicherebbe un'estensione dell'oggetto della disciplina giuridica, che dovrà rivolgersi a entrambi i profili della decisione algoritmica: un profilo definito «interno», concernente il fun-

[40] Per una ricognizione dei settori di operatività delle tecniche biometriche, cfr. R. Ducato, *I dati biometrici*, cit., 1286.

[41] Ivi, 1287.

[42] V. S. Bisi., *Il furto d'identità: panoramica attuale e prospettive giuridiche*, in *Ciberspazio e dir.*, 2004, 303 ss.

[43] Sui rischi di discriminazione derivanti precipuamente dal trattamento di dati biometrici, che possono riguardare anche i lavoratori, v. A. Pierucci, *Videosorveglianza e biometria*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, 1627 ss., e M. De Bernart, *Art. 114, Garanzie in materia di controllo a distanza*, in E. Caravà - R. Sciaudone (a cura di), *Il codice della privacy - Commento al d.lgs. 196/2003 e al d.lgs. 101/2018*, Pisa, 2019, 575 ss.

[44] Così B. Friedman - H. Nissenbaum, *Bias in Computer Systems*, in *14 ACM Transactions on Information Systems*, 1996, 332 ss. Cathy O'Neil usa l'efficace espressione «Armi di distruzione matematica», che dà il titolo al suo scritto tradotto da Cavallini e edito nel 2016 da Bompiani.

[45] Ci si può limitare in questa sede a citare il «Manuale di diritto europeo della non discriminazione» edito nel 2011 ad opera della Corte europea dei diritti dell'uomo e dell'Agenzia dell'Unione europea per i diritti fondamentali.

[46] A. Simoncini, *L'algoritmo incostituzionale*, cit., 84 osserva ulteriormente come se anche l'algoritmo sia conoscibile e comprensibile, esso può essere di per sé discriminatorio e dunque incostituzionale.

zionamento dell'intelligenza artificiale, rispetto al quale occorrerà dettare regole volte ad evitare che il sistema possa generare decisioni discriminatorie; e un profilo definito «esterno» al funzionamento dell'intelligenza artificiale, relativo al peso che l'algoritmo esplica sulla decisione finale, e al possibile intervento umano in chiave mitigatrice e di controllo[47].

Dall'altro lato, vi è invece chi, partendo dal presupposto per cui non sia pensabile che gli sviluppatori degli algoritmi possano definire in maniera autoreferenziale e senza rischio di distorsioni i valori codificati negli algoritmi impiegati per governare la società, prospetta non un intervento legislativo, ma piuttosto l'adozione di un approccio partecipativo al processo di analisi del rischio, quale mezzo idoneo anche a consentire la piena attuazione del diritto dei consociati a prendere parte alle decisioni che li riguardano[48]. In tale ottica, si propone pertanto l'ampliamento della valutazione del rischio anche alla partecipazione di comitati di esperti o comitati etici, in grado di rappresentare le istanze sociali insite nelle soluzioni tecnologiche elaborate[49].

Quale che sia la soluzione preferibile, emerge con evidenza che il problema di fondo si traduce sul piano della programmazione e "*design*" dei modelli algoritmici e delle soluzioni tecnologiche che di quei modelli fanno applicazione.

4. Verso una concretizzazione della *privacy by design*: le recenti indicazioni del Garante

Dinanzi alle rilevate difficoltà, una soluzione "a monte" potrebbe essere di tipo "progettuale" e consistere nel compiere opportune scelte appunto di progettazione del programma di assistenza vocale. Così, esso dovrà essere strutturato ad esempio sulla minimizzazione dei dati raccolti, o sull'uso di tecniche di crittografia e/o pseudonimizzazione, per quanto possibile, nella trasmissione degli stessi all'*Internet Service Provider*; e ancora dovrà attivarsi solo quando riconosca l'apposito comando vocale dell'utente primario, escludendo dunque la raccolta e il trattamento di dati riguardanti altri soggetti[50] e dovrà consentire all'utente la possibilità di programmare determinate modalità di funzionamento.

Si tratta di una direzione, quella incentrata sulla progettazione, incoraggiata anche dalla Scheda informativa diffusa dal Garante per la protezione dei dati personali nel

[47] G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, 202, e P. Zuddas, *Intelligenza artificiale e discriminazione*, in *Consulta Online*, 16 marzo 2020, 11.

[48] A. Mantelero, *La gestione del rischio nel GDPR, limiti e sfide nel contesto dei* Big Data *e delle applicazioni di* Artificial Intelligence, in A. Mantelero - D. Poletti (a cura di), *Regolare la tecnologia, il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 304.

[49] A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Computer Law & Security Review,* 34(4), 2018, 754 ss.

[50] Con riguardo proprio ai *voice assistants* C. Hoofnagle, *Designing for Consent*, in *EuCML*, 2018, 167, ove si afferma che «[t]echnology may evolve to solve the problem of the secondary user consent. For instance, Amazon already has "voice profiles" that could evolve to the point that Alexa will only "listen" to those it recognizes».

marzo 2020, relativa proprio agli *smart assistant*[51]. Tale documento contiene alcune raccomandazioni, rivolte agli utenti, finalizzate ad un migliore utilizzo degli assistenti vocali. Alcune delle precauzioni formulate appaiono, per vero, assai semplicistiche e manifestano un eccessivo affidamento sulle capacità di discernimento dell'utilizzatore dello *speaker*. Fra queste «Informati sempre su come vengono trattati i tuoi dati» e «Non dire troppe cose allo *smart assistant*»: indicazioni che presumono la possibilità di conseguire un'informazione e una conoscenza di buon livello circa il funzionamento dello *speaker*, per vero raramente verosimili nell'utenza.

Altre raccomandazioni, invece, alludono, ben più significativamente, alle plurime modalità, in termini di operatività, dello *smart assistant* stesso. Fra esse «Decidi quali funzioni dell'assistente digitale mantenere attive[52]», «Disattiva l'assistente digitale quando non lo usi»: simili indicazioni presuppongono, oltre a un livello minimo di conoscenza da parte dell'utente, che l'assistente vocale offra concretamente la possibilità di impostare tali modalità determinando le relative opzioni.

L'adozione di una soluzione di tipo "progettuale", come è stata definita, consentirebbe l'immissione sul mercato di un prodotto o servizio che sia già stato testato non solo come efficiente (ad esempio sul versante energetico) e come sicuro[53], ma anche come conforme alla normativa, dal punto di vista dei trattamenti dei dati.

Verrebbe così a concretizzarsi pienamente la *privacy by design*[54] di cui al GDPR stesso (art. 25); e la *data protection* acquisirebbe un ruolo autonomo appunto nel *design* — inteso come progettazione ma anche come applicazione di opportune *business policies* o strategie organizzative[55] — del programma/dispositivo. Da ciò deriverebbe anche un significativo incoraggiamento, in favore dei produttori, verso l'adozione di criteri di tipo proattivo, anziché reattivo, nell'ottica appunto di prevenire potenziali lesioni ai danni degli interessati[56].

---

[51] La scheda, datata 4 marzo 2020, è reperibile nel sito web dell'Autorità.

[52] La scheda in questione fa espresso riferimento all'opportunità di disattivare funzioni particolarmente "invasive", quali l'invio di messaggi, la pubblicazione sui social o il compimento di acquisti *online*, ovvero, in alternativa, alla possibilità, sempre che sia contemplata dal programma, di inserire una *password* per autorizzare l'attivazione di simili funzioni solo su specifica richiesta dell'utente.

[53] La disciplina della sicurezza generale dei prodotti è contenuta nella direttiva 3 dicembre 2001, n. 95, attuata nel nostro ordinamento giuridico dal d.lgs. 21 maggio 2004, n. 172, poi confluito negli artt. 102 ss. cod. cons. In particolare, secondo il disposto dell'art. 104, c. 1, cod. cons., i produttori possono immettere sul mercato soltanto prodotti sicuri. Con specifico riguardo al tema della sicurezza nel settore della robotica intelligente e degli algoritmi, v. M. Gambini, *Algoritmi e sicurezza*, in *Giur. it.*, 2019, 1726 ss.

[54] Sul rilievo della *privacy by design*, cfr. A. Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019, 211 ss., la quale, sebbene a proposito dei servizi *online*, evidenzia la necessità di adottare soluzioni — riconducibili proprio al paradigma della *privacy by design* — che, adottando un approccio «*user-centric*», rafforzino il potere decisionale dell'interessato, non valorizzato invece dalle soluzioni incentrate sul rilascio del consenso.

[55] Cfr. F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, cit., 1236.

[56] E. Tosi, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo* Codice Privacy, cit., 40.

5. L'analisi dei rischi e il sistema delle certificazioni

D'altronde, la *privacy by design* è un principio strettamente legato all'analisi del rischio, che a sua volta rappresenta un vero e proprio caposaldo del GDPR. Dal momento che spesso né i titolari né i responsabili del trattamento[57] posseggono però gli strumenti adeguati per operare questa analisi, come è stato proposto, si tratterebbe di traslare l'obbligo di effettuare l'analisi stessa, in modo che i rischi che derivano dai trattamenti operati, nel caso in esame dagli *smart assistant*, siano necessariamente e previamente valutati ad opera di terzi, in maniera sostanzialmente analoga a quanto già avviene in materia di sicurezza dei prodotti[58]. Tali terzi potrebbero essere, come suggerito, le Autorità garanti stesse[59].

In questa prospettiva, si osserva che la valutazione del rischio si sposterebbe, almeno parzialmente e indirettamente, anche a carico del produttore/fornitore del servizio/prodotto *smart*, che verrebbe ad esempio ad essere gravato dell'obbligo di procurarsi idonea certificazione.

È, in effetti, altamente probabile (ed anche auspicabile) che nel contesto in questione un ruolo operativo importante venga assunto dalle certificazioni di cui agli artt. 42 ss. GDPR, ad oggi non ancora operanti nel nostro Paese, ma verso cui si sono ormai mossi i primi passi: la convenzione firmata in data 20 marzo 2019 tra Accredia e l'Autorità Garante, intervenuta subito dopo la pubblicazione del report finale della Commissione europea sui meccanismi di certificazione[60] ha impegnato i due soggetti ad uno scambio di informazioni sulle attività di accreditamento e sulle certificazioni previste dal GDPR. Nello specifico, ad Accredia è affidato il compito di attestare la competenza degli organismi in conformità alla norma UNI CEI EN ISO/IEC 17065, per la certificazione dei prodotti e servizi, e in base ai «requisiti aggiuntivi» che saranno individuati dal Garante a partire dalle Linee guida comuni elaborate dal Comitato europeo per la protezione dei dati personali. Sicuramente, il meccanismo delle certificazioni contribuirà all'identificazione dei rischi, nell'intento di individuare le migliori prassi per attenuare gli stessi e dovrebbe dunque prevenire la verificazione dei relativi danni.

Un'importanza significativa, su un piano distinto ma collaterale, è destinata ad essere assunta dalla normativa in tema di *cybersecurity*, dopo l'approvazione della direttiva 2016/1148 (c.d. direttiva NIS, recante misure per un livello comune elevato di sicurez-

[57] È pur vero che gli stessi soggetti del trattamento sono, in contesti tecnologicamente avanzati, di ardua individuazione, e la scansione operata dal GDPR dagli stessi possa apparire semplicistica. Sul punto, v. A. Mantelero, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it.,* 2019, 2779. Pone in luce le relative difficoltà individuando una vera e propria concatenazione di trattamenti, F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 44 ss. e 76-77.

[58] V. A. Mantelero, *Responsabilità e rischio nel Reg. Ue 2016/679*, cit., 149, e F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things*,* cit., 1225, che, nella stessa ottica, valorizza il ruolo del c.d. *Data Protection Impact Assessment* (DPIA).

[59] Cfr. A. Mantelero, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer law & security review*, 2014, 643 ss., spec. 661 ss., che si pronuncia a favore della rivitalizzazione del modello autorizzatorio impiegato dalle prime generazioni di normative sui dati personali.

[60] Cfr. il *Final report* della Commissione europea del febbraio 2019 *Data Protection Certification Mechanisms under Articles 42 and 43 of the General Data Protection Regulation* (GDPR) (EU) 2016/679 (*Study on*).

za delle reti e dei sistemi informativi dell'Unione). Anche se questa normativa riguarda un rischio diverso da quello della *Data Protection*, ossia il rischio dell'interruzione o dell'attacco *cyber* al servizio, nel caso del *Cloud computing* il rispetto di essa e l'acquisizione della certificazione europea di *cybersecurity* rafforzerà l'affidabilità del fornitore, specie quando questi si avvalga a sua volta di servizi (ad esempio di stoccaggio delle informazioni) forniti da ulteriori terzi[61]. Non vi è dubbio che gli *smart assistant* rientrino a pieno titolo in questo contesto.

In effetti, il GDPR ha inteso attribuire un ruolo fondamentale proprio agli strumenti di *soft law*[62]: codici di condotta e certificazioni *in primis*. Dall'art 42.1 GDPR risulta infatti evidente come agli Stati membri, alle autorità di controllo, al comitato e alla commissione, sia attribuito il compito di "incoraggiare", a livello di Unione Europea, meccanismi di certificazione della protezione dei dati allo scopo di dimostrare la conformità al regolamento. L'istituzione di meccanismi di certificazione, sigilli e marchi di protezione dei dati rappresenta — o meglio, dovrà rappresentare — un importante strumento di autoregolamentazione privata anche nel settore della *data protection*. Come ulteriormente osservato su un piano più generale, con l'avvento del GDPR, il ruolo delle Autorità di controllo e vigilanza è profondamente mutato in direzione espansiva: esse, nel contesto della società digitale, non si limitano infatti alla mera vigilanza sul rispetto delle norme, bensì devono necessariamente svolgere anche un «ruolo proattivo» nella direzione della protezione concreta dei diritti dei soggetti coinvolti[63]. Tale impianto appare perfettamente in linea proprio con l'esigenza che la protezione dei dati personali venga garantita fin dalla progettazione dei trattamenti, complessivamente intesa nell'accezione di predisposizione, ma anche applicazione di opportune strategie organizzative, conformemente alla tecnica della *privacy by design*.

Nell'assetto del regolamento 2016/679, la centralità degli obblighi che gravano su titolare e responsabile del trattamento assegna alle certificazioni il ruolo non certo di produrre l'effetto di *discharge* di tali obblighi[64], ma piuttosto di agevolare nella dimostra-

---

[61] V. in argomento G. Vaciago, *L'attuazione della Direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi: i punti di contatto con il Regolamento UE 2016/679*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 1147 ss., il quale osserva come in proposito assumerà un'importanza fondamentale l'applicazione del regolamento volto a creare un quadro europeo per la certificazione della sicurezza informatica di prodotti ICT e servizi digitali, c.d. Cybersecurity Act, che idealmente si colloca dopo l'approvazione della Direttiva NIS del 2016. Il Cybersecurity Act mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali, oltre che a rafforzare il ruolo dell'ENISA. Esso è entrato in vigore il 27 giugno 2019. Sul tema, più in generale, v. inoltre A. Contaldo - L. Salandri, *La disciplina della cybersecurity nell'Unione Europea*, in A. Contaldo - D. Mula - *Cybersecurity Law*, Pisa, 2020, 1 ss.

[62] La cui non vincolatività non è considerata tale da mettere a rischio quanto meno l'obiettivo dell'armonizzazione da G.M. Riccio, F. Pezza, *Certification Mechanism as a Tool for the Unification of the Data Protection European Law*, in *Medialaws*, 2018, 252.

[63] F. Pizzetti, *Codici di condotta, certificazioni, sigilli, marchi e altri poteri di* soft law *previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in A. Mantelero - D. Poletti (a cura di), *Regolare la tecnologia*, cit., 78.

[64] Come ribadito anche dalla versione definitiva dell'allegato 2 delle Linee guida sulla certificazione del Comitato europeo per la protezione dei dati, aggiornate al 4 giugno 2019.

zione della *compliance* alla normativa europea[65], al punto che le certificazioni vengono definite come veri e propri *accountability tools*[66]. Le certificazioni saranno rilasciate — una volta che il relativo meccanismo diverrà operativo — oltre che da autorità indipendenti, da organismi privati accreditati, chiamati a verificare la conformità del trattamento a criteri approvati alle autorità nazionali o dal Comitato europeo, nell'ottica, in questo secondo caso, di pervenire ad un vero e proprio «sigillo europeo per la protezione dei dati»[67]. Sicuramente, il meccanismo delle certificazioni contribuirà all'identificazione dei rischi, nell'intento di individuare le migliori prassi per attenuare gli stessi[68] e dovrebbe dunque prevenire la verificazione dei relativi danni.

Nella direzione individuata, la nozione di sicurezza del servizio/prodotto da tenere a riferimento non sarebbe più la mera sicurezza informatica[69] o la sicurezza del solo processo di trattamento dei dati, ma, in un'ottica più ampia, la sicurezza che deriva dalla garanzia del rispetto dei diritti e delle libertà fondamentali della persona, che dall'operatività di quel servizio/prodotto possono essere compromessi[70]. L'analisi del rischio finirebbe in tal modo per "entrare" già dentro il prodotto o il servizio fornito all'utente, il quale non dovrebbe quindi preoccuparsi (sempre che sia in grado di farlo) di comprendere la reale incidenza del funzionamento del programma o dispositivo acquistato — nel caso qui considerato l'assistente vocale — sulla protezione dei propri dati personali.

[65] V. D. Poletti - M.C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. Tosi (a cura di), Privacy *digitale*, cit., 376 ss.

[66] Cfr. ancora ivi, 379 e G.M. Riccio - F. Pezza, *Certification Mechanism as a Tool for the Unification of the Data Protection European Law*, cit., 256 ss.

[67] S. Sileoni, *I codici di condotta e le funzioni di certificazione*, in V. Cuffaro - R. D'Orazio - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., 924 e D. Poletti - M.C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, cit., 410.

[68] Considerando 77 GDPR.

[69] E. Tosi, Privacy *digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice* Privacy, cit., 52, propone un approccio integrato che consideri sia le istanze della *privacy* che quelle della *cybersecurity*.

[70] A. Mantelero, *La gestione del rischio nel GDPR*, cit., 305.

Processo penale e rivoluzione digitale: da ossimoro a endiadi?*

Serena Quattrocolo

Abstract

Queste brevi riflessioni mettono a fuoco i principali aspetti problematici, fino ad ora emersi, dell'impatto della rivoluzione digitale sulla sfera del processo penale. In particolare, tre sono gli aspetti qui segnalati. Gli effetti della rivoluzione digitale sono intanto considerati sotto il profilo dell'attività investigativa di ricerca della prova, con particolare riguardo allo sfruttamento dell'enorme potenziale intrusivo di certi strumenti digitali. In secondo luogo, l'attenzione si porta sull'impiego processuale di dati generati automaticamente - attraverso algoritmi e, più in generale, modelli computazionali – il cui vaglio di attendibilità si scontra con il tradizionale diritto probatorio. Da ultimo, viene considerata l'ampia gamma di rischi insiti nell'uso di modelli computazionali di ausilio alla decisone giurisdizionale, in qualsiasi fase del procedimento essa sia adottata.

The paper focuses on the main issues related to the impact of the digital turn and the use of algorithms and computational models in the realm of criminal proceedings. The analysis encompasses three main topics: the impact of digital technologies as means to intrude individuals' privacy, in gathering evidence; the use of algorithm-generated data, used as evidence in trials; the compliance of computational models, as instruments supporting the decision-making process, with fundamental rights.

Sommario

Keywords

algoritmi - modelli computazionali - procedimento penale - equo processo - prova

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo èstato sottoposto a referaggio anonimo

1. Qualche cenno introduttivo

Nel ricco ciclo di seminari organizzati per gli studenti dell'Università del Piemonte orientale ha trovato spazio, grazie alla sensibilità degli organizzatori, anche un profilo che, solo recentemente, sta conquistando spazio nella riflessione degli studiosi e nell'elaborazione della dottrina. Come sempre accade, i riflessi dei più profondi mutamenti della società si proiettano sulla giustizia penale con un significativo ritardo, ovvero quando quei mutamenti possono considerarsi ormai sedimentati nel sentire comune, tanto da arrivare ad incidere sulla sfera del diritto cui è demandato il presidio degli interessi più essenziali, attraverso la pena[1]. È certamente tempo di riconoscere, infatti, che la rivoluzione digitale in corso da alcuni decenni e fortemente accentuatasi proprio negli ultimi due lustri, pone la giustizia penale e, in primo luogo, il processo penale di fronte ad un cambiamento profondo, sia degli attori sociali, sia degli strumenti con i quali essi operano. È frequente – ed icastico – parlare di "società algoritmica", per riferirsi a quell'ampio fenomeno[2] che coinvolge individui e soluzioni tecnologiche nell'elemento che maggiormente distingue e contraddistingue l'odierna realtà: l'ipertrofica produzione di dati generati automaticamente – per lo più al di fuori del controllo di un agente umano - i quali possono essere impiegati con le più varie finalità, addirittura, appunto, all'interno del procedimento penale[3]. È impossibile ricostruire sinteticamente l'ampio dibattito filosofico sviluppatosi in questi ultimi anni, soprattutto attorno alla teoria di Luciano Floridi, che fotografa il percorso dell'evoluzione umana dalla preistoria alla c.d iper-storia[4]. Un cammino lungo e scandito da periodi storici assai eterogeni, che passa attraverso l'invenzione della stampa per arrivare a certificare l'affermazione - oltre le teorie classiche, westfaliane e poi montesquieuiane, del potere – dell'odierno "potere computazionale", con la sfera di ricadute, ancora per lo più inesplorate, che esso proietta sulla società, sul sapere e, ovviamente, sul diritto[5]. La locuzione "algoritmo", correlata al termine "società", può poi assumere una varietà di significati a seconda del contesto in cui viene utilizzato, con sfumature e variazioni anche considerevoli, spesso non condivise dagli stessi esperti del medesimo settore. Ai limitati fini di queste brevi riflessioni, si prenderanno le mosse dalla definizione offerta da Tarleton Gillespie, nel 2014, che è stata altresì assunta come paradigma dal prezioso studio già pubblicato dal Consiglio d'Europa, *Algorithms and Human Rights* nel dicembre 2017[6]. L'autore afferma: «*algorithms need not be software: in the broadest sense, they are encoded procedures for transforming input data into a desired output, based on specified calcula-*

[1] S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for a European Legal Discussion*, New York, 2020, 3.

[2] Si veda L. Floridi et alii, *AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, 689 ss.

[3] Interessante la lettura proposta da A. Garapon – J. Lassègue, *Justice digitale*, Parigi, 2018, 9 ss., che vede nel digitale una rivoluzione grafica la quale – sulla scia di quelle che in precedenza hanno segnato la storia, come ad esempio il comparire dell'alfabeto greco – sta producendo un impatto epocale sulla comunicazione e sui suoi riflessi.

[4] L. Floridi, *The Fourth Revolution*, Oxford, 2017, *passim*.

[5] M. Durante, *Potere computazionale*, Milano, 2019.

[6] Reperibile alla pagina https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

tions. The procedures name both a problem and the steps by which it should be solved»[7]. Tali "*encoded procedures*" presuppongono la realizzazione e l'impiego di un modello computazionale, che riproduce un fenomeno, prendendo in considerazione tutte le variabili rilevanti e regolandone l'interazione.

Allo stesso modo, anche la locuzione "intelligenza artificiale", spesso usata in queste pagine, assume significati molto vari, a seconda del contesto in cui viene utilizzata. Per le finalità di questo lavoro, la più adatta pare quella contenuta nel EC JRC[8] report sull'intelligenza artificiale, ove si afferma che «"intelligenza artificiale" è un termine generico che si riferisce ad ogni macchina o algoritmo in grado di osservare l'ambiente, imparare e, sulla base dell'apprendimento e delle esperienze pregresse, assumere comportamenti intelligenti o proporre decisioni»[9].

Alla luce di queste due definizioni si può affermare che il fenomeno che stiamo vivendo e che stiamo cercando di analizzare non è, necessariamente, l'affermarsi di una società che delega la scelta alla macchina – come una certa visione distopica spesso suggerisce – ma che, a fronte della discrezionalità insita nell'intuito del singolo, ritiene utile circoscrivere i processi decisori, anche quello giudiziario, in una relazione prestabilita, rappresentata in un modello computazionale, affiancando i risultati di questa alla tradizionale attività umana[10].

In questo contesto, anche la sfera della giustizia penale deve misurarsi con l'effetto del vasto impiego di algoritmi e di intelligenza artificiale in software anche di uso quotidiano, non espressamente sviluppati per essere utilizzati in tale ambito. Infatti, la rivoluzione digitale ha fatto segnare, nell'ultimo decennio, un clamoroso balzo, alimentato da due fattori principali[11]: la diffusione globale di smartphones e altri strumenti di comunicazione telematica che generano quotidianamente, e in modo gratuito, quantità incommensurabili di dati; un aumento esponenziale della capacità computazionale, che consente di processare con tempi e costi assai ridotti rispetto ad alcuni anni fa, quella massa pressoché infinita di dati.

Come anticipato, si possono mettere a fuoco tre aree nelle quali l'impiego di dati generati automaticamente (non necessariamente personali e non necessariamente sensibili), elaborati attraverso modelli computazionali, per finalità legate al processo penale, rischia di porsi in contrapposizione con i principi enunciati nella Costituzione italiana e nelle carte internazionali, a garanzia, tanto di diritti e libertà strettamente attinenti alla sfera personale - come la riservatezza – la cui violazione può essere perpetrata attraverso atti del procedimento penale, quanto, più specificamente, dell'equità del processo penale stesso. Il primo ambito è quello investigativo - dei mezzi di ricerca della prova - nel quale il proliferare di forme di comunicazione digitale ha aperto squarci sempre maggiori di vulnerabilità della riservatezza personale: più informazioni, più

---

[7] T. Gillespie, *The relevance of Algorithms*, in T. Gillespie - P. Boczkowski - K. Foot (eds.), *Media Technologies*, Cambridge US, 2014, 167.

[8] Joint Research Center, presso il servizio Scienza e Conoscenza della Commissione europea.

[9] M. Craglia, *Artificial Intelligence: a European Perspective*. EU Publication Office, Luxembourg, 2018.

[10] Cfr. M. Durante, *Potere computazionale,* cit., 231 ss.

[11] U. Pagallo – M. Durante, *The Philosophy of Law in an Information Society*, in L. Floridi (ed.), *The Routledge Handbook of Philosophy of Information*, New York, 2016, 396 ss.

strumenti di intrusione sono i fattori di un'operazione aritmetica dalle conseguenze impressionanti[12], come dimostrato anche dal recente attivarsi del legislatore processuale penale italiano. Il secondo ambito è quello più propriamente probatorio, investito dall'afflusso di dati generati in maniera automatizzata, fuori dal processo, con scarse se non inesistenti possibilità di verifica processuale della loro attendibilità. Il terzo è quello dell'impiego di modelli computazionali per assistere i diversi soggetti del processo penale nell'assunzione di scelte o nell'effettuazione di valutazioni, sulla base di ricchi o addirittura completi data-base, analizzati attraverso software capaci di stabilire, in tale massa di informazioni, correlazioni e rispondenze.

Per ragioni di coerenza, l'attenzione qui è focalizzata sul procedimento penale e, dunque, sul reato consumato (o tentato, naturalmente) e non sulle considerevoli applicazioni dei modelli computazionali in ambito di predizione e prevenzione del reato[13]. Tale ambito costituisce, ormai, un settore di studio autonomo che, pur ricorrendo alla modellizzazione matematica e all'efficienza dell'intelligenza artificiale, si fonda su considerazioni del tutto extra-giuridiche, legate allo studio dei fenomeni criminosi e dei contesti sociali. Esso rappresenta, dunque, uno scenario estraneo o, quantomeno, precedente a quello del procedimento penale, che si instaura a seguito della commissione del reato.

2. Rivoluzione digitale, investigazione penale e riservatezza

Il tema dell'impiego di software capaci di carpire segretamente informazioni e dati a fini investigativi è ampio e articolato. L'appena ricordata spinta della rivoluzione digitale ha inciso significativamente sulle modalità di investigazione, sempre più massicciamente fondate sull'*hacking*, l'accesso occulto a sistemi di produzione o elaborazione di dati digitali. Le brevi considerazioni che seguono sono basilari e non approfondiscono l'argomento, che meriterebbe un'ampia trattazione autonoma.

L'estrazione, occulta, di informazioni contenute in dati generati automaticamente è divenuta un irrinunciabile strumento investigativo. La gamma di azioni intrusive che possono essere realizzate, ad esempio, attraverso *malwares*, inoculati da remoto nei dispositivi *hardware,* è considerevole. Per *malwares* si intendono vari tipi di *malicious software*, un'ampia gamma di captatori informatici che possono accedere a molteplici funzioni degli apparati digitali in cui vengono inseriti, nascosti all'interno di files o di applicativi apparentemente innocui (c.d. *trojan horses*). Invisibile all'utente che ha in uso l'apparecchio infettato, il *malware* consente varie forme di intrusione nella sfera digitale dell'interessato e, in particolare: a) acquisizione di informazioni scambiate attraverso il mezzo infettato; b) attivazione da remoto di strumenti di geolocalizzazione, ripresa o

[12] Si veda, sul recente caso di cronaca legato al malware Exodus, F. Palmiotto, *Captatori informatici e diritto alla* difesa. Il caso Exodus, in *lalegislazionepenale.eu*, 16.10.2020.

[13] Per un'interessante sintesi, v. F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *Diritto Penale Uomo,* 2019, C. Costanzi, *Big data e garantismo digitale. Le nuove frontiere della giustizia penale nel XXI secolo*, in *lalegislazionepenale.eu,* 21 dicembre 2019.

registrazione audio; c) accesso e manipolazione dei *files* presenti nell'*hardware* infetto[14]. Si tratta di strumenti che vantano una evidente potenzialità investigativa che è stata prontamente sfruttata dagli organi inquirenti, in tutto il mondo, per lo più in assenza di un apposito quadro normativo. Per un verso, infatti, gli operatori e la prima giurisprudenza si sono mossi entro i margini della disciplina esistente, per lo più in tutti gli ordinamenti, per la regolamentazione delle intercettazioni di comunicazioni – ambientali, telefoniche e telematiche – partendo dal (discutibile) presupposto che i *malwares* altro non siano che nuove modalità tecniche di svolgimento di tradizionali mezzi di ricerca della prova, appunto. Per altro verso, le autorità giudiziarie hanno consapevolmente minimizzato l'evidente divario, in termini di intrusività, che i captatori informatici presentano rispetto ai tradizionali strumenti intercettivi[15]. Sul punto, nell'impossibilità di proporre in questa sede un approccio più approfondito, si devono sviluppare due riflessioni. In primo luogo, rinviando all'esaustivo rapporto commissionato dal LIBE Committee del Parlamento europeo in materia di *hacking by law enforcement*[16], dove i profili di tale superiore insidiosità per la sfera di riservatezza degli individui sono dettagliatamente trattati[17], va sottolineata la necessità di una disciplina normativa apposita dei captatori telematici, che non possono essere regolati secondo il paradigma delle tradizionali intercettazioni. Per quanto riguarda l'ordinamento italiano, la situazione normativa è decisamente fluida, poiché a seguito della riforma delegata dalla "legge Orlando" al Governo, sulla materia delle intercettazioni di comunicazioni e sull'impiego dei captatori informatici nel procedimento penale si è inserita una cospicua decretazione d'urgenza, prima con il d.l. 161/2019 (conv. con mod. in l. 7/2020) e, da ultimo, nel contesto dell'emergenza sanitaria, con il d.l. 28/2020, conv. con mod. in l. 70/2020),[18] che hanno segnato una progressiva estensione dell'impiego – pur appositamente regolamentato – del captatore informatico.

In secondo luogo, appare evidente la perdita di significato che i concetti ai quali è ancorata, nel linguaggio costituzionale nazionale e nelle carte internazionali, la tutela della riservatezza, subiscono di fronte a mezzi di ricerca della prova così intrusivi. Domicilio e corrispondenza, architravi delle garanzie costituzionali contro le interferenze statuali, anche investigative, nella sfera personale degli individui, hanno perso signifi-

[14] In argomento, *ex multis*, M. Torre, *Il Captatore informatico*, Milano, 2017, spec. 12-17; M. Pittiruti, *Digital Evidence e processo penale*, Torino, 2017, 69 ss.; S. Signorato, *Le indagini digitali*, Torino, 2018, 237 ss.

[15] In questo senso, M. Daniele, *La prova digitale processo penale*, in *Riv. Dir. Proc.*, 2011, 288: «La loro capacità lesiva della *privacy* è addirittura superiore a quella delle intercettazioni».

[16] Studio commissionato dal Libe Committee del Parlamento europeo e realizzato dal Directorate-General for Internal Policies, *Legal Frameworks for hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices* (reperibile alla pagina *europarl.europa.eu*).

[17] A p. 21 si afferma: «*although the use of hacking techniques will bring improvements in investigative effectiveness, the significant amount and sensitivity of data that can be accessed through these means acts as a stimulus for another key debate: ensuring the protection of the fundamental right to privacy*».

[18] Complesso riassumere brevemente la vicenda italiana. A seguito di una nota decisione delle Sezioni Unite della Corte di cassazione (Cass. pen., sez. un., 1° luglio 2016, n. 26889) un documento sottoscritto da quasi tutti i docenti italiani di diritto processuale penale aveva sollecitato la necessità di uno specifico intervento normativo (v. *penalecontemporaneo.it*, 16 ottobre 2016), avvenuto poi con il d.lgs. 216/2017 (e d.m. 20 aprile 2018), che ha inserito nel codice di procedura penale una specifica disciplina del captatore informatico, ad oggi non ancora entrata in vigore. I recenti interventi hanno poi sempre procrastinato l'entrata in vigore della nuova disciplina, avvenuta nel settembre 2020.

cato, di fronte alla possibilità di produrre, scambiare, conservare – ma anche carpire, intercettare, copiare – dati immateriali in uno spazio che non è più quello fisico. La più o meno consapevole accettazione, generalizzata, di apparecchi digitali che, per le loro ridotte dimensioni, seguono l'individuo ovunque e sempre, rende decisamente impossibile continuare ad applicare la tradizionale distinzione tra luoghi pubblici, luoghi aperti al pubblico e luoghi privati, come il domicilio, nel quale la captazione occulta è consentita solo in via eccezionale, a condizioni ancora più stringenti di quelle previste in via generale[19].

A fronte di un'interferenza, destabilizzante, tra strumenti digitali basati su modelli computazionali e valori essenziali del nostro patrimonio giuridico, il quadro delle garanzie fondamentali, sancite dalla Convenzione europea dei diritti dell'uomo e dalla Costituzione italiana, rappresenta ancora, certamente, la cornice normativa di riferimento. Per un verso, nell'art. 8 CEDU, la Corte di Strasburgo ha individuato dei limiti ben precisi anche all'attività investigativa di analisi e profilazione dei dati,[20] che possono rappresentare un utile parametro per gli ordinamenti nazionali. Per altro verso, la Convenzione stessa lascia intravedere, sullo sfondo, altri principi che possono rappresentare il criterio per stabilire (o ristabilire) i confini del concetto di *fairness* processuale anche nell'era della rivoluzione digitale. L'operazione, però, richiede, quantomeno, la disponibilità e la capacità di uscire dai paradigmi più familiari – i concetti di "domicilio", di "comunicazione", appunto, ma anche di "prova" e di "attendibilità" – per comprendere come essi siano stati riscritti nell'ultimo decennio, per riportarli poi, nell'alveo dei principi fondamentali della cultura giuridica europea.

3. La prova generata automaticamente e i rischi per la parità delle armi

Il secondo profilo di analisi riguarda i mezzi di prova. Se, poco sopra, l'attenzione si è soffermata sui nuovi mezzi di ricerca della prova, la realtà attuale dimostra come, anche senza l'impiego di strumenti di captazione occulta, da tutti i supporti digitali si possono estrarre informazioni di grande rilievo per il procedimento penale. Può trattarsi anche di metadati, che precisano condizioni oggettive riferite alla genesi del dato. Con la crescente rilevanza dell'IoT, può trattarsi di dati generati automaticamente, senza alcun intervento umano nella loro rilevazione, da oggetti di uso quotidiano collegati alla rete internet, come gli assistenti vocali di vario genere o gli elettrodomestici smart. Questi rappresentano, evidentemente, un patrimonio conoscitivo talvolta fondamentale per le indagini e per il procedimento penale: si pensi, ad esempio, al diffuso aspirapolvere Rumba, che immagazzina e conserva dati sui percorsi e sugli ingombri esistenti in ciascuna stanza della casa… L'insieme dei dati rilevati e conservati fornirà

[19] V. ampiamente, S. Signorato, *Le indagini digitali*, cit., 49 ss.

[20] Volendo, U. Pagallo - S. Quattrocolo, *The impact of AI on criminal law, and its twofold aspects*, in W. Barfield - U. Pagallo (eds.), *Research Handbook on the Law of Artificial Intelligence*, Cheltenham, 2018, 391. In generale, v. R. Sicurella - V. Scalia, *Data mining and profiling in the Area of Freedom, Security and Justice*, in *New Journal of European Criminal Law*, 2013, 409 ss.

informazioni determinati agli investigatori che indaghino, ad esempio, su un omicidio avvenuto in una specifica stanza…

La questione che qui si pone come oggetto centrale della riflessione riguarda la verifica dell'accuratezza del dato, generato e/o raccolto esclusivamente attraverso uno strumento digitale. È possibile contestarne l'attendibilità? Oppure la "prova digitale", per la sua natura e per la sua genesi, è oggettivamente impermeabile al confronto dialettico tra le parti nel processo? Tutti gli apparecchi digitali generano dati, attraverso un processo che, basato su algoritmi o, più in generale, modelli computazionali, difficilmente è trasparente: l'elemento conoscitivo che ne traiamo (perché no, a fini processuali?) è generato da un processo di cui possono non essere noti né gli input né i processi elaborativi… Una scatola nera, insomma, dalla quale si estrae qualcosa di utile, spesso, però, senza sapere come.

La metafora, calata nel contesto processuale, esprime l'estrema difficoltà o l'impossibilità di falsificare il dato elaborato da una "black box" se non è possibile accedere al codice sorgente che governa l'algoritmo stesso[21] o se, nonostante la disponibilità del codice sorgente, il processo che ha generato l'*output* non sia verificabile *ex post*. Tale scenario, che assumiamo al momento come valido, rischia di determinare una situazione di squilibrio conoscitivo estremo tra le parti del processo.

Invero, lo squilibrio conoscitivo è fenomeno che si riscontra nel processo penale sin da quando, per la soluzione di casi complessi, si è iniziato a fare ricorso a competenze tecniche, scientifiche o artistiche[22]. Tuttavia, l'ingresso di saperi specialistici nel processo difficilmente è equilibrato, poiché una delle parti - quella pubblica - ha accesso alla scienza e alle tecnologie migliori, anche perché dispone di mezzi economici non limitati. Evidentemente, il fenomeno di *knowledge impairment* non è nuovo e ogni stagione del complicato rapporto tra scienza e processo penale ne ha riproposta una versione più o meno intensa (si pensi al debutto della profilazione del DNA nelle aule di giustizia, o al ricorso alla fMRI per l'accertamento di profili legati all'imputabilità). La prova generata automaticamente, tuttavia, rischia di introdurre una forma estrema di tale squilibrio, poiché il risultato probatorio può essere non criticabile laddove, appunto, l'inaccessibilità del codice sorgente o altre caratteristiche del software non consentano alla parte contro la quale la prova è introdotta nel processo di contestarne l'accuratezza e l'attendibilità[23].

Il tema si innesta, evidentemente, sul cuore del diritto probatorio, le cui regole rappresentano le chiavi del cancello che regola l'accesso delle conoscenze al processo. Per quanto appaia difficile formulare considerazioni generali in materia di prova – geloso appannaggio delle legislazioni nazionali[24], assai restie all'armonizzazione su tale profilo

---

[21] U. Pagallo - S. Quattrocolo, *The impact of AI on criminal law*, cit., 392 ss.

[22] V. A.J. Brimicombe – P. Mungroo, *Algortihms in the Dock: Should Machine Learning Be Used in British Courts?,* Proceedings of the fourth Winchester Conference on Trust, Risk, Information and the Law, 3 maggio 2017.

[23] E. Van Buskirk-V.T. Liu, *Digital Evidence: Challenging the Presumption of reliability*, in *Journal of Digital Forensic Practice*, 1, 2006, 20; C. Chessman, *A Source of Error: Computer Code, Criminal Defendants, and the Constitution*, *Calif. L. Rev.*, 2017, 179 ss.

[24] Si veda l'esplicita affermazione (spesso reiterata) della Corte europea dei diritti dell'uomo in GC, *Gäfgen v. Germany,* ric. 22978/05 (2010), § 162: *«while Article 6 guarantees the right to a fair hearing, it does not*

– l'importanza della questione che si pone spinge a verificare l'esistenza di principi generali che possano guidare la gestione processuale del fenomeno delle prove generate automaticamente.

È noto che né a livello convenzionale, né nel più recente quadro delle direttive europee processuali penali emanate sulla base dell'art. 82, §2 TFUE, si reperisce traccia di un sistema di invalidità[25] della prova ispirato alla tradizione romano-germanica, in cui, a fronte della predisposizione normativa di uno schema legale dell'atto probatorio, si ritrova una sanzione processuale, che "neutralizza" la prova non corrispondente allo schema[26]. Nemmeno si reperisce, nel contesto europeo *lato sensu* inteso, una regola generale di esclusione probatoria dei "frutti dell'albero avvelenato", elaborata dalla letteratura e dalla giurisprudenza nord-americana[27]. Piuttosto, la Corte europea tende a convogliare tutte le valutazioni sull'ammissibilità e sulla utilizzabilità della prova in un generale test di compatibilità con il processo equo[28], inteso come nozione onnicomprensiva che calibra e combina le singole garanzie di dettaglio[29].

Ed è proprio in forza del generale canone del giusto processo e, più in particolare, del principio della parità delle armi, che anche l'ammissione e la valutazione di prove generate automaticamente pare porsi potenzialmente in contrasto con garanzie fondamentali del dettato convenzionale. È noto che, innanzitutto e pur nell'assenza di una esplicita enunciazione nel testo dell'art. 6 CEDU, il principio della parità delle armi è stato modellato dalla giurisprudenza della Corte come architrave, insieme al connesso canone del contraddittorio, dell'equità processuale nel suo complesso[30]. Notoriamente, *equality of arms* non implica una presunta, necessaria identità di facoltà o di posizioni

lay down any rules on the admissibility of evidence as such, which is primarily a matter for regulation under national law».

[25] R. Kostoris (ed.), *Handbook of European Criminal Procedure*, New York, 2018, 58.

[26] L. Bachmaier Winter, *The EU Directive on the Right to Access to a Lawyer: A Critical Assessment*, in S. Ruggeri (ed.), *Human Rights in European criminal Law*, Springer, 2015, 114; A. Cabiale, *I limiti alla prova nella procedura penale europea*, Padova, 2019, 311 ss., M. Caianiello, *To Sanction (or not to Sanction) Procedural Flaws at EU Level? A Step forward in the Creation of an EU Criminal Process*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2014, 317 ss., S. Quattrocolo*, Artificial Intelligence*, cit., 74 ss.

[27] Si veda l'interessante raffronto di S. Thaman*, 'Fruits of the Poisonous Tree' in Comparative Law*, in *Southwestern Journal of International Law*, 2010, 333 ss.

[28] Impossibile riassumere qui l'ampio ventaglio delle posizioni adottate della Corte in un percorso pluridecennale, nel quale l'approccio dei giudici di Strasburgo alla "tainted evidence" è significativamente mutato e non nel senso di un ampliamento delle garanzie dell'imputato. Si rimanda, dunque, in generale ad A. Cabiale, *I limiti*, cit., 87 ss. e, con specifico riguardo al tema qui trattato a S. Quattrocolo*, Artificial Intelligence*, cit., 77 ss.

[29] V. Manes - M. Caianiello, *Introduzione al diritto penale europeo*, Torino, 2020, 217 ss.

[30] Cfr. M. Chiavario, *Art. 6,* in S. Bartole - B. Conforti - G. Raimondi, *Commentario alla convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2002, 192. Si tratta di un'acquisizione risalente nella giurisprudenza di Strasburgo, su cui v. già CEDU, *Neumeister v. Austria*, ric. 1936/63 (1968), § 22 delle motivazioni in diritto, che riconosce la parità delle armi come una caratteristica del dair trial, sulla base di numerose precedenti decisioni e opinioni della Commissione europea, allora incaricata di svolgere un filtro d'accesso alla Corte; CEDU, *Delcourt v. Belgium*, ric. 2689/65 (1970), § 28: *«The principle of equality of arms does not exhaust the contents of this paragraph; it is only one feature of the wider concept of fair trial by an independent and impartial tribunal»* e poi, successivamente, tra le tante, CEDU, *Brandstetter v. Austria*, ric. 11170/84 (1991), § 66; *Ruis-Mateos v. Spain*, ric. 12952/87 (1993), § 63; *Fitt v. UK*, ric. 29777/96 (2000), § 44; *Sabayev v. Russia*, ric. 11994/03 (2010), § 35; *J.M. e altri v. Austria*, ricc. 61503/14, 61673/14, and 64583/14 (2017), § 119.

di cui le parti essenziali del processo debbano sempre fruire, soprattutto laddove si tratti, appunto, di processo penale, il quale è caratterizzato – specialmente nelle sue fasi prodromiche – da un insuperabile squilibrio tra parte pubblica e difesa[31]. In questa connaturata differenza di ruoli istituzionali, il paradigma essenziale della parità delle armi è rappresentato dalla possibilità di presentare i propri argomenti in condizioni che non svantaggino una parte rispetto alle altre[32]. Insomma, il principio esprime nel suo nucleo essenziale e irrinunciabile, un giusto equilibrio tra le parti processuali[33]. Se indubbiamente tale affermazione può apparire per lo più declamatoria, essa va coniugata con più specifiche messe a punto della parità delle armi, come quella scolpita nel *leading case Brandstetter c. Austria*, in cui la Corte ha ribadito che è necessario che ciascuna parte abbia effettiva conoscenza delle allegazioni e delle argomentazioni della controparte e che fruisca della concreta possibilità di contestarle e falsificarle. «*An indirect and purely hypothetical possibility for an accused to comment on prosecution argument*»[34] non soddisfa il parametro convenzionale. All'interno del procedimento probatorio - ambito che la Corte riconosce, appunto, come devoluto alle discipline nazionali - è proprio la possibilità, per tutte le parti e, principalmente, per la difesa, di contestare l'accuratezza della prova a carico ad esprimere il senso proprio del suddetto giusto equilibrio. È stato, infatti, ripetutamente sottolineato che «*it must be examined in particular whether the applicant was given the opportunity of challenging the authenticity of the evidence and of opposing its use. In addition, the quality of the evidence must be taken into consideration, including whether the circumstances in which it was obtained cast doubt on its reliability or accuracy*»[35]. Ciò, invero, è funzionale a realizzare l'obiettivo intrinseco della parità delle armi, ossia consentire a tutte le parti le stesse *chances* di poter convincere il giudice della propria prospettazione dei fatti oggetto di prova[36].

Calando il tema delle prove raccolte e generate in via del tutto automatizzata all'interno del paradigma elaborato dalla Corte europea in lunghi anni di giurisprudenza, emerge un dato rilevante. L'eventuale impossibilità di accedere al codice sorgente o di poter effettivamente comprendere il funzionamento della *black box* che le ha generate, determina un rischio implicito per la parità delle armi, così come intesa dalla richia-

[31] Cfr. Van Dijk – Van Hoof, *Theory and Practice of the European Convention on Human Rights*, 3rd ed., Leiden, 1998, 430 ss.

[32] In questo senso, CEDU, *Kress* v. *France*, ric. 39594/98 (2001), § 72.

[33] J.F. Renucci, *Droit européen des Drotis de l'Homme. Droits aux libertés fondamentaux garantis par la CEDH*, 5a ed., Paris, 2013, 378.

[34] CEDU., *Brandstetter v. Austria*, cit., § 68.

[35] Così, CEDU, *Bykov v. Russia*, cit., § 90, da ultimo ripresa in *Svetina* v. *Slovenia*, cit., § 44, nella quale la questione denunciata dal ricorrente riguardava proprio l'impiego di prove raccolte sulla base di un iniziale, illegittimo (perché non espressamente autorizzato dal locale "giudice istruttore") accesso al telefono della vittima. Posta ancora una volta di fronte al problema dell'applicabilità della teoria dei frutti dell'albero avvelenato, la Corte ha rilevato che le giurisdizioni interne hanno fatto applicazione della contraria dottrina della "inevitable discovery"; tuttavia, poiché la questione della ammissibilità o meno delle susseguenti prove – che, appunto, secondo la Suprema Corte slovena sarebbero state scoperte comunque, a prescindere dall'illegittimo accesso – riguarda in definitiva l'interpretazione di norme interne, la Corte europea si limita ad osservare che le risultanze dell'accesso illegittimo non sono state poste alla base della decisione sulla colpevolezza dell'imputato, fondata, invece, su prove validamente raccolte, secondo la disciplina nazionale.

[36] CEDU, *Martinie* v. *France*, ric. 58675/00 (2006), § 46.

mata giurisprudenza europea. Se l'essenza dell'equità processuale risiede nel pieno diritto di poter provare a convincere, con strumenti efficaci, il giudice della propria ricostruzione dei fatti, anche contestando l'ammissibilità e l'accuratezza della prova, l'impossibilità di verificare *a posteriori* l'*output* di un algoritmo può rappresentare *in nuce* una violazione dell'art. 6, §1 CEDU (a prescindere dall'esistenza di una violazione, a monte, del diritto alla riservatezza).

Occorre dunque verificare se e quali rimedi possono essere utilizzati nel processo per contrastare l'intrinseca mancanza di trasparenza che circonda un dato generato automaticamente[37], difetto di trasparenza che può essere dettato, appunto, dall'impossibilità di rivelare il codice sorgente o dal funzionamento del modello computazionale utilizzato, non concepito per essere verificabile *ex post*.

L'ormai tradizionale risposta al problema dell'opacità[38] dei processi algoritmici e computazionali è la trasparenza[39]. Tuttavia, nell'ambito della trattazione automatizzata dei dati, la trasparenza pare essere divenuta l'unico e determinante parametro di legittimità del trattamento, sostituendosi subdolamente al canone della legalità. Se il software è concepito secondo parametri di trasparenza, la possibilità di validazione o di falsificazione dei suoi *outputs* è più elevata e a questo assunto sembrano ispirati il GDPR, recentemente entrato in vigore, e per certi versi anche la direttiva UE 2016/680, in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali (art. 20), recentemente trasposta anche in Italia con il d.lgs. 51/2018[40].

Tuttavia, la trasparenza non è un concetto autosufficiente, ma si articola in relazione al risultato che si desidera ottenere[41]. Essa, ad esempio, si può raggiungere ottenendo l'accesso al *source code*, agli *inputs* e agli *outputs* del *software*[42]. In primo luogo, però, va precisato che tale accesso non garantisce una generale comprensione del processo che ha generato il risultato, perché soltanto gli esperti informatici possono essere in grado, e non sempre (vedi qui di seguito), di trarne degli elementi significativi e comprensibili. È stato osservato, quindi, che, in ogni caso, si tratta di una trasparenza "mediata"[43] dall'esperto. In secondo luogo, i codici sorgente possono essere sottoposti a segreti commerciali o industriali da parte dei proprietari del

---

37 F. Palmiotto, *The Impact of Algorithmic Opacity on Fair Trial Rights in Criminal Proceedings*, in M. Ebers - M. Canero Gamito (eds.), *Algorithmic Governance and Governance of Algorithms*, New York, 2020, 49 ss.

38 J. Burrell, *How machines think: Understanding opacity in machine-learning algorithms*, in *Big Data and Society*, 1, 2016, 1 ss.

39 M. Hildebrandt, *Profile transparency by design? Re-enabling double contingency*, in M. Hildebrandt - de Vries, *Privacy, Due Process and the Computational Turn*, London, 2013, 239; J. Danaher, *Algorithmic Decision-making and the Problem of Opacity*, in *Computers and Law*, 8, 2016, 29 ss.

40 Pubblicato in G.U. 24 maggio 2018 ed entrato in vigore il 6 giugno 2018.

41 F. Palmiotto, *The Impact*, cit. 52.

42 J.A. Kroll - J. Huey - S. Barrocas - E.W. Felten - J.R. Reidenberg - D.G. Robinson - H. Yu, *Accountable Algorithms*, in *University of Pennsylvania Law Review*, 165(3), 2017, 675.

43 A. Koene - H. Webb - M. Patel, *First UnBias Stakeholders workshop*, 2017, in *unbias.wp.horizon.ac.uk*.

software[44]. In base al diverso atteggiamento dei singoli ordinamenti sul punto[45], si può verificare una ipotesi di impossibilità di accesso ai fini della verifica dell'attendibilità della prova.

Inoltre, nemmeno l'*open source code* – che parrebbe a prima vista la principale garanzia di trasparenza - può garantire la possibilità di un'effettiva giustificazione[46] a posteriori dei risultati prodotti dall'algoritmo, se questo non è stato concepito con criteri, più che di trasparenza, di responsabilità (*accountability*, intesa come possibilità, capacità di dar conto di come i risultati sono stati prodotti, partendo da determinati *inputs*)[47]. Per un verso, nell'ambito della ricerca e della raccolta della prova difficilmente è possibile utilizzare *software open source*, proprio perché l'efficacia dei captatori occulti sta nella segretezza, innanzitutto, del loro operare, ma anche delle loro modalità di funzionamento. Per altro verso, poi, quando il *software* faccia uso di forme anche non particolarmente ricercate di *machine learning*, la validazione *ex post* del risultato può diventare impossibile anche per lo stesso designer, in ragione dei processi di autoapprendimento appunto impiegati dal software.

Tuttavia, l'*explainable AI* è una sfida che vede oggi impegnati studiosi di vari settori, concentrati nel tentativo di arginare la tradizionale aura di opacità algoritmica. Se è vero che la "prova computazionale" esalta e mette in luce il rischio che, in una società basata sulla produzione, sulla comunicazione e sul trasferimento di dati, i soggetti processuali (*in primis*, le parti) vengano fortemente deprivati della loro rilevanza nel procedimento probatorio (dalla raccolta, ma anche dalla valutazione, dalla discussione e dalla valutazione)[48], i tempi sono maturi per esplicitare il rischio e neutralizzarlo. Riconosciuto che, nell'attuale realtà storica, i dati raccolti o elaborati digitalmente rischiano di vedersi garantita una patente di intrinseca attendibilità probatoria, semplicemente perché la verificazione dell'iter che li ha generati è troppo complessa o sfugge, almeno in parte, ad un controllo *ex post*[49] nelle scienze computazionali e nei consolidati principi del sistema processuale penale europeo possono rinvenirsi adeguate reazioni al descritto pericolo.

In primo luogo, come accennato, la conoscenza del problema dell'opacità algoritmica spinge gli esperti del settore a elaborare soluzioni che, pur senza disvelare i codici

---

[44] L'esistenza del segreto commerciale è stata considerata dirimente in un noto caso deciso dalla Corte suprema del Wisconsin, nel 2017; v., *infra*, nt. 56.

[45] Per quanto riguarda l'ordinamento italiano, si sono al momento registrare tre significative pronunce del Consiglio di Stato, le prime due decisamente orientate alla prevalenza dell'interesse pubblico alla trasparenza degli atti amministrativi (Cons. Stato, sez. VI, 8 aprile 2019, n. 2270; Cons. Stato, sez. VI, 13 dicembre 2019, n. 8472) e una terza che, tuttavia, riconosce il ruolo di controinteressato, nel processo amministrativo, al titolare di segreti commerciali del software, poiché la sua sfera giuridica potrebbe subire degli effetti negativi dal disvelamento dei codici sorgente (Cons. Stato, sez. VI, 2 gennaio2020, n. 30).

[46] M. Hildebrandt, *Algorithmic Regulation and the Rule of Law*, *Phil. Trans. R. Soc*, 2018, 1-11.

[47] Cfr. A. Kroll - J. Huey - S. Barrocas - E.W. Felten - J.R. Reidenberg - D.G. Robinson - H. Yu, *Accountable Algorithms*, cit., 662 ss.

[48] C. Chessman, *A Source of Error: Computer Code, Criminal Defendants, and the Constitution*, in *Calif. L. Rev.,* 2017, 179 ss.

[49] S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della giurisprudenza della Corte europea dei diritti dell'uomo*, in *Rev. italo-española dir. proc.*, 2, 2019, 1 ss.

sorgente di un software, ne spieghino in maniera esaustiva, validandolo, il funzionamento[50]: il loro impiego nel processo potrebbe risultare sufficiente a garantire la parità delle armi. In secondo luogo, è possibile pensare che, nella insuperabile necessità di accedere ai codici sorgente, per la verifica della prova, e a fronte di istanze di tutela del segreto commerciale da parte del proprietario del software, si possano elaborare, all'interno delle discipline processuali nazionali, regole di *disclosure* "garantita", ovvero circoscritta all'interno del procedimento penale, pur compatibilmente con il principio di pubblicità del giudizio. In terzo luogo, ove nessuna delle soluzioni precedenti sia percorribile, in ragione delle specifiche qualità del software, e la verifica *ex post* dell'attendibilità della prova risulti impossibile, la via pare segnata verso l'esclusione dell'ammissione o dell'utilizzazione della medesima, sulla scorta della incompatibilità con l'essenza irrinunciabile del processo equo. Pur riconosciuta, infatti, la ritrosia della Corte europea a stabilire delle *exclusionary rules* probatorie[51], nell'evoluzione della giurisprudenza di Strasburgo sulla «*overall fairness of the proceeding*», sembra potersi leggere proprio la soluzione indicata[52].

4. Decisori giurisdizionali e... ausili digitali

Terzo e più complesso profilo di analisi riguarda la sfera di applicazione in talune articolazioni del procedimento penale, di software "predittivi" che possono asseritamente assistere l'autorità giudiziaria in operazioni decisorie. Tali strumenti sono, per ora, più diffusi negli ordinamenti di *common law*, per lo più nella fase dell'esecuzione della pena, anche se non sono pochi gli Stati che vi fanno ricorso per decisioni di *bail*[53] e/o *sentencing*, ovvero in materia di custodia cautelare.

In numerose giurisdizioni degli Stati del Nord America si utilizzano, ormai da tempo, software predittivi per sciogliere prognosi di pericolosità sociale e, in particolare, di rischio di recidivanza. Si tratta di strumenti di *risk assessment* strutturati sulla base di valutazioni psico-criminologiche[54], vietate, nel giudizio di cognizione italiano, dall'art. 220 c. 2 c.p.p. Per ragioni che qui non si possono approfondire, un simile divieto risulta assai raro, nel panorama mondiale, tanto più che in numerosi ordinamenti si è verificato, nel XX secolo, un fenomeno di forte apertura verso le scienze psico-criminologiche, che ne ha fatto, talvolta il centro del sistema sanzionatorio[55]. A prescindere dall'atteggiamento riservato alle scienze psicologiche, permangono a tutt'oggi, nel giudizio pe-

[50] Cfr. A. Kroll - J. Huey - S. Barrocas - E.W. Felten - J.R. Reidenberg - D.G. Robinson - H. Yu, *Accountable Algorithms,* cit., 676, segnalano, per esempio i c.d. sistemi "*zero-knowledge proof*", in grado di fornire risposte esaustive senza rivelare necessariamente i dati posti alla base del funzionamento di un modello.

[51] A. Cabiale, *I limiti*, cit., 89.

[52] S. Quattrocolo, *Artificial Intelligence*, cit., 96.

[53] Molto noto, poichè applicato in 39 giurisdizioni degli Stati Uniti, il *Public Safety Assessment:* strumento attuariale basato su 9 fattori, tra cui età, accusa e precedenti/carichi pendenti.

[54] Per una completa panoramica sull'evoluzione degli strumenti di risk assessment, G. Zara - D. P. Farrington, *Criminal Recidivism: explanation, prediction and prevention*, Oxon, 2016, 148 ss.

[55] S. Quattrocolo, *Artificial Intelligence*, cit., 144 ss.

nale, numerosi momenti in cui l'autorità giudiziaria è chiamata a svolgere valutazioni di tipo prognostico-predittivo, gravando il decisore di una prognosi estremamente complessa. Non solo il problema è rappresentato dalla indecifrabilità del comportamento umano, ma anche dalla tendenziale scarsità di informazioni disponibili, soprattutto laddove sia intervenuta una dichiarazione di colpevolezza da pare dell'imputato a porre fine all'attività istruttoria: soprattutto negli ordinamenti in cui il ricorso al *plea bargaining* sia massiccio, l'ausilio di strumenti algoritmici di *risk assessment* risulta particolarmente appetibile. Quindi, come accennato in precedenza, prima ancora che a una delegazione di scelte decisorie alla macchina, siamo di fronte alla riduzione – auspicata e cercata! - della discrezionalità del singolo, attraverso l'ausilio della "decisione algoritmica".
I lettori che hanno un minimo di familiarità con questi temi hanno già riconosciuto, in questi cenni, il richiamo ad un noto caso deciso dalla Corte Suprema del Wisconsin nel 2017[56], ove, da tempo, è stato adottato uno strumento attuariale di *risk assessment* chiamato COMPAS[57]. Tale strumento, ben noto agli studiosi di fenomeni di recidivanza, si basa sia su informazioni ottenute direttamente dall'imputato, in un'intervista, sia sul certificato del casellario e dei carichi pendenti, le quali vengono elaborate attraverso un modello computazionale in relazione a dati statistici di controllo, riferiti a un campione di popolazione non necessariamente corrispondente a quella dello Stato in cui si svolge il procedimento. Sul piano predittivo, quindi, lo strumento prevede il rischio di ricaduta violenta, in rapporto al dato statistico, senza tuttavia offrire una spiegazione di tale rischio.

---

[56] *State v. Loomis*, 881 NW 2d 749 (Wis 2016). Per un commento alla sentenza v. *Criminal Law – Sentencing Guidelines – Wisconsin Supreme Court Requires Warnings before Use of Algorithmic Risk Assessment in Sentencing – State v. Loomis*, in *Harward Law Review*, 2017, 1530 ss. Nella vicenda richiamata, sulla base del *risk assessment*, la corte locale aveva inflitto la pena della reclusione a sei anni (senza *parole*), e cinque anni di *extended supervision*, pena certamente elevata se rapportata ai fatti, marginali, per cui egli si era dichiarato colpevole, destando l'attenzione di tutti i media nazionali e di molti stranieri.
Nell'ambito di una istanza di *post-conviction release*, decisa dalla *circuit court* locale, l'imputato contestava diversi profili di violazione del principio del *due process*. Il consulente tecnico presentato dalla difesa evidenziava alcuni aspetti critici legati all'uso in fase deliberativa della pena dello strumento di *risk assessment*.

[57] *Correctional Offenders Managment Profilying for Alternative Sanctions*. Si tratta di uno strumento attuariale che valuta il rischio statico, non dinamico: infatti, gli strumenti attuariali non spiegano il recidivismo, si limitano a segnalarlo, valutando i fattori di rischio attraverso statistiche ufficiali e prospettive teoriche comprensive. Sul mercato, lo strumento è commercializzato in forma di software, da Northpointe inc. che ne detiene i diritti e le licenze commerciali. Gli strumenti di *risk assessment*, però, non sono necessariamente dei software. Nel panorama italiano l'applicazione del *risk assessment* non ha ancora trovato un riconoscimento ufficiale all'interno del sistema della giustizia penale (v. però nt. 43); tuttavia, esso è molto diffuso in altri ordinamenti e da tempo oggetto di studi anche da parte di autori italiani: G. Zara, F. Freilone, *Psychological assessment*, in B.A. Arrigo (a cura di), *The SAGE Encyclopedia of Surveillance, Security, and Privacy*, Thousand Oaks, 2018, 830 ss; G. Zara, *La validità incrementale della psico-criminologia e delle neuroscienze in ambito giuridico*, in *Sistemi intelligenti,* 2, 2013, 311. Le teorie psicologiche applicate dal COMPAS sono illustrate in v. T. Brennan – W. Dietrich – B. Ehret, *Evaluating the Predictive Validity of the Compas Risks and Needs Assessment System*, in *Criminal Jusice and Behaviour*, 2009, 21 ss. (Brennan risulta aver guidato anche gruppi di ricerca per conto del produttore del medesimo software). Esistono numerosi studi, di segno non univoco, sull'attendibilità del COMPAS e sui rischi di implicit bias ad esso connessi: T. L. Fass - K. Heilbrun - D. Dematteo; R. Fretz, *The LSI-R and the COMPAS: Validation Data on Two Risk-Needs Tools*, in *Crim. Just. & Behavior*, 35, 2008, 1095 ss., i quali concludevano per un evidente fattore di discriminazione su base razziale dei risultati del software COMPAS; J. Skeem - J. Eno Louden, *Assessment of Evidence on the Quality of COMPAS*, 2007.

Nel caso richiamato, presa visione della valutazione dell'imputato fornita dal COMPAS, la corte locale lo aveva condannato alla reclusione a sei anni (senza *parole*), e cinque anni di *extended supervision*, pena certamente elevata se rapportata ai fatti, marginali, per cui l'imputato si era dichiarato colpevole. La difesa aveva presentato una *post conviction motion*, al rigetto della quale veniva proposto ricorso innanzi alla Corte suprema statale. I motivi della doglianza consistevano in tre punti. Innanzitutto, si denunciava la violazione del diritto dell'imputato ad essere valutato sulla base di informazioni accurate. Poi, si lamentavano la violazione del diritto ad una sentenza individualizzata, nonché l'impiego, erroneo, da parte dello strumento, del sesso fra i parametri presi in considerazione nel giudizio di pericolosità. Inoltre, essendo lo strumento tutelato da segreto commerciale, la difesa riteneva che le parti e il giudice non avessero avuto sufficienti spiegazioni sui criteri con cui erano stati determinati i punteggi di rischio, e i singoli fattori pesati, introducendo così nel *sentencing* elementi decisori sottratti alla *discovery* della difesa.

La Corte suprema statale, tuttavia, confermava la decisione di primo grado, senza apparentemente cogliere tutti gli spunti formulati dalle argomentazioni difensive, ma limitandosi ad escludere la violazione del *due process*, data la possibilità per l'imputato di confrontare i dati individuali di partenza (*input*) e le valutazioni di rischio finali (*output*) sulla base del manuale d'uso dello strumento, potendo così adeguatamente confutarne l'attendibilità[58]. A prescindere dalla criticabilità di tale assunto, un passaggio importante della sentenza è sfuggito all'attenzione dei molti media che si sono occupati della vicenda, proposta come un esempio di "pena stabilita dalla macchina"[59]. Nel testo della decisione, infatti, si ritrova una sorta di "decalogo cautelativo" che i giudici devono impiegare nell'utilizzo di tali strumenti "predittivi", articolato in cinque avvertimenti che devono sempre essere inseriti nel *pre-sentencing report*, ovvero: l'eventuale esistenza di un segreto commerciale che copre il software; l'incapacità del software di effettuare una valutazione altamente individualizzata, essendo basato su un set di dati riferiti a gruppi sociali, non normalizzata rispetto alla popolazione di ciascuno Stato; la creazione dello strumento per finalità specificamente collegate a scelte proprie della fase esecutiva, successiva al *sentencing*, nonchè l'esistenza di dubbi, nella comunità scientifica, circa l'attendibilità del modello computazionale - pur segreto – che lo regola.

Alle precauzioni suggerite dalla Corte Suprema del Wisconsin fa da eco una successiva sentenza, pronunciata dalla Corte Suprema del District of Columbia, sezione minorile, del 15 maggio 2018. La vicenda era molto simile alla precedente, ma aveva ad oggetto un diverso strumento di *risk assessment*, il SAVRY, non digitalizzato, somministrabile solamente attraverso un professionista[60], ed elaborato per la valutazione di minorenni.

---

[58] Uno studio di Angwin et alii (V. J. Angwin et alii, *Machine bias*, in 23 maggio 2016), pubblicato dalla ONG americana ProPublica ha mostrato la scarsa rilevanza criminogenica di alcuni fattori utilizzati nel COMPAS. È bene tuttavia segnalare che le conclusioni dello studio diffuso da ProPublica sono state fortemente criticate (v. A.W. Flores – K. Bechtel – C.T Lowenkamp, *False Positives, False Negatives and False Analysis: A Rejoinder to «Machine Bias: There is Software used across the Country to Predict Future Criminals. And it is biased against the Blacks»*, in *Federal Probation,* 2016).

[59] A. Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, in *The New York Times*, 1 maggio 2017.

[60] Si tratta del SAVRY, impiegato in almeno nove Stati dell'Unione, su cui cfr. G.M.Vincent - J. Chapman - N. E. Cook, *Risk-Needs Assessment in Juvenile Justice: Predictive Validity of the SAVRY, Racial Differences, and*

In questo caso, la difesa formulava una istanza rivolta alla Corte di esclusione della prova fornita dal *risk assessment*, nonché di tutta la relazione predisposta dai servizi sociali, anche sulla base del medesimo e di qualsiasi testimonianza o altra prova ad esso collegata, denunciandone la inutilizzabilità sulla base della *rule* 702 delle *Federal Rules of Evidence*, così come interpretato dalla Corte Suprema federale nel caso *Daubert v. Merrel Dow Pharmaceutics*[61]. Tale decisione, infatti, rappresenta, a tutt'oggi, lo statuto di ammissibilità e utilizzabilità della prova tecnico-scientifica nel procedimento penale e non solo negli Stati Uniti, ma anche in numerosissimi altri ordinamenti che hanno seguito tale pronuncia.

La Corte, in parziale accoglimento delle richieste della difesa dell'imputato, minore al tempo del fatto contestato, ha fatto divieto di utilizzare per la decisione del caso specifico, la valutazione generale di *violence risk* predisposta dalla *Child Guidance Clinic* sulla base del *risk assessment*: pur senza pronunciarsi, in generale, sulla validità della teoria scientifica che sorregge il SAVRY, la Corte ha infatti ritenuto che, nell'applicazione al caso specifico, i risultati del test non fossero scientificamente attendibili.

Il richiamo a queste due recenti decisioni nordamericane ha una duplice ricaduta. Per un verso, ci ricorda come anche la tradizione europea e, in particolare, quella italiana, continuino a gravare il giudice penale di valutazioni di carattere predittivo: dalla decisione cautelare, fino alla quantificazione della pena in sentenza (si pensi, oltre che al generale paradigma dell'art. 133, 2 c.p., al perdono giudiziale), alla concessione di benefici, anche poi penitenziari, l'andamento del processo, il suo esito, la sanzione, il successivo trattamento, spesso si basano su predizioni che il giudice è chiamato a svolgere, senza dettagliati parametri, né specifiche informazioni. Per altro verso ci dimostra la necessità di avviare, senza ritardo, una seria riflessione giuridica che si sovrapponga a quella squisitamente computazionale che si concentra soltanto sulla efficacia, in termini di attendibilità, dello strumento algoritmico o computazionale, come effettivamente suggerito dalla Carta etica europea per l'impiego dell'intelligenza artificiale nei sistemi giudiziari, pubblicata dalla CEPEJ, nel dicembre del 2018[62].

the Contribution of Needs Factors, in *Crim. Just. &Behavior*, 2011, 47 ss. V., più recentemente e più in generale, J. Skeem - N. Scurich - J. Mohanan, *Impact of the Risk Assessment on Judges' Fairness in Sentencing Relatively Poor Defendants*, in *University of Virginia School of Law SSRN Papers series*, 15 gennaio 2019.

[61] 509 U.S. 579 (1993).

[62] Disponibile in *coe.int*. In tema, volendo, S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *lalegislazionepenale.it*, 18 dicembre 2018.

Altri saggi

La riforma della diffamazione: da Strasburgo al Senato, passando per Palazzo della Consulta*

Carlo Melzi d'Eril - Giulio Enea Vigevani**

Abstract

L'articolo mira a offrire un primo commento sulla riforma della diffamazione in corso di esame al Senato.
A questo fine, nella prima parte ricostruisce sinteticamente i principi individuati nella giurisprudenza della Corte europea dei diritti e nella recente ordinanza n. 132 del 2020 della Corte costituzionale.
Nella seconda parte, gli autori analizzano criticamente le soluzioni prospettate nel disegno di legge, prospettando le possibili ricadute di una riforma in tale direzione.

The article aims to offer a first comment on the defamation reform pending before the Italian Senate.
To this end, the first part briefly reconstructs the principles identified in the jurisprudence of the European Court of Human Rights and in the recent ordinance no. 132 of 2020 of the Constitutional Court.
In the second part, the authors critically analyse the provisions of the bill, envisaging the possible consequences of a reform in this direction.

Sommario

Keywords

diffamazione - stampa - giornale on line - direttore responsabile - rettifica.

* L'articolo è stato inviato su richiesta della direzione e, pertanto, in conformità all'art. 15 del regolamento della Rivista, non è stato sottoposto a referaggio.
** Il presente scritto costituisce il frutto delle riflessioni condivise degli autori. Giulio Enea Vigevani ha redatto i paragrafi 1-5 mentre Carlo Melzi d'Eril i paragrafi 6-11.

1. Ripensare la diffamazione tra giudice costituzionale e legislatore

In questa legislatura, il dialogo tra giudice costituzionale e politica non è stato facile. Dall'inerzia del legislatore sul suicidio assistito o sulle misure sanzionatorie in materia di reati sul traffico di stupefacenti (che hanno condotto alle sentenze n. 242 e n. 40 del 2019), alle reazioni spesso sguaiate di leader politici alla sentenza n. 253 del 2019 sulla concessione dei permessi premi per i condannati per i reati ostativi di cui all'art. 4 *bis* dell'ordinamento penitenziario, l'auspicio per una proficua e leale collaborazione, tante volte udito tra le mura del palazzo della Consulta[1], raramente ha trovato ascolto nelle stanze della politica.

La normativa in materia di diffamazione potrebbe costituire un'eccezione. Sembra, infatti, che stia producendo qualche reazione il richiamo della Corte, contenuto nell'ordinanza n. 132 del 2020[2], a rimeditare la normativa in tema, alla luce della giurisprudenza della Corte europea dei diritti dell'uomo. È all'esame dell'aula del Senato il disegno di legge n. 812-A[3] che, come si illustrerà nel seguito, non si limita a intervenire sulla questione della pena detentiva per tale reato, ma modifica in modo sostanziale tale fattispecie, anche alla luce della radicale trasformazione del sistema dei media.

Ora il disegno di legge dovrà trovare spazio nell'affollato calendario parlamentare dominato dall'emergenza sanitaria, ma, sul piano politico, il consenso sembra piuttosto ampio. Soprattutto non vi sono quelle distanze ideologiche che hanno reso impossibile l'approvazione di una legge sul suicidio assistito.

Al momento in cui scriviamo, non è certo né l'esito del procedimento legislativo né il testo che eventualmente sortirà dall'esame parlamentare. Tra l'altro, alcuni emendamenti proposti dal relatore, qualora approvati dall'assemblea, potrebbero incidere non poco sul punto di equilibrio individuato in commissione Giustizia.

Resta l'opportunità di una prima indagine sul disegno di legge, per riflettere se le norme in discussione siano effettivamente in grado di allineare la legislazione italiana alle prescrizioni ricavabili dalla giurisprudenza di Strasburgo e dalla medesima ordinanza del giudice costituzionale. Inoltre, con un codice penale ormai novantenne e una legge sulla stampa poco più giovane, appare utile verificare se il legislatore stia sfruttando l'occasione per scrivere la disciplina degli illeciti dell'informazione del XXI secolo, per rivedere in radice la responsabilità del direttore, per introdurre strumenti che consentano una rapida rimozione dei contenuti illeciti presenti in rete, per ripensare il concetto stesso di informazione e le distinzioni fondate sull'iscrizione agli albi professionali o sulla registrazione nelle cancellerie dei tribunali.

---

[1] Si veda da ultimo la Relazione sull'attività della Corte costituzionale nel 2019 del Presidente Marta Cartabia, disponibile all'indirizzo *cortecostituzionale.it*.

[2] Il cui testo è disponibile in *giurcost.org*.

[3] XVIII legislatura, d.d.l. n. S-812-A - Testo proposto dalla Commissione Giustizia e comunicato alla Presidenza del Senato in data 7 luglio 2020, "Modifiche alla legge 8 febbraio 1948, n. 47, al codice penale, al codice di procedura penale, al codice di procedura civile e al codice civile, in materia di diffamazione, di diffamazione con il mezzo della stampa o con altro mezzo di diffusione, di ingiuria e di condanna del querelante nonché di segreto professionale, e disposizioni a tutela del soggetto diffamato", disponibile in *senato.it*.

Prima di tali analisi, appare necessario ripercorrere il processo tuttora pendente avanti al giudice costituzionale e il ragionamento seguito dalla Corte.

Con l'ordinanza n. 132 del 2020, depositata il 26 giugno 2020, la Corte costituzionale ha rinviato all'udienza del 22 giugno 2021 la trattazione di due questioni di costituzionalità relative alle pene detentive per la diffamazione, sollevate dai tribunali di Salerno e Bari. Riprendendo la tecnica decisoria adottata per la prima volta con l'ordinanza n. 207 del 2018 relativa al delitto di aiuto al suicidio ("caso Cappato"), ha invitato in questo tempo il Parlamento a intervenire sul tema, rimuovendo i profili di incostituzionalità evidenziati e rivedendo nel suo insieme la legislazione in materia[4].

In sintesi, la Corte fa un passo indietro, lasciando che sia il legislatore ad occuparsi di scrivere una normativa capace di aggiornare la disciplina dei *reati di penna* in un contesto ove le insidie alla reputazione provengono principalmente dalla telecamera o dalla tastiera. Se anche in questo caso il Parlamento abdicherà alle sue funzioni, la Corte dovrà ancora una volta supplire a tale inerzia, pur con i limitati rimedi a sua disposizione. Si tratta, riteniamo, di un *self-restraint* comprensibile per molte ragioni: la fedeltà al principio della leale collaborazione tra le istituzioni della Repubblica nell'attuazione dei principi costituzionali; la delicatezza del bilanciamento tra due diritti inviolabili così intimamente connessi ai principi fondanti dell'ordinamento repubblicano; l'ampia discrezionalità riservata al legislatore in materia penale, anche se la Corte pare avere ormai completamente superato la propria tradizionale ritrosia nel sindacare tali norme.

Vi è altresì nel caso concreto una difficoltà per il giudice costituzionale a rinvenire nell'ordinamento previsioni normative di riferimento che consentano «l'individuazione di soluzioni, anche alternative tra loro, che siano tali da "ricondurre a coerenza le scelte già delineate a tutela di un determinato bene giuridico, procedendo puntualmente, ove possibile, all'eliminazione di ingiustificabili incongruenze"»[5].

Come si dirà più avanti, la questione sollevata dal giudice di Bari individua nell'art. 595, c. 3, c.p. la disposizione già esistente, ancorché non "costituzionalmente obbligata", che possa sostituirsi alla previsione sanzionatoria prevista nell'art. 13 legge stampa. Il medesimo art. 595, c. 3, c.p. costituisce, tuttavia, la norma oggetto della questione sollevata dal tribunale di Salerno, che richiede *sic et simpliciter* la dichiarazione di incostituzionalità di ogni pena detentiva per i reati di diffamazione aggravata.

In questo quadro, la scelta della Corte di attendere l'intervento del legislatore appare quasi obbligata e offre a quest'ultimo uno stimolo per occuparsi di una materia trascurata per decenni, che si è evoluta solo grazie alla supplenza della giurisprudenza

[4] Tra le prime riflessioni, si vedano 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 Costituzionale*, 5, 2020, 121 ss.; M. Pisapia – C. Cherchi, *Detenzione e libertà di espressione. Riflessioni sul trattamento sanzionatorio del reato di diffamazione a mezzo stampa in occasione della pronuncia della Corte Costituzionale*, in *Giurisprudenza Penale Web*, 6, 2020, 1 ss.; 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 *Consulta Online*, Studi, III, 2020, 622 ss. e, in relazione alla tecnica utilizzata dalla Corte, R. Pinardi, *La Corte ricorre nuovamente alla discussa tecnica decisionale inaugurata col caso Cappato*, in *Forum di Quaderni Costituzionali*, 3, 2020, 104 ss.; A. Ruggeri, *Replicato, seppur in modo più cauto e accorto, alla Consulta lo schema della doppia pronuncia inaugurato in Cappato (nota minima a margine di Corte cost. n. 132 del 2020)*, in *Consulta Online*, Studi, II, 2020, 406-407.

[5] Così Corte cost., 8 marzo 2019, n. 40, richiamando la sentenza n. 236 del 2016.

ordinaria e che merita invece un intervento saggio ed equilibrato.

2. Le pene per la diffamazione tra Corte di Strasburgo, legislazione nazionale e giudici italiani

La Corte era chiamata a pronunciarsi su questioni che avevano a fondamento un indirizzo ormai consolidato della Corte europea dei diritti dell'uomo – che ha il suo debutto con la decisione della Grande Camera del 17 dicembre 2004 nel caso *Cumpănă et Mazăre*[6] e che ha visto condannata anche l'Italia in alcuni recenti casi[7] – secondo cui in sede di controllo sulla proporzionalità della restrizione occorre verificare che la natura e la gravità della sanzione non siano tali dal dissuadere altri soggetti dall'esercizio del diritto di critica. In base a tale orientamento, sanzioni o risarcimenti particolarmente afflittivi[8], e pene detentive in particolare[9], anche solo minacciate e poi non eseguite[10], contrastano con l'art. 10 della Convenzione, in materia di libertà di espressione. Nel ragionamento della Corte di Strasburgo, il solo timore di simili ripercussioni potrebbe intimidire il giornalista e renderlo meno libero di informare, specie su argomenti "pericolosi". E poiché i temi che hanno maggiori rischi sono spesso quelli di maggiore interesse pubblico, sanzioni talmente gravi da non consentire errori ai giornalisti, nemmeno in buona fede, possono indebolire la libertà di espressione e la qualità della vita democratica di un Paese.

Così, per i giudici di Strasburgo, il ricorso alla pena detentiva nei confronti degli operatori dell'informazione deve essere limitato ad ipotesi eccezionali, in particolare quando altri diritti fondamentali siano stati gravemente lesi. Tra esse, la Corte indica sempre e solo la diffusione di un discorso di odio o l'incitazione alla violenza[11], senza tuttavia

[6] CEDU, *Cumpănă e Mazăre c. Romania*, ric. 33348/96 (2004).

[7] CEDU, *Belpietro c. Italia*, ric. 43612/10 (2013), *Sallusti c. Italia*, ric. 22350/13 (2019) e, in riferimento al reato di rivelazione al pubblico del contenuto di comunicazioni avvenute all'interno di un sistema informatico o telematico (art. 617-*quater* c.p.), *Ricci c. Italia*, ric. 30210/06 (2013). Con riferimento a casi di condanna a risarcimenti ritenuti eccessivi, anche in relazione alle capacità reddituali dei ricorrenti, *Riolo c. Italia*, ric. 42211/07 (2008) e, da ultimo, *Magosso e Brindani c. Italia*, ric. 59347/11 (2020), ove due giornalisti furono condannati a versare alle parti civili la somma provvisionale di 120.000 EUR a titolo di risarcimento danni, oltre alle spese processuali.

[8] CEDU, *Kasabova c. Bulgaria*, ric. 22385/03 (2011); *Bozhkov c. Bulgaria*, ric. 3316/04 (2011); *Koprivica c. Montenegro*, ric. 41158/09 (2011).

[9] CEDU, *Kydonis c. Grecia*, ric. 24444/07 (2009); *Mika c. Grecia*, ric. 10347/10 (2013); *Taranenko c. Russia*, ric. 19554/05 (2014); *Haldimann and Others c. Switzerland*, ric. 21830/09 (2015); *Şahin Alpay c. Turchia*, ric. n. 16538/17 (2018); *Mehmet Hasan Altan c. Turchia*, ric. n. 13237/17 (2018).

[10] CEDU, *Belpietro c. Italia*, ric. 43612/10 (2013), *Ricci c. Italia*, ric. 30210/06 (2013).

[11] In questo senso, da ultimo, S. Lonati, *Diffamazione a mezzo stampa e applicazione della pena detentiva: ancora qualche riflessione a margine del cd. caso Sallusti in (perenne) attesa di un intervento del legislatore*, in *questa Rivista*, 1, 2020, 69 ss., che dalla sentenza *Sallusti* del 2019 rileva la tassatività delle fattispecie indicate dalla Corte. Lo studioso osserva saggiamente che l'ipotesi di sostituire le pene detentive con pene pecuniarie più severe non è immune da rischi. Infatti, «la sanzione viene di fatto trasferita dal soggetto autore della diffamazione ad un altro soggetto, ovvero l'editore, in violazione del principio costituzionale della personalità della pena e con la possibilità che la sanzione sia considerata come un costo d'impresa. Ne potrebbe derivare la paradossale situazione che i grandi editori potrebbero avallare una linea editoriale diffamatoria mettendo "in bilancio" il pagamento della conseguente pena pecuniaria. Al contrario, per

mai escludere altre fattispecie, quali i casi di diffamazione di notevole gravità[12].
Di qui, il contrasto con la legislazione italiana, che prevede un trattamento sanzionatorio rigoroso per la diffamazione, attraverso un largo utilizzo della pena detentiva. La diffamazione "semplice" (art. 595 c.p.) è punita con la sanzione alternativa della reclusione fino a un anno o la multa fino a euro 1032. Il legislatore ha previsto ipotesi aggravate: se l'offesa consiste in un fatto determinato la pena è della reclusione fino a due anni o della multa fino a euro 2065; se è commessa con il mezzo della stampa o con qualsiasi altro mezzo di pubblicità (internet, ad esempio), ovvero in un atto pubblico, la pena aumenta ancora ed è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516. Qualora poi l'offesa sia recata ad un Corpo politico amministrativo o giudiziario, ad una sua rappresentanza o ad una Autorità costituita in collegio le pene sono aumentate di un terzo. Oltre a quelle elencate, esiste un'ulteriore disposizione contenuta nell'art. 13 della l. 47/1948 (legge stampa): quando la diffamazione è commessa con il mezzo della stampa e consiste nell'attribuzione di un fatto determinato, si prevede l'applicazione cumulativa di pena detentiva e pecuniaria (reclusione da uno a sei anni e della multa non inferiore a euro 258), mentre in tutte le altre fattispecie le due sanzioni sono alternative[13].
A tale severità della lettera della legge non corrisponde un analogo rigore nel momento dell'applicazione e in quello dell'effettiva esecuzione. In concreto sono piuttosto rare le sentenze che irrogano il carcere nei confronti dei giornalisti, anche nell'ipotesi di cui all'art. 13 legge stampa. Ciò in virtù di un particolare meccanismo: la fattispecie di cui si tratta non è considerata un delitto a sé stante, bensì un'aggravante del reato di cui all'art. 595 c.p. e ciò ne fa un elemento del bilanciamento fra circostanze che il giudice è chiamato a compiere. Così, qualora riconosca le attenuanti generiche anche solo equivalenti alla aggravante *ex* art. 13, il giudice applica la pena prevista per la diffamazione "semplice", di cui all'art. 595 c.p., che prevede la reclusione o la multa, in genere irrogando solo quest'ultima. E anche nei rarissimi casi di condanna alla pena detentiva (spesso da parte dei giudici di merito), pressoché sempre la sua esecuzione viene condizionalmente sospesa.
Del resto, chi frequenta le aule penali dei tribunali sa bene che l'esito dei processi per diffamazione si misura più sull'entità della provvisionale alla parte civile che su quella della pena.
A limitare la pena detentiva dall'orizzonte dei processi per diffamazione ha contribuito di recente anche la Cassazione, che ha risposto alle "pressioni" di Strasburgo in modi forse non del tutto consueti e ortodossi, attraverso l'uso estremo del canone

le società editoriali con minore capacità economica la minaccia dell'applicazione di sanzioni rischierebbe di provocare un effetto simile al cd. chilling effect tanto caro alla Corte europea» (ivi, 83).

[12] Per una lettura nel senso che la Corte europea non sembra escludere in casi eccezionali la previsione della pena detentiva anche per la diffamazione, si rinvia a C. Melzi d'Eril, *La Corte Europea condanna l'Italia per sanzione e risarcimento eccessivi in un caso di diffamazione. Dalla sentenza qualche indicazione per la magistratura, il legislatore e le parti*, in *Diritto Penale Contemporaneo*, 12 novembre 2012, 4 ss. e a M. Cuniberti, *Pene detentive per la diffamazione, responsabilità del direttore e insindacabilità delle opinioni del parlamentare: il "caso Belpietro" davanti alla Corte europea dei diritti dell'uomo*, in *Osservatorio costituzionale*, 2014, 5 ss.

[13] G.E. Vigevani, *L'informazione e i suoi limiti: il diritto di cronaca*, in G.E. Vigevani - O. Pollicino - C. Melzi d'Eril - M. Cuniberti - M. Bassini, *Diritto dell'informazione e dei media*, Torino, 2019, 28 ss.

dell'interpretazione conforme alla Convenzione, per giungere a una soluzione, quella di evitare condanne a pene detentive per il delitto di diffamazione, per la verità già cristallizzata da anni nella giurisprudenza[14].

Così, nel 2013 la V sezione penale[15] ha annullato con rinvio una sentenza di condanna a una pena di sei mesi di reclusione, ancorché condizionalmente sospesa, per diffamazione aggravata a carico di un giornalista (e, per omesso controllo, a carico del direttore del periodico), per la sola ragione che il giudice del merito aveva optato per la pena detentiva anziché per quella pecuniaria. La Cassazione ha ritenuto tale scelta incompatibile con «l'orientamento della Corte EDU che, ai fini del rispetto dell'art. 10 della Convenzione relativo alla libertà di espressione, esige la ricorrenza di circostanze eccezionali per l'irrogazione, in caso di diffamazione a mezzo stampa, della più severa sanzione, sia pure condizionalmente sospesa»[16]. Ciò sul rilievo che, altrimenti, non sarebbe stato assicurato il ruolo di "cane da guardia" dei giornalisti, il cui compito è di comunicare informazioni su questioni di interesse generale e, conseguentemente, di assicurare l'interesse del pubblico a riceverle.

Analogamente, nel 2019 la medesima sezione della Suprema Corte ha ritenuto sproporzionata in relazione allo scopo perseguito e contraria alla Convenzione una pena detentiva sospesa di tre mesi di reclusione comminata a un giornalista che aveva leso la reputazione di un magistrato[17].

Vi era, dunque, spazio per percorrere la strada dell'interpretazione convenzionalmente orientata, riservando la pena detentiva alle sole ipotesi di diffamazione che rivestano i caratteri dell'eccezionalità. Entrambi i giudici remittenti non hanno ritenuto, peraltro, di seguire questa via, preferendo investire la Corte costituzionale del giudizio sulle norme che prevedono la sanzione detentiva per tale reato di diffamazione.

3. Le due (diverse) ordinanze di rimessione

Le questioni sollevate erano in verità tra loro differenti sia per ciò che concerne l'oggetto che il parametro invocato, per taluni aspetti addirittura inconciliabili[18].

In particolare, il tribunale di Salerno dubitava della compatibilità con la Convenzione europea dei diritti dell'uomo (e dunque con l'art. 117, c. 1, Cost.) delle pene edittali stabilite sia nell'art. 13 della legge stampa che nell'art. 595, c. 3, del codice penale, che pure la prevede in via alternativa[19]. Inoltre, dubitava della compatibilità delle norme

[14] G.E. Vigevani, *Libertà di espressione, onore e controllo del potere. Sviluppi del diritto di critica politica, tra giudice nazionale ed europeo*, in *Federalismi.it*, 3, 2015, 15.

[15] Cass. pen., sez. V, 11 dicembre 2013, n. 12203.

[16] Ivi, § 10.

[17] Cass. pen., sez. V, 19 settembre 2019, n. 38721.

[18] 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*, cit., 129.

[19] Il caso di specie concerneva la pubblicazione di un articolo di giornale ove, secondo l'ipotesi accusatoria, veniva attribuita alle persone offese una condotta determinata lesiva della loro reputazione (di qui la contestazione dell'aggravante di cui all'art. 13 della citata l. 47/1948), poi risultata non essere vera a seguito di accertamenti investigativi.

impugnate con il principio di ragionevolezza, ritenendo la pena detentiva totalmente sproporzionata sia rispetto al bene giuridico leso (la libertà di espressione), sia a quello tutelato (la reputazione personale). Di qui la asserita violazione degli artt. 3, 21 e 25 Cost. Infine, tali previsioni sarebbero incompatibili con il principio della necessaria funzione rieducativa della pena di cui all'art. 27, c. 3, Cost., «attesa la inidoneità della minacciata sanzione detentiva a garantire il pieno rispetto della funzione generalpreventiva e specialpreventiva della pena stessa»[20].

Da tale prospettiva radicale, che presuppone l'assoluta incompatibilità della pena detentiva in tutti i casi di diffamazione, si distacca la seconda ordinanza di rimessione: il Tribunale di Bari sollevava, in riferimento all'art. 117, c. 1, Cost., in relazione all'art. 10 CEDU, questione di legittimità costituzionale del solo art. 13 della legge stampa, «nella parte in cui sanziona il delitto di diffamazione aggravata, commessa a mezzo stampa e consistente nell'attribuzione di un fatto determinato, con la pena cumulativa della reclusione da uno a sei anni e della multa non inferiore a 256 [recte: 258] euro, invece che in via alternativa»[21]. Una pronuncia di accoglimento «consentirebbe al giudice di verificare in concreto la sussistenza delle circostanze eccezionali in cui la gravità della condotta e dell'offesa che ne deriva giustifica l'irrogazione di una pena detentiva, lasciando così un adeguato spazio discrezionale utile per conformare la decisione giurisdizionale nazionale ai principi dell'ordinamento CEDU in materia».

Il *petitum* era dunque più circoscritto: non poneva in discussione la legittimità in astratto del carcere per il reato di diffamazione, ma mirava solo a rendere la pena detentiva applicabile in via alternativa e non più cumulativa rispetto alla pena pecuniaria, utilizzando come riferimento proprio quell'art. 595, c. 3, c.p. di cui il giudice di Salerno dubitava della legittimità costituzionale.

Alla base di tale differenza vi è un interrogativo a cui la Corte di Strasburgo non ha mai risposto con nettezza, ossia se, nei casi più gravi (esemplificando, le diffamazioni seriali, le campagne stampa preordinate ad annientare la reputazione di una persona, le violente offese basate su fatti che il giornalista sa essere falsi e non ha mai ritenuto di rettificare[22]), la pena detentiva possa essere prevista anche per il reato di diffamazione. Si tratta di una questione cruciale anche per il legislatore, come sottolinea con la consueta chiarezza Marco Cuniberti, quando evidenzia come «la pura e semplice eliminazione della sanzione detentiva dalle pene previste per il reato di diffamazione potrebbe non rivelarsi la soluzione più idonea a garantire una adeguata tutela alle persone offese»[23].

---

[20] Per un'analisi approfondita di tale ordinanza di rimessione si rinvia a D. Butturini, *La problematica della pena detentiva come limitazione del diritto di informazione tra Costituzione e CEDU. Spunti di riflessione a partire da una questione di legittimità costituzionale sollevata nel 2019 dal Tribunale penale di Salerno*, in *questa Rivista*, 3, 2019, 61 ss.

[21] Il giudizio *a quo* concerneva la responsabilità di un direttore di giornale per i delitti di cui agli artt. 595 c.p. e 13 della l. 47 del 1948, in ragione della pubblicazione di un articolo privo di firma, nel quale si attribuiva alla persona offesa la cessione di stupefacente a una terza persona, malgrado l'avvenuto proscioglimento del medesimo in relazione a tale fatto.

[22] C. Melzi d'Eril, *La Corte Europea condanna l'Italia per sanzione e risarcimento eccessivi in un caso di diffamazione. Dalla sentenza qualche indicazione per la magistratura, il legislatore e le parti*, cit., 10.

[23] 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*, cit., 126, ove osserva altresì che: «È tutto da dimostrare,

Occorre ora analizzare se una risposta si può rinvenire nella ordinanza n. 132 del 2020 della Corte costituzionale.

4. La prudenza della Corte costituzionale: l'ordinanza n. 132 del 2020

Per quanto concerne specificamente la pena detentiva, oggetto delle questioni poste dai giudici remittenti, l'ordinanza potrebbe apparire deludente. Riprendendo quasi alla lettera la giurisprudenza della Corte europea dei diritti dell'uomo, la Corte invita il legislatore a riservarla alle «condotte che, tenuto conto del contesto nazionale, assumano connotati di eccezionale gravità dal punto di vista oggettivo e soggettivo, fra le quali si iscrivono segnatamente quelle in cui la diffamazione implichi una istigazione alla violenza ovvero convogli messaggi d'odio» (§ 8 considerato in diritto), senza chiarire espressamente se all'interno di tali condotte possano essere inclusi i casi più gravi di diffamazione.

L'ordinanza non si limita, però, alla questione della legittimità della pena detentiva per la diffamazione, sollevata dai giudici *a quibus*. Al contrario, la Corte mira a offrire al legislatore le coordinate per «una complessiva rimeditazione del bilanciamento [...] tra libertà di manifestazione del pensiero e tutela della reputazione individuale, in particolare con riferimento all'attività giornalistica» (§ 7.1 considerato in diritto).

Secondo i giudici costituzionali, infatti, la rapida evoluzione della tecnologia e dei mezzi di comunicazione negli ultimi decenni impone di non considerare il punto di equilibrio tra tali diritti come «fisso e immutabile» Di qui l'esortazione a «coniugare le esigenze di garanzia della libertà giornalistica .... 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» (§ 7.3 considerato in diritto).

La Corte, in altri termini, evita di sottoscrivere la *vulgata* che si legge di frequente sugli organi di stampa, che si limita a sventolare "bavagli" o a gridare allo scandalo per ogni sanzione severa a carico di un giornalista. Al contrario, offre al legislatore le coordinate

insomma, che una scomposta invettiva a sfondo razzista sia più idonea a mettere in pericolo diritti fondamentali della persona di quanto non accada per una ben costruita operazione diffamatoria che, magari conservando le vesti formali di una informazione obiettiva e misurata, si traduca nell'attribuzione di condotte disonorevoli e infamanti, come ad esempio il compimento di crimini particolarmente odiosi: un'operazione di tale fatta, specie se compiuta nella consapevolezza della falsità degli addebiti, e tanto più in quanto si presenti sotto le spoglie di una accurata ed obiettiva informazione giornalistica, rischia di arrecare al soggetto danni anche più gravi, ben potendo pregiudicare la sua posizione in seno alla famiglia ed alla società, la sua posizione lavorativa e le sue prospettive professionali, la sua salute, ed infine anche la sua vita e la sua incolumità».

per un corretto intervento in questa delicata e complessa materia, tenendo conto che il mestiere del giornalista è pericoloso, per chi lo esercita ma anche per chi subisce le conseguenze di una cattiva informazione. Così la Corte rimarca che la reputazione di una persona costituisce un diritto connesso a doppio filo con la sua stessa dignità, che merita di essere adeguatamente protetto contro illegittime – e talvolta maliziose – aggressioni.

In questa prospettiva più ampia, il Giudice delle leggi affronta il tema dell'apparato sanzionatorio più idoneo ad assicurare un corretto bilanciamento, suggerendo «il ricorso – nei limiti della proporzionalità rispetto alla gravità oggettiva e soggettiva dell'illecito – a sanzioni penali non detentive nonché a rimedi civilistici e in generale riparatori adeguati (come, *in primis*, l'obbligo di rettifica), ma anche a efficaci misure di carattere disciplinare, rispondendo allo stesso interesse degli ordini giornalistici pretendere, da parte dei propri membri, il rigoroso rispetto degli standard etici che ne garantiscono l'autorevolezza e il prestigio, quali essenziali attori del sistema democratico» (§ 8 considerato in diritto).

Quindi, se abbiamo ben colto il senso della pronuncia, da questa emerge che: a) la pena, in particolare detentiva, non può essere la regola, come invece è, almeno secondo la lettera della legge italiana; b) il legislatore deve preferire altre sanzioni, meno lesive, ma nella gran parte dei casi più efficaci (sembra un paradosso ma non lo è), che non incidono sulla libertà personale ma semmai sul patrimonio o la vita professionale, nella logica di un diritto penale minimo; c) in casi eccezionali, qualora queste sanzioni siano inadeguate alla tutela della reputazione, il legislatore può prendere in considerazione il ricorso alla pena, eventualmente persino detentiva, anche per il reato di diffamazione.

In questa prospettiva sembra essersi mossa una recentissima decisione della Cassazione[24] – a quanto consta la prima che richiama l'ordinanza n. 132 del 2020 della Corte costituzionale, riportandola quasi integralmente – relativa al caso di un direttore di un periodico, condannato a otto mesi di reclusione per diffamazione aggravata continuata a mezzo stampa per una serie di articoli non firmati o firmati con un acronimo, relativi ad alcuni ufficiali dei carabinieri.

Per la Cassazione, la pronunzia interlocutoria del Giudice delle leggi «fornisce una traccia esegetica di grande rilievo, che non può essere trascurata nell'ottica di una lettura costituzionalmente e convenzionalmente orientata del tema del trattamento sanzionatorio». E secondo tale direttrice «in attesa delle determinazioni del legislatore e di quelle, eventuali, della Consulta stessa», la scelta di applicare la pena detentiva va attribuita al giudice del merito alla luce dell'apprezzamento della «eccezionale gravità» della condotta diffamatoria.

5. Dalla Corte al Parlamento: il disegno di legge n. S-812-A

L'invito della Corte è rivolto primariamente al legislatore, invitato a ragionare sul bi-

[24] Cass. pen, sez. V, 9 settembre 2020, n. 26509.

lanciamento tra libertà di informare e tutela della reputazione, sulle peculiarità delle diffamazioni on-line, sull'efficacia di strumenti quali la rettifica o le sanzioni disciplinari, sui casi più gravi nei quali la pena detentiva forse costituisce ancora l'unico deterrente e, più in generale, sollecitato a ripensare una normativa costruita su un *medium*, la stampa, che ormai da tempo ha perduto la propria centralità nel panorama mediatico, a vantaggio della televisione e della rete.

E, in effetti, il legislatore sembra aver reagito alle sollecitazioni della Corte. La commissione giustizia del Senato ha concluso, pochi giorni dopo il comunicato che preannunciava l'ordinanza, l'esame del disegno di legge Caliendo in materia di diffamazione, dando mandato al relatore per riferire in Aula e il testo è al momento in cui scriviamo all'esame dell'assemblea del Senato. Esso affronta molti dei temi posti dalla Corte: sostituisce le pene detentive con multe assai elevate; estende la normativa prevista per la stampa a testate giornalistiche radiotelevisive o telematiche; modifica la disciplina della rettifica; attribuisce la garanzia del segreto sulla fonte anche ai pubblicisti, introduce meccanismi sanzionatori per le querele e le azioni civili temerarie; favorisce l'eliminazione dalla rete dei contenuti diffamatori.

Prima di ritornare al tema più noto della riforma – e già qui accennato più volte, ovvero la eliminazione della pena detentiva – proviamo a offrire una prima analisi degli ulteriori punti che ci paiono più rilevanti.

6. L'estensione della disciplina della stampa ai quotidiani on line

In primo luogo, e lo affrontiamo per primo perché si tratta di uno dei problemi che maggiormente hanno agitato dottrina[25] e giurisprudenza negli ultimi anni, il disegno di legge si incarica di risolvere la questione delle regole da applicare alla manifestazione del pensiero diffusa on-line. Come noto, il legislatore ha modellato le regole di dettaglio della materia, sanzioni comprese, distinguendo i mezzi con i quali il pensiero veniva diffuso. La stampa, fin dal 1948, con la Costituzione e la legge stampa, poi la radiotelevisione, prima con la legge Mammì (l. 223/1990), poi con il testo unico dei servizi di media audiovisivi e radiofonici (d.lgs. 177/2005). Da questo panorama è finora sempre rimasta esclusa la rete Internet, sicché la giurisprudenza ha dapprima escluso che a quanto diffuso on-line potesse applicarsi la disciplina della stampa[26] poi

[25] In tema, volendo, C. Melzi d'Eril, *La complessa individuazione dei limiti alla manifestazione del pensiero in internet*, in *Diritto dell'informazione e dell'informatica*, 2011, 571 ss., anche per i riferimenti in dottrina e giurisprudenza. Sull'applicabilità dello statuto penale della stampa alla rete si v. il contributo di M. Bassini, *La disciplina penale della stampa alla prova di internet: avanzamenti e arresti nella dialettica giurisprudenziale da una prospettiva costituzionale*, in R. Flor - D. Falcinelli - S. Marcolini (a cura di), *La giustizia penale nella "rete"*, Milano, 2015, 9 ss.

[26] Sul punto si vedano le sentenze che negavano l'applicabilità dell'art. 57 c.p. al direttore di un periodico online: il riferimento è a Cass. pen., sez. V., 16 luglio 2010, n. 35511, in *Diritto dell'informazione e dell'informatica*, 2010, 895 ss.; in dottrina tra i numerosi commenti alla decisione si v. N. Lucchi, *Internet, libertà di informazione e responsabilità editoriale*, in *Quaderni costituzionali*, 2011, 415-418; I. Salvadori, *La normativa penale della stampa non è applicabile,* de iure condito*, ai giornali telematici*, in *Cassazione penale*, 2011, 2982- 2994; S. Turchetti, *L'art. 57 c.p. non è applicabile al direttore del periodico online*, in *penalecontemporaneo.it*, 17

– a seguito delle due sentenze delle Sezioni Unite prima penali e poi civili, in materia di sequestro di periodici telematici registrati[27] – ha cambiato rotta (ma ancora l'approdo non è sicuro), rendendo applicabili anche alle testate giornalistiche che diffondono informazione a livello professionale le disposizioni incriminatrici previste *ad hoc* per la stampa (art. 57 c.p. e artt. 13 e 16 legge stampa[28]).

A prescindere dalla incertezza dei confini di quest'ultimo *medium* e dalla ragionevolezza di una simile partizione, pare evidente che il legislatore aveva atteso fin troppo a intervenire.

Ora lo sta facendo, prevedendo una normativa che non sembra, tuttavia, cogliere

novembre 2010; I. Campolo, *Diffamazione: il direttore della testata telematica non è imputabile per reato di omesso controllo*, in *Guida al diritto*, n. 44, 2010, 18-23, nonché da ultimo C. Melzi d'Eril, Roma locuta*: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica* on line, in *Diritto dell'informazione e dell'informatica*, 2010, 899-907. Nello stesso senso anche Cass. pen., sez. V, 28 ottobre 2011, n. 44126, in *Diritto dell'informazione e dell'informatica*, 2011, 795 ss.; tra gli autori che hanno commentato tale pronuncia si v. S. Turchetti, *Un secondo "alt" della Cassazione all'applicazione dell'art. 57 c.p. al direttore del periodico on line*, in *penalecontemporaneo.it*, 16 dicembre 2011; G. Corrias Lucente, *Al direttore responsabile di un periodico on line non si applica il reato previsto dall'art. 57 del codice penale*, in *Diritto dell'informazione e dell'informatica*, 2012, 82 ss.; D. Petrini, *Il direttore della testata telematica, tra* horror vacui *e prospettive di riforma; sperando che nulla cambi*, in *Rivista italiana di diritto e procedura penale*, 2012, 1611 ss. e infine G.E. Vigevani, *La «sentenza figlia» sul direttore del giornale telematico: il caso Hamaui*, in *Diritto dell'informazione e dell'informatica*, 2011, 798 ss. In tema, si veda anche Cass. pen., sez. III, 10 maggio 2012, n. 23230 che ha escluso l'applicabilità ai periodici diffusi in rete del reato di stampa clandestina, in *Diritto dell'informazione e dell'informatica*, 2012, 1118 ss., con nota di P. Di Fabio, *Blog, giornali on line e «obblighi facoltativi» di registrazione delle testate telematiche: tra confusione del legislatore e pericoli per la libera espressione del pensiero su internet*. Sull'inapplicabilità alla rete dell'art. 13 legge stampa, tra le più recenti decisioni si v. Cass. pen., sez. V, 1° febbraio 2017, n. 4873 in *Diritto Penale Contemporaneo*, 4, 2017, 286 ss., con nota di E. Birritteri, *Diffamazione e Facebook: la Cassazione conferma il suo indirizzo ma apre a un'estensione analogica in malam partem delle norme sulla stampa*.

[27] Il riferimento è a Cass. pen., sez. un., 29 gennaio 2015 (dep. 17 luglio 2015), n. 31022, *Fazzo e altro*. Con tale decisione, le Sezioni Unite, chiamate a decidere sulla possibile estensione delle garanzie costituzionali in materia di sequestro alle manifestazioni del pensiero in rete, hanno coniato una inedita definizione di stampa: non dovrebbe più essere tratta dall'interpretazione letterale dell'art. 1 della legge stampa (l. 47/1948), ma dovrebbe essere intesa in senso figurato e corrisponderebbe all'informazione giornalistica professionale. Da qui, l'estensione della disciplina costituzionale a tutela degli stampati all'informazione on line, purché diffusa da una testata registrata, che abbia un direttore e veicoli informazione in modo professionale. Per un commento a tale decisione, tra i molti P. Caretti, *La Cassazione pone, meritoriamente, alcuni punti fermi in tema di regolazione dell'informazione via internet*, in *Quaderni costituzionali*, 4, 2015, 1013 ss.; L. Diotallevi, *La Corte di cassazione sancisce l'"equiparazione" tra giornali cartacei e telematici ai fini dell'applicazione della disciplina in materia di sequestro preventivo: un nuovo caso di "scivolamento" dalla "nomofilachia" alla "nomopoiesi"?*, in *Giurisprudenza costituzionale*, 2015, 1062 ss.; L. Paoloni, *Le Sezioni Unite si pronunciano per l'applicabilità alle testate telematiche delle garanzie costituzionali sul sequestro della stampa:* ubi commoda, ibi et incommoda*?*, in *Cassazione penale*, 2015, 3454 ss. e volendo C. Melzi d'Eril, *Contrordine compagni: le Sezioni Unite estendono le garanzie costituzionali previste per il sequestro degli stampati alle testate on-line registrate*, in *penalecontemporaneo.it*, 9 marzo 2016. L'anno successivo, le Sezioni Unite civili (Cass. civ., sez. un., 25 ottobre 2016, n. 23469, in *Il Foro italiano*, 12, 2016, 3767 ss., con nota di A. Palmieri, *In tema di estensione delle garanzie costituzionali alle pubblicazioni telematiche*) ribadiscono l'estensione della garanzia all'informazione professionale veicolata tramite la rete.

[28] Sull'applicabilità dell'art. 57 c.p. all'informazione in rete, l'orientamento, cristallizzato dal 2010 che negava tale possibilità, ha ricevuto la sua prima smentita nel 2018 quando la Cassazione ha stabilito che il direttore responsabile della testata telematica registrata può essere chiamato a rispondere del reato di omesso controllo (Cass. pen., sez. V, 22 marzo 2018, n. 13398, in *questa Rivista*, 2, 2018, 324 ss., con nota di S. Vimercati, *Il* revirement *della Cassazione: la responsabilità per omesso controllo si applica al direttore della testata telematica*). Nello stesso senso, Cass. pen., sez. V, 23 ottobre 2018, n.1275, in *questa Rivista*, 2, 2019, 283 ss., con nota di L. Amerio, *La responsabilità ex art. 57 c.p. del direttore di testate telematiche: tra estensione interpretativa ed analogia* in malam partem.

pienamente le peculiarità della diffusione del pensiero in rete, limitandosi per lo più a estendere a una realtà così diversa una normativa pensata molti decenni fa per la stampa. Del resto, il legislatore si è rivelato negli ultimi anni in materia talmente maldestro da avere creato più danni dei problemi che ha risolto. Si pensi all'introduzione della diffamazione televisiva (mirabile esempio di strabismo legislativo), alla misteriosa nozione di "prodotto editoriale" coniata nel 2001[29], che ha avuto bisogno di ulteriori interventi di interpretazione autentica per dissiparne (e non del tutto) l'oscurità[30], alla regola sulla diffusione di dati personali nell'ambito dell'attività giornalistica, dalla sintassi faticosa, oltre che dal significato a volte imperscrutabile[31].

Il testo all'esame del Senato modifica l'art. 1, c. 2, della legge stampa, estendendo le regole tradizionalmente previste per la stampa ad altri prodotti editoriali registrati *ex* art. 5 della legge stampa stessa. Più precisamente, tale dilatazione riguarda, in virtù dell'art. 1, c. 2, lett. *a)*, i «quotidiani on line di cui all'articolo 1, comma 3 bis della legge 7 marzo 2001, limitatamente ai contenuti prodotti, pubblicati, trasmessi o messi in rete dalla redazione degli stessi». Quest'ultima disposizione introduce la definizione di «quotidiano on line», ovvero «quella testata giornalistica: a) regolarmente registrata presso una cancelleria di tribunale; il cui direttore responsabile sia iscritto all'Ordine dei giornalisti, nell'elenco dei pubblicisti ovvero dei professionisti; c) che pubblichi i propri contenuti prevalentemente on line; d) che non sia esclusivamente una mera trasposizione telematica di una testata cartacea; e) che produca principalmente informazione; f) che abbia frequenza di aggiornamento almeno quotidiana; g) che non di configuri esclusivamente come un aggregatore di notizie». Il nuovo art. 1, c. 2, lett. *b)*, inoltre, amplia il perimetro della estensione ai telegiornali e ai giornali radio di cui all'art. 32 *quinquies* del d.lgs. 177/2005.

Così, sembra che lo speciale statuto previsto dall'ordinamento per la stampa non si basi più, come i Costituenti avevano a suo tempo stabilito, sulla tipologia del mezzo

---

[29] L'art. 1 della l. 62/2001, infatti, ha introdotto la definizione di prodotto editoriale, che comprende «il prodotto realizzato su supporto cartaceo, ivi compreso il libro, o su supporto informatico, destinato alla pubblicazione o, comunque, alla diffusione di informazioni presso il pubblico con ogni mezzo, anche elettronico, o attraverso la radiodiffusione sonora o televisiva». Al contempo, tale provvedimento ha previsto che al prodotto editoriale si applichino le indicazioni obbligatorie di cui all'art. 2 legge stampa e che quando tale prodotto sia diffuso al pubblico con periodicità regolare e contraddistinto da una testata, sia sottoposto all'obbligo di registrazione *ex* art. 5 della legge stampa. In dottrina, si è molto dibattuto sul preteso impatto che la l. 62/2001 avrebbe sortito in ordine all'applicabilità del regime della stampa alla rete. Sul punto ritiene tutt'altro che risolutivo l'intervento operato con la l. 62/2001 M. Cuniberti, *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici,* Milano, 2008, 220 ss. Sul piano generale della applicabilità della disciplina della stampa a Internet, anche dopo la l. 62/2001, scettico è V. Zeno Zencovich, *I "prodotti editoriali" elettronici nella L. 7 marzo 2001 n. 62 e il preteso obbligo di registrazione,* in *Diritto dell'informazione e dell'informatica,* 2001, 153 ss. Più aperto, ma incline a circoscrivere le condizioni per tale assimilazione è E. Nania, *L'estensione a Internet del regime giuridico della stampa,* in *Nomos,* 2002, 155 ss.

[30] Ad affermare il carattere settoriale dell'intervento normativo del 2001 ci ha pensato il legislatore il quale con l'art. 7, c. 3, del d.lgs. 70/2003, a mo' di interpretazione autentica, ha chiarito che «La registrazione della testata editoriale telematica è obbligatoria esclusivamente per le attività per le quali i prestatori del servizio intendano avvalersi delle provvidenze previste dalla legge 7 marzo 2001, n. 62», escludendo quindi una generalizzata equiparazione tra stampa e internet.

[31] In tema, volendo, G. E. Vigevani, *Diritto all'informazione e* privacy *nell'ordinamento italiano: regole ed eccezioni*, in *Diritto dell'informazione e dell'informatica*, 2016, 483 ss.

di comunicazione, bensì sulla materia trattata, ovvero l'informazione, e sulla tipologia di soggetti che la produce, ovvero i professionisti. Con tutte le difficoltà di definire con esattezza e precisione quali mezzi possano ritenersi "di informazione" e i dubbi sulla ragionevolezza di ritenere che l'informazione professionale, qualunque nozione si voglia assumere di essa, passi oggi soltanto dai giornali, cartacei e non, e che quindi la particolare disciplina solo a essi debba essere riservata.

Poiché, come noto, e come si approfondirà più avanti, la diffusione tramite stampa o "prodotto editoriale registrato" implica un non irrilevante aumento di pena in caso di diffamazione, la scarsa tassatività della nozione introdotta nel disegno di legge si riverbera sulla fattispecie penale, ponendo dubbi di costituzionalità.

Peraltro, va notato che la "novella" prevede l'applicazione della legge stampa ai prodotti editoriali registrati, senza però che sia stato introdotto un obbligo di registrazione di questi ultimi. Sicché un modo per eludere del tutto la disposizione in esame è quello semplicemente di non registrare la testata o di cancellare la registrazione eventualmente già intervenuta[32].

Tornando alla disciplina prevista nel disegno di legge, l'art. 13 della l. 47/1948, che prevede un'aggravante per la diffamazione a mezzo stampa e con l'attribuzione di un fatto determinato, viene esteso ai quotidiani on line, così come la responsabilità *ex* art. 57 c.p., per omesso controllo, del direttore responsabile.

Al di là della pur deprecabile abitudine dei rinvii ad altre fonti normative che rende il testo di una legge cardine del sistema di più difficile lettura, le pecche qui sono ben altre. Anzitutto il legislatore si mostra prigioniero di una burocrazia del secolo passato, e con ciò lontanissimo dal comprendere, primo passo per regolare con saggezza, il fenomeno della diffusione dell'informazione via internet.

L'intenzione, facile da intuire, come anticipato, è quella di estendere le disposizioni in materia di stampa all'informazione professionale diffusa in rete. Rimane oscura la ragione per cui le disposizioni in materia di stampa vengano estese non tanto alle manifestazioni del pensiero immesse in rete (che ha soppiantato la stampa come mezzo a cui il maggior numero di persone si affida per diffondere il proprio pensiero) quanto a mezzi di comunicazione che sembrano piuttosto analoghi ai periodici (nozione tutt'affatto diversa).

Ciò implica irragionevoli disparità di trattamento: per citarne solo una, per quale ragione all'articolo dell'editorialista dovrebbe applicarsi una disciplina diversa rispetto al post della stessa "firma" sul suo blog o sulla sua pagina Facebook? Ancora, per quale ragione l'estensione è limitata ai quotidiani on line? Se la *ratio* era quella di estendere la disciplina della stampa ai periodici on line, perché limitarsi ai quotidiani? Non vogliamo pensare che la pigrizia del legislatore si sia spinta fino a preferire questa soluzione perché di quotidiano on line esiste già una definizione a cui operare un rinvio, mentre se si fosse dovuto estendere la nozione, sarebbe stato necessario inventarsi una definizione *ex novo*.

Infine, il mero aumento del perimetro della applicabilità della legge stampa ci pare essere insieme la più facile e la peggiore soluzione possibile per risolvere la obiettiva

[32] A tal proposito, C. Melzi d'Eril - G. E. Vigevani, *Niente carcere per diffamazione a mezzo stampa: la riforma è ora al Senato per essere completata*, in *Guida al diritto*, 2, 2014, 14.

disparità di trattamento, soprattutto in termini di sanzioni, tra la diffamazione a mezzo stampa e quella on line. Con ciò non si fa altro che ingessare in una normativa, già vecchia per la carta, un fenomeno che ha nella agilità e nella facilità all'ingresso due tra le proprie caratteristiche più apprezzabili. Senza risolvere gli interrogativi che in molti già ora si pongono sulla esigibilità di un controllo come quello affidato al direttore responsabile, anzi se possibile aumentando le perplessità riguardo a una simile disposizione, tenuto conto della quantità di informazioni che un periodico on line può diffondere e del fatto che molto spesso le informazioni vengono aggiornate, come un rullo continuo, senza delle vere e proprie edizioni giornaliere[33].

7. La nuova rettifica

Alla disciplina della rettifica vengono aggiunte disposizioni ragionevoli, alcune delle quali ricalcano le soluzioni adottate dalla giurisprudenza per casi problematici. Anzitutto la dimensione del testo della rettifica: oltre a dover essere di trenta righe, si precisa che ogni riga dovrà contare sessanta battute.

Poi è prevista una sanzione da 5.165 a 51.646 euro che accompagna l'ordine di pubblicazione della rettifica da parte del giudice, cui come oggi l'interessato può rivolgersi nel caso in cui il direttore non l'abbia pubblicata. Inoltre, qualora il direttore non ottemperi all'ordine di pubblicazione, l'inottemperanza è punita ai sensi dell'art. 388, c. 2, c.p.

Entrambe sembrano disposizioni ragionevoli e opportune, da un lato per indurre alla pubblicazione della rettifica, quando vi siano i presupposti, senza far compiere fatica burocratica ai tribunali, dall'altro per contrastare il malcostume della mancata attuazione dei provvedimenti del giudice.

Come pare altrettanto non inopportuna, anche se pure qui la giurisprudenza aveva dato direttive ormai consolidate, la precisazione che la rettifica debba fare riferimento all'articolo da rettificare e debba essere pubblicata nella sua interezza. Si tratta ancora una volta di disposizioni che cristallizzano interventi dei giudici di merito e di legittimità che si sono occupati della materia.

L'estensione della rettifica alla stampa non periodica sembra anch'essa una soluzione corretta al fine di tutelare le persone menzionate in quel genere di pubblicazioni, rimaste fuori dagli strumenti previsti dall'ordinamento.

Altre regole sono meno condivisibili, come la eliminazione delle «risposte» e la introduzione delle «smentite». La nozione di «risposta» poteva trovare una propria nicchia nel sistema; meno usata della rettifica, poteva trattarsi di una sorta di replica senza che vi sia contenuta una vera e propria correzione di quanto pubblicato, come è viceversa appunto la rettifica. Non è poi chiaro cosa debba intendersi per «smentita» e quindi quali differenze vi siano tra la smentita e la rettifica.

Altro punto che non convince è la causa di non punibilità (prevista, nel testo in itinere, all'art. 13, c. 4, legge stampa) per il delitto di diffamazione a mezzo stampa con l'attribuzione di un fatto determinato, qualora siano pubblicate, con le modalità previste

[33] Sul punto, volendo, C. Melzi d'Eril, Roma locuta*: la Cassazione esclude l'applicabilità dell'art. 57 c.p. al direttore della testata giornalistica* on line, cit., 904 ss.

dall'art. 8 della legge stampa, rettifiche o smentite idonee a riparare l'offesa. Un emendamento su cui sembra essere convogliata la maggioranza dei senatori prevede che la causa di non punibilità si applichi solo se la pubblicazione della rettifica sia avvenuta prima della apertura del dibattimento nel processo per diffamazione.
Una simile regola lascia intendere che la mera correzione di quanto affermato, purché in grado di «riparare l'offesa», sia sufficiente a risarcire il danno causato. Anzitutto quello di «riparare l'offesa» è concetto non semplice da delineare, oltre che non strettamente giuridico: quando un'offesa può dirsi riparata? Forse mai, tenuto conto del fatto, se non altro, che è assai improbabile che tutti quelli che hanno letto la prima affermazione lesiva della reputazione siano raggiunti anche dal secondo messaggio "riparatore". In secondo luogo, la rettifica potrebbe intervenire dopo molto tempo dall'offesa, che dunque rimarrebbe nella memoria, cerebrale o elettronica, della comunità di riferimento, come unico messaggio offensivo per mesi se non per anni. Come si vede, quindi, residua una "quota" di lesione della reputazione che non potrebbe essere coperta dalla nuova pubblicazione riparatrice.
La presenza di questa causa di non punibilità è anche l'origine della inedita previsione di una possibile rettifica chiesta dall'autore dell'articolo al proprio direttore. Ciò al fine di consentire, almeno al giornalista, di non essere sanzionato qualora si attivasse autonomamente per far pubblicare la rettifica, nell'ipotesi in cui il direttore fosse contrario. Non sembra una eventualità frequente, ma comprendiamo che possa essere necessario per tenere in equilibrio il sistema.
Infine, la riforma della rettifica, all'interno della più ampia riforma della disciplina della stampa, avrebbe forse dovuto occuparsi di un tema che invece viene ignorato. L'art. 8, nel testo originario ma anche in quello oggi in discussione, impone la pubblicazione delle rettifiche dei soggetti di cui è stata diffusa un'immagine, o a cui è stato attribuiti atti, pensieri o affermazioni «da essi ritenuti lesivi della loro dignità, del loro onore o della loro reputazione *o* contrari a verità». La presenza della congiunzione «o» ha consentito e quindi consentirà ancora di ottenere la forzata introduzione tra le "colonne" dei periodici di rettifiche ad affermazioni vere.
Se lo scopo dell'istituto è quello di consentire alla persona di correggere quanto i mezzi di informazione hanno diffuso sul suo conto, imponendo la pubblicazione di una simile correzione, uno dei presupposti per l'applicazione di questo strumento sembra debba essere proprio la falsità di quanto si intende correggere. Il falso non è illecito di per sé, ma certamente qualora la propalazione di un fatto falso implichi altresì la lesione di un altro bene giuridico, anche soltanto la ritenuta lesione di dignità o reputazione, la circostanza ben può essere ritenuta presupposto di una pubblicazione imposta. È molto più difficile ritenere accettabile una simile imposizione, in presenza della pubblicazione di fatti corrispondenti a verità.

8. Il ruolo del direttore responsabile

Si è già detto della assai discutibile estensione *tout court* della disciplina prevista per la stampa alla rete, tra cui quella dello *status* del direttore responsabile è una delle colonne

principali.
Merita invece un plauso la precisazione secondo cui il direttore responsabile può delegare ad altri professionisti, idonei a svolgere tale ruolo, il controllo sui contenuti del periodico. Si tratta di una figura, quella della delega, ormai estremamente diffusa in ambito imprenditoriale, gemmata nella materia della salute e sicurezza sul lavoro, per espandersi poi in relazione ad altre materie.
Qui forse sarebbe stato utile, tenuto conto della peculiarità del compito, prevedere che il delegato fosse non solo professionalmente in grado di svolgere tale incombente ma altresì dotato dei poteri, anzitutto disciplinari, necessari per rendere un simile controllo effettivo. Come in altri ambiti è stato prima previsto e poi superato, anche in questo pare invece un "fuor d'opera" legare la possibilità di conferire una delega efficace alle «dimensioni organizzative» e alla «diffusione» del periodico, senza peraltro fornire alcun parametro di riferimento.

9. Le disposizioni a favore del danneggiato

Del tutto condivisibile, anche se forse non indispensabile, tenuto conto che cristallizza arresti giurisprudenziali ormai acquisiti, quanto previsto dal nuovo art. 11 *bis* della legge stampa. Qui il legislatore si incarica di indicare al giudice alcuni parametri su cui quantificare il danno da diffamazione a mezzo stampa. E si menzionano, come indici di cui tenere conto, la diffusione quantitativa e la rilevanza nazionale o locale del *medium*, la gravità dell'offesa, nonché l'effetto riparatorio della rettifica. Quest'ultimo criterio non è del tutto chiaro come si combini con la disposizione che prevede viceversa una causa di non punibilità per la diffamazione a cui è seguita una rettifica pubblicata secondo i criteri di cui all'art. 8. In questo caso, infatti, la causa di non punibilità avrebbe tra i propri effetti quello di escludere del tutto la risarcibilità del danno. Probabilmente, il legislatore ha inteso includere tra i parametri per la valutazione del danno quelle rettifiche non idonee a riparare del tutto l'offesa.
Viene poi introdotto un nuovo meccanismo di «notifica e rimozione» mediante l'inserimento dell'art. 17 *bis* nel d.lgs. 70/2003. Gli Internet Service Provider con almeno cinquecentomila utenti registrati avranno l'obbligo di individuare tra i giornalisti pubblicisti una persona a cui affidare il compito di ricevere i reclami di chi si ritiene diffamato dai contenuti pubblicati. La mera violazione di tale obbligo è assistita da una sanzione amministrativa da 15.000 a 20.000 euro. Il prestatore di servizi, se non ritiene di accedere alla richiesta di rimozione entro ventiquattro ore, può attivare nei successivi sette giorni una procedura di conciliazione in contraddittorio davanti a un organismo indipendente presso l'Agcom, che può sfociare nell'ordine di rimozione, qualora il messaggio fosse ritenuto offensivo. Se l'ordine non viene eseguito è prevista una sanzione amministrativa da 20.000 a 40.000 mila euro. Chi si ritiene leso da contenuti non rimossi mediante la procedura appena descritta può rivolgersi al giudice civile. La rimozione dei contenuti, a seguito di notifica dell'interessato, da parte degli ISP, in buona fede, non determina una responsabilità nei confronti dei terzi, ovvero bisogna immaginare, gli autori dei contenuti stessi.

Un simile obbligo di procedimentalizzare le richieste di cancellazione si inserisce nella scia della decisione Google Spain[34] e conferma la tendenza degli ordinamenti a coinvolgere gli ISP nel tentativo di limitare le condotte illecite. Al soggetto che trae profitti dalla diffusione di contenuti viene attribuita, infatti, la responsabilità non tanto per gli eventuali danni arrecati, quanto per le modalità di organizzazione degli obblighi di previa valutazione della liceità dei medesimi.
L'idea di imporre a chi fornisce la piattaforma di contribuire a organizzare un sistema di primo controllo dei messaggi ivi contenuti, in modo tale che la mole di richieste non pesi esclusivamente sul sistema giudiziario, determinandone o il collasso o la indifferenza, di per sé non sembra né irragionevole, né arbitraria. Non sappiamo, tuttavia, valutare se il sistema così congegnato sarà realizzabile e funzionerà, in particolare se i tempi assai stretti previsti potranno essere rispettati o no.
Vi sono poi oggettive sbavature nel testo legislativo.
Risulta oscura la ragione per cui gli ISP debbano affidare a un giornalista pubblicista il compito della prima "scrematura" delle richieste. Perché non un professionista? O, ancora meglio, tenuto conto che si tratta di valutare la liceità di un messaggio, un laureato in legge?
Poco chiaro anche come debba connotarsi la condotta di «buona fede» dell'ISP che elimini il contenuto per andare esente da responsabilità nei confronti dei terzi. Di quali responsabilità, inoltre, è pure non del tutto comprensibile, tenuto conto che pressoché sempre viene contrattualizzata, al momento dell'utilizzo del servizio, la facoltà del provider di cancellare quanto non corrisponde anche soltanto alle policy, che ormai tendono sempre più a escludere qualunque contenuto illecito.

10. Le disposizioni processuali

L'art. 200 c.p.p. viene, finalmente, applicato non solo ai giornalisti professionisti ma anche ai pubblicisti, cui viene garantito, nei limiti previsti dalla legge, il segreto sulla fonte della notizia. Non è chiaro perché dalla disposizione siano esclusi i praticanti, nonché chi si limita a esercitare la libertà di manifestazione del pensiero producendo inchieste, indipendentemente dalla iscrizione in un albo, ma se non altro viene così eliminato un tratto di irragionevolezza della disciplina, da molti (e da tempo) stigmatizzato[35].
Viene altresì introdotto il comma 3 *bis* all'art. 427 c.p.p., secondo il quale con la sentenza di assoluzione perché il fatto non sussiste o perché l'imputato non l'ha commesso il giudice può, su richiesta dell'imputato, condannare a una somma determinata in via equitativa il querelante, la cui richiesta di punizione è risultata temeraria. Analoga disposizione è prevista nel processo civile, con la modifica dell'art. 96 c.p.c. ove è previsto, più specificamente, che nei casi di diffamazione, con il mezzo della stampa

[34] CGUE, C-131/12, *Google Spain* (2014); per un commento alla pronuncia, volendo, G.E. Vigevani, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano*, in *federalismi.it*, 2, 2014.

[35] G.E. Vigevani, *La protezione del segreto del giornalista al tempo di internet*, in *costituzionalismo.it*, 2, 2011 (5 dicembre 2011).

e della televisione (non però a mezzo di "prodotto editoriale registrato"…), se risulta la malafede o la colpa grave di chi agisce in giudizio, a richiesta del convenuto, con il rigetto della domanda, il giudice può condannare l'attore al pagamento di una somma determinata in via equitativa a favore del richiedente.
La disposizione pare ragionevole, ma è verosimile che abbia scarsa applicazione, almeno nei procedimenti penali: quasi sempre le assoluzioni dal delitto di diffamazione sono pronunciate perché il fatto non costituisce reato, in quanto l'offesa, pur esistente, è ritenuta scriminata per la verità del fatto. In questo caso, una querela, pur temeraria, poiché la sedicente persona offesa magari era perfettamente consapevole della correttezza di quanto riportato dalla stampa, non determinerebbe l'applicazione della nuova regola.
Nel processo civile, invece, il presupposto del mero rigetto della domanda consentirà una applicazione meno sporadica.
Il disegno di legge inserisce altresì il c. 1 *bis* nell'art. 321 c.p.p. in base al quale il giudice può ordinare ai fornitori di servizi telematici e di telecomunicazione di rendere inaccessibili contenuti la cui libera circolazione possa aggravare o protrarre le conseguenze del reato o agevolarne la commissione di altri. La regola altro non è che un esempio di una recente tendenza: le soluzioni trovate dalla giurisprudenza vengono, in un secondo momento, cristallizzate nella in disposizioni di legge. Così è stato per questa.

11. Le pene per la diffamazione

Escludere la pena detentiva per i casi (più gravi) di diffamazione è stato il *casus belli*, la ragione dell'intervento della Corte costituzionale, che ha dato impulso all'iniziativa del legislatore. Non sorprende che il disegno di legge operi tra l'altro una rimodulazione complessiva dell'impianto sanzionatorio della materia. Vediamo come: la diffamazione semplice (art. 595, c. 1, c.p.) viene punita con la multa da 3.000 a 10.000 euro, aumentata della metà se l'offesa viene arrecata con qualunque mezzo di pubblicità o con atto pubblico (art. 595, c. 3, c.p.). Se poi la diffamazione è commessa con il mezzo della stampa o di un "prodotto editoriale registrato", la multa aumenta fino alla forbice tra 5.000 e 10.000 euro (art. 13, c. 1, legge stampa); qualora l'offesa consista anche in un fatto determinato falso, la cui diffusione sia avvenuta con la consapevolezza della falsità, la multa sale fino alla quantificazione da 10.000 a 50.000 euro (art. 13, c. 2, legge stampa). Alla condanna per tale delitto segue la pena accessoria dell'interdizione alla professione per un periodo da uno a sei mesi.
Si è già detto che la diffamazione costituita dalla diffusione di un fatto che l'autore sa falso potrebbe rientrare nei casi gravi che, secondo la giurisprudenza europea e oggi anche costituzionale, potrebbero meritare una sanzione afflittiva, fino a giungere alla detenzione, magari prevista solo in astratto, ovvero con meccanismi che la rendano in sostanza non applicata nel concreto, o almeno non automaticamente applicata.
Sappiamo qual è la *ratio* della riforma: chi esprime il proprio pensiero non deve essere terrorizzato all'idea di sbagliare, poiché altrimenti evita di rischiare nell'affrontare argomenti complessi e delicati, che tuttavia sono spesso quelli di maggior pubblico interes-

se. L'errore, dunque, non deve avere conseguenze catastrofiche per chi lo compie. Per questo motivo sanzioni detentive o pecuniarie assai elevate o anche alti risarcimenti, sono ritenuti contrari all'art. 10 Cedu e, quindi, in contrasto con la Costituzione.
In quest'ottica sanzioni più afflittive possono essere viceversa previste per condotte non solo gravi, ma anche frutto di una precisa volontà di screditare o di distruggere l'immagine di una persona. Certamente, la diffusione di un fatto offensivo e falso, da parte di chi è consapevole della sua falsità, può essere ritenuta condotta estranea rispetto a quelle "tutelate" dalla disposizione della Convenzione, fattispecie che quindi può essere dotata di una sanzione davvero afflittiva.
Destano invece perplessità le tariffe penali previste per la diffamazione punita dall'art. 595 c.p., non tanto per la cifra prevista nel massimo, quanto nel minimo. La sanzione più mite per una offesa recata tramite la stampa è di 5.000 euro, cui si deve aggiungere il risarcimento alla persona offesa. Non sarà difficile giungere alla "somma" totale, in concreto di 10.000 euro, cui vanno naturalmente aggiunte le spese di difesa legale.
È ragionevole ritenere che la maggior parte dei piccoli editori non riescano a sopportare più di qualche condanna di queste pur minime "dimensioni", tenuto conto della cornice edittale. Inoltre, come scriveva qualche anno fa Stefano Rodotà riprendendo un celebre saggio di Giorgio Bocca, «il padrone diventa padrone in redazione perché, nel momento in cui cresce il rischio di impresa a causa dei risarcimenti dei danni che gli possono essere chiesti in base a quella disciplina [n.d.r. si riferiva a una progettata riforma della pubblicazione delle intercettazioni], vorrà controllare di più. Avrà un'occasione in più per chiedere di contare»[36].
Inoltre, proprio la previsione di una seria pena pecuniaria a carico del presunto diffamatore potrebbe indurre il soggetto che si ritiene leso a percorrere la via penale anziché quella civile, con un'inversione di tendenza rispetto agli ultimi decenni, che hanno registrato un progressivo spostamento delle controversie per diffamazione dalle aule penali a quelle civili. Infatti, la minaccia della sanzione pecuniaria – assai più concreta di quella invero ipotetica della pena detentiva – potrebbe indurre gli indagati ad accordarsi con le persone offese, anche di fronte a rischi ridotti di soccombenza. Questo possibile effetto della riforma meriterebbe forse un approfondimento in sede legislativa, specie poiché la politica del diritto sembra da tempo orientata a una deflazione dei processi penali.
Soprattutto, la previsione di pene pecuniarie elevate, del risarcimento del danno e, nei casi più gravi, della pena accessoria dell'interdizione dalla professione di giornalista per un periodo da un mese a sei mesi possono far dubitare della conformità della normativa *in itinere* con la giurisprudenza della Corte di Strasburgo che, come si è ricordato, adotta criteri stringenti nella valutazione della proporzionalità della restrizione anche in relazione all'entità delle pene pecuniarie e dei risarcimenti. Di qui il rischio di nuovi ricorsi e nuove condanne, specie se saranno approvati gli emendamenti presentati al Senato, che mirano a rendere le sanzioni pecuniarie ancora più afflittive.
Insomma, la Corte di Strasburgo ha passato il testimone ai giudici di merito che lo hanno consegnato alla Corte costituzionale, che a sua volta l'ha passato al Parlamento,

[36] S. Rodotà, *I media e la sovranità popolare*, in *Supplemento a Critica liberale*, 2010, 173-174 e ora in E. Marzo, *I diritti dei lettori. Una proposta liberale per l'informazione in catene*, Milano, 2020, 120.

a cui tocca quest'ultima frazione, determinante per portare a termine la gara. Se fossimo davvero in una competizione, non si può dire che l'allenatore abbia affidato il rush finale al fuoriclasse della squadra.

Social media e responsabilità penale dell'*Internet Service Provider*[*]

Sofia Braschi

Abstract

Il saggio affronta il tema della responsabilità penale dell'*Internet Service Provider*, approfondendo il ruolo dei *social media* nel contrasto ai reati commessi nella rete. Dopo avere dato conto delle caratteristiche essenziali del *Web 2.0*, l'Autrice analizza i più recenti orientamenti della giurisprudenza italiana relativi alla responsabilità dell'amministratore del *blog*, per passare poi a considerare i contenuti della *Netzwerkdurchsetzungsgesetz*, entrata in vigore in Germania il 1° ottobre 2017, e i progetti di legge in discussione in questo paese, che mirano a sanzionare i gestori delle piattaforme attive nel *dark web*. L'indagine evidenzia il progressivo superamento del modello di disciplina delineato dalla direttiva 2000/31/CE e suggerisce alcune riflessioni conclusive intorno alla necessità di adeguare la normativa vigente all'attuale realtà economico-sociale.

The paper addresses the criminal liability of the Internet Service Provider, focusing on the role of social media in tackling cybercrime. After considering the main features of Web 2.0, the Author examines the most recent Italian judgments on the liability of the blog administrator. The essay then explores the contents of the Netzwerkdurchsetzungsgesetz, which came into force in Germany on 1 October 2017, as well as the recent German bills aimed at punishing providers operating on the dark web. The study highlights the constant overcoming of the rules defined by Directive 2000/31/EC and suggests some final reflections, whose aim is to adapt the current legislation to the economic and social reality.

Sommario

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

Keywords

responsabilità penale dell'*internet service provider* - *social media* - diffamazione - *Netzwerkdurchsetzungsgesetz* - *dark web.*

1. Premessa.

Alcuni recenti orientamenti legislativi e giurisprudenziali suggeriscono di tornare a riflettere sul ruolo dell'*Internet Service Provider* (di seguito ISP) nel contrasto ai reati commessi all'interno del *web*.

Con riferimento al versante legislativo, possiamo menzionare l'esempio offerto dalla Germania, ove il *Bundestag* ha introdotto a carico dei gestori di *social network* di grandi dimensioni una serie di obblighi volta ad assicurare l'efficace funzionamento dei meccanismi di segnalazione e rimozione dei contenuti illeciti immessi nella rete[1]; sempre in questo paese sono inoltre in discussione due proposte di legge che mirano a sanzionare gli amministratori delle piattaforme *online* in cui si svolgono traffici criminali[2].

Quanto invece alla giurisprudenza, è sufficiente osservare che all'interno del nostro sistema va consolidandosi un'interpretazione vieppiù restrittiva del d. lgs. 9 aprile 2003, n. 70, di attuazione della direttiva 2000/31/CE, con una conseguente contrazione delle aree di impunità tradizionalmente riservate agli ISP.

Se indubbiamente questi indirizzi segnano un passo in avanti rispetto alla disciplina eurounitaria, va peraltro evidenziato che essi riflettono una più generale tendenza alla responsabilizzazione dei prestatori di servizi nella rete. In effetti, malgrado la mancata revisione della summenzionata direttiva sul commercio elettronico, la Commissione Europea ha affermato la necessità che le piattaforme *online* siano «proattive nell'eliminazione dei contenuti illegali»[3] e, in linea con questa impostazione, la recente direttiva 2019/790/UE sulla protezione del diritto d'autore ha sensibilmente incrementato i doveri di collaborazione dei *provider*[4]. In maniera ancor più netta, la Corte Europea

[1] È opportuno evidenziare che anche nel nostro paese sono state avanzate proposte di legge intese a implementare la tutela degli utenti delle reti sociali: in questa prospettiva si consideri il d.d.l. n. 3001, comunicato alla Presidenza il 14 dicembre 2017, il quale replicava il modello di disciplina frattanto adottato in Germania (*Atti parlamentari (Senato della Repubblica), XVII legislatura, Disegni di leggi e relazioni*, stampato n. 3001), e il d.d.l. n. 2688, comunicato alla Presidenza il 7 febbraio 2017, il quale proponeva invece l'introduzione di due nuove fattispecie incentrate sulla diffusione di notizie false e stabiliva alcuni obblighi in capo ai gestori delle piattaforme sociali, come quello di rettifica delle false informazioni e di rimozione dei contenuti diffamatori circolanti nella rete (*Atti parlamentari (Senato della Repubblica), XVII legislatura, Disegni di leggi e relazioni*, stampato n. 2688). Infine, sottolineiamo che nel senso di una maggiore responsabilizzazione dei gestori dei *social network* si è orientato anche il legislatore francese con la *loi n° 2018-1202* del 22 dicembre 2018.

[2] Si allude ai disegni di legge BR-Drs. 33/19 e IT-SiG 2.0, a proposito dei quali *infra*, § 7.

[3] Così si legge nella COM (2017) 555 (*Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni* "*Lotta ai contenuti illeciti online. Verso una maggiore responsabilizzazione delle piattaforme online*"), 21.

[4] L'art. 17 della direttiva 2019/790/UE del 17 aprile 2019 stabilisce infatti che le piattaforme di *file-sharing* non beneficiano delle esenzioni stabilite dalla direttiva sul commercio elettronico. La responsabilità per la condivisione non autorizzata di materiali protetti da diritto d'autore è comunque esclusa se il gestore

dei Diritti dell'Uomo ha ripetutamente censurato la creazione di aree di impunità in favore dei prestatori di servizi nella rete, così addirittura sollecitando un ripensamento generale del diritto dell'Unione[5].

Dinanzi al quadro tratteggiato, sembra utile fare il punto sulle attuali tendenze relative alla responsabilità degli ISP e cercare di delineare i possibili sviluppi della materia. Nelle pagine che seguono approfondiremo dunque il ruolo dei gestori dei *social media* nel contrasto ai reati commessi nella rete: inizieremo richiamando alcuni profili generali della responsabilità dei fornitori di servizi *internet* nell'ambito del c.d. *Web 2.0*[6]; quindi esamineremo gli orientamenti emersi nella nostra giurisprudenza penale con riferimento alla punibilità dei *blogger* per gli illeciti realizzati dagli utenti, per passare poi a considerare il modello di disciplina proposto dalla "legge per il miglioramento della tutela dei diritti sui *social networks*" (*Netzwerkdurchsetzungsgesetz*), entrata in vigore in Germania il 1° ottobre 2017. Per finire, faremo alcuni cenni alle problematiche inerenti ai *provider* che svolgono un'attività essenzialmente criminale; i risultati dell'indagine costituiranno la base per una breve riflessione intorno alle linee evolutive della materia.

2. La responsabilità dell'ISP nell'era del *Web 2.0*: inquadramento del tema.

Che l'assetto normativo disegnato dalla direttiva sul commercio elettronico sia stato superato dall'evoluzione tecnologica è un dato oramai ampiamente acquisito all'interno della comunità giuridica. È infatti noto che con l'avvento del c.d. *Web 2.0* l'attività svolta dai *provider* è andata incontro a una profonda mutazione, di talché solo in parte essa può attualmente essere descritta ricorrendo alle categorie – *mere conduit*, *hosting* e

del sito dimostra 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 [abbia] ricevuto le informazioni pertinenti e necessarie dai titolari dei diritti»; in ogni caso, il *provider* non risponde se prova «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». Va peraltro precisato che, a norma dell'art. 2, n. 6, 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».

[5] Di particolare importanza è la sentenza della Grande Camera nel caso *Delfi c. Estonia*, ric. 64569/09 (2015), con la quale i giudici di Strasburgo hanno affermato la compatibilità con l'art. 10 CEDU, relativo alla libertà di espressione, della condanna al risarcimento del danno emessa nei confronti di un portale d'informazione per la mancata rimozione dei contenuti illeciti pubblicati dagli utenti; sulla sentenza e sui successivi orientamenti della Corte EDU R. Petruso, *Responsablità delle piattaforme* online, *oscuramento di siti* web *e libertà d'espressione nella giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *Dir. inf.*, 5, 2018, 520 ss.

[6] Con questa espressione s'intende «un sistema di interconnettività ove gli utenti non sono più solamente destinatari di contenuti, ma possono interagire immettendo essi stessi materiali in forma di testi, video, musica o immagini, con dinamiche comunicative» (S. Seminara, Internet, in *Enc. dir.*, 2014, Ann. VII, 568).

caching – utilizzate dal legislatore dei primi anni duemila[7]. Mentre l'espansione della "mediasfera"[8], derivante dalla comparsa nel mercato di nuovi strumenti tecnologici (*smartphone*, *tablet*) e dalla capillare diffusione di quelli più tradizionali, ha determinato il venir meno delle esigenze economico-sociali che avevano giustificato l'adozione di quella disciplina[9].

Ciò nondimeno, il Parlamento Europeo non è ancora approdato a una revisione organica della normativa; il dibattito all'interno dell'Unione si è concentrato invece sulla soddisfazione di specifici bisogni di protezione, essenzialmente collegati all'utilizzo delle reti sociali[10]. Si è invero osservato che, nei *social network*, la possibilità per l'utente di nascondere la propria identità personale, unita alla facoltà di scegliere la propria rete di connessioni, agisce da detonatore rispetto a fenomeni che attingono beni personali d'importanza primaria (si allude soprattutto alla realtà dei cosiddetti "discorsi d'odio", ma la considerazione vale anche per i più tradizionali reati di opinione[11]). Mentre il sempre maggiore ricorso ai *social media* come strumenti di informazione aumenta il rischio di diffusione di notizie false (le c.d. *fake news*), con notevoli ricadute sulla tenuta democratica delle istituzioni[12]. Donde l'assunzione di iniziative volte a contrastare le forme più aggressive o menzognere di comunicazione nella rete[13].

---

[7] Così, *ex multis*, L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi-S. Canestrari-A. Manna-M. Papa (diretto da), Cybercrime, Torino, 2019, 87; S. Seminara, Internet, cit., 601; R. Flor, Social networks *e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità dei fornitori del servizio?*, in *Riv. trim. dir. pen. ec.*, 3, 2012, 673 ss.

[8] L'uso di questa espressione per individuare «un ambiente […] in cui i media elettronici in rete giocano un ruolo fondamentale» è mutuato da R. De Simone, *Presi nella rete. La mente ai tempi del* web, Milano, 2012, 11, secondo il quale «la fase attuale è caratterizzata da un'ubiquità dei media che non ha precedenti nella storia. […] Siamo immersi in permanenza nella mediasfera».

[9] Nella dottrina penalistica, per tutti, L. Picotti, *Diritto penale e tecnologie*, cit., 87; nella letteratura civilistica, per un'analoga considerazione e una sintetica esposizione delle ragioni ispiratrici della direttiva 2000/31/CE R. Panetta, *Il ruolo dell'*internet service provider *e i profili di responsabilità civile*, in *Resp. civ. e prev.*, 3, 2019, 1019 ss.; in tema vd. anche M. Montanari, *La responsabilità delle piattaforme* on-line *(il caso di Rosanna Cantone)*, in *Dir. inf.*, 2, 2017, 256-257.

[10] Va detto che questo approccio trova riscontro all'interno della giurisprudenza della Corte Europea dei Diritti dell'Uomo, la quale, in ossequio al principio di proporzione, diversifica i criteri di responsabilità dei *provider* in relazione ai singoli fenomeni criminali: su questa base, ad esempio, accoglie soluzioni maggiormente responsabilizzanti ogniqualvolta viene in rilievo il fenomeno dell'incitamento all'odio e alla violenza (sul punto R. Petruso, *Responsabilità delle piattaforme* online*,* cit., 534-535).

[11] In argomento A. Spena, *La parola(-)odio*, in *Criminalia*, 2016, 579-580; da ult. V. Nardi, *I discorsi d'odio nell'era digitale: quale ruolo per l'*internet service provider?, in *Dir. pen. cont.*, 7 marzo 2019, 6-7. In aggiunta alle considerazioni riportate nel testo, si può evidenziare che l'avvento delle reti sociali sembra avere favorito anche la crescita dei movimenti negazionisti: in tema G. Ziccardi, *Il negazionismo in* Internet*, nel* deep web *e sui* social network*: evoluzione e strumenti di contrasto*, in *notizie di Politeia*, 2017, 108 ss.

[12] Secondo un'impostazione piuttosto diffusa, riconducibile alla letteratura nordamericana, le *fake news* consistono in «articoli recanti notizie che sono intenzionalmente e verificabilmente false e potrebbero trarre in inganno i lettori»; sul punto e per approfondimenti relativi alle ricadute costituzionali di questo fenomeno G. Pitruzzella, *La libertà di informazione nell'era di* Internet, in *Parole e potere. Libertà di espressione,* hate-speech *e* fake-news, Milano, 2017, ora in *questa Rivista*, 1, 2018, 13 ss. Per un inquadramento del tema nella prospettiva penale, invece, T. Guerini, *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle* fake news *e delle infodemie*, in *disCrimen*, 15 giugno 2020, 11 ss.

[13] A tal proposito si segnala che la Commissione Europa ha promosso, in collaborazione con alcuni colossi del *web* e del *social networking*, la redazione e applicazione di un codice di condotta (*Code of conduct countering illegal hate speech online*) volto a contrastare il fenomeno dei discorsi d'odio. Maggiori dettagli

Di fronte dell'inerzia del legislatore, il nostro diritto pretorio ha preso dunque ad allargare l'ambito di responsabilità dei *provider*. Valorizzando le indicazioni provenienti dalle Corti superiori, la giurisprudenza dapprima ha ricondotto i portali di informazione *online* entro il perimetro dell'art. 57 c.p.[14], quindi – ed è questo il problema che c'interessa adesso analizzare – ha incominciato a delineare criteri di imputazione affatto originali per gli illeciti commessi nelle reti sociali. È chiaro, peraltro, che una simile operazione deve fare i conti con i limiti posti dal diritto positivo; pertanto, occorre verificare la fondatezza a livello sistematico di queste soluzioni e la loro compatibilità con i principi stabiliti dalla direttiva 2000/31/CE. Prima di procedere in tale direzione, è opportuno però precisare le nozioni di *social network* e riepilogare i tratti salienti della disciplina vigente, di cui occorre tenere conto per inquadrare l'attività di questi *provider*; senza trascurare inoltre che nella giurisprudenza civile va consolidandosi un'interpretazione evolutiva del d. lgs. 70/2003.

Iniziando dal concetto di *social network*, in un'accezione più lata l'espressione viene utilizzata come sinonimo di *social media*, per individuare tutti i siti la cui caratteristica principale consiste nell'offerta di uno spazio virtuale, all'interno del quale gli utenti hanno la possibilità di comunicare e condividere contenuti[15]. È bene precisare che, sotto questo profilo, reti come *Facebook* e *Twitter* non si differenziano da altri *user content aggregator service provider*, quali piattaforme di *video-sharing* o *blog* che contengono aree a disposizione per i commenti dei lettori; rispetto a tali figure, essi si contraddistinguono essenzialmente per la possibilità riconosciuta al singolo fruitore di creare un'identità personale e una rete di contatti con la quale condividere le proprie connessioni[16]. Data l'ampiezza della nozione, non sorprende che alla denominazione di *social network* possano essere ricondotti siti che variano notevolmente per i temi oggetto della comunicazione così come per il regolamento economico-contrattuale. Sotto il primo profilo, occorre invero considerare che mentre alcune piattaforme hanno un contenuto generalistico (ad esempio *Facebook*), altre mettono in collegamento i membri di una comunità definita (si pensi ad *Academia.edu*) ovvero toccano specifici ambiti della vita sociale (come quello professionale: così *LinkedIn*); non mancano nemmeno *network*

possono essere rinvenuti alla pagina *The EU Code of conduct on countering illegal hate speech online*; per un quadro più completo delle iniziative assunte all'interno dell'Unione nella lotta all'*hate speech* V. Nardi, *I discorsi d'odio*, cit., 8-9. Infine, con riferimento alle proposte di regolamentazione volte a contrastare il fenomeno delle *fake news* nel quadro europeo, E. Lehner, Fake-news *e democrazia*, in *questa Rivista*, 1, 2019, 98 ss.

[14] Questo filone giurisprudenziale è stato inaugurato da Cass. pen., 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. Per un commento critico sul tema 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.

[15] Alcuni autori utilizzano in questo senso solo l'espressione *social media*: per una simile e più opportuna soluzione, C. Fuchs, *La politica economica dei* social media, in *Sociologia della comunicazione*, 43, 2012, 62; la definizione proposta nel testo si trova ad esempio in S. Martinelli, *L'autorità privata del* provider, in P. Sirena-P. Zoppini (a cura di), *I poteri privati e il diritto della regolazione*, Roma, 2018, 556 s.

[16] Sul punto e per una panoramica dell'evoluzione storica delle reti sociali G. Riva, *I* social network, in *Manuale di informatica giuridica e diritto delle nuove tencologie*, a cura di M. Durante-U. Pagallo, Torino, 2012, 467 ss.; la definizione richiamata nel testo è accolta anche da E. Rosati-G. Sartor, Social networks *e responsabilità del* provider, in *EUI working papers*, LAW 2012/05, 1-2. Nella dottrina penalistica vd. L. Picotti, *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. mer.*, 12, 2012, 2523B.

focalizzati sulla vendita di beni o servizi (ad esempio, *Airbnb*) ovvero sullo scambio di determinate tipologie di contenuti (come fotografie – *Instagram* – e materiali audiovisivi – *TikTok*). A livello economico, invece, accanto a *social network* che offrono un servizio gratuito e traggono utilità dalla profilazione degli utenti e dalla vendita delle relative informazioni (è il caso di *Facebook*), vi sono piattaforme che guadagnano dall'attività pubblicitaria (ad esempio *Youtube*) ovvero mettono in comunicazione i soggetti interessati alla vendita e all'acquisto di un bene, ottenendo un profitto dalle singole transazioni (si pensi ad *Airbnb*).

Venendo adesso al quadro normativo, bisogna anzitutto premettere che l'attività del fornitore di servizi di *social networking* può essere ricondotta all'interno del d. lgs. n. 70/2003; è noto che tale normativa si basa sul principio di neutralità del *provider* e in maniera coerente con questo presupposto esclude la responsabilità del fornitore di servizi per la memorizzazione prolungata o temporanea di contenuti illeciti. Più nel dettaglio, premessa la mancanza di un «obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza», il d. lgs. 70/2003 all'art. 16 stabilisce che il prestatore di servizi della società dell'informazione 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[17].

Tuttavia, dinanzi alla obsolescenza della vigente disciplina, la giurisprudenza civile ha preso ad elaborare diversi criteri di imputazione[18]. Invero, alcune sentenze hanno recepito la nozione di "*host provider* attivo" elaborata dalla Corte di Giustizia dell'Unione Europea per individuare le situazioni in cui il *provider* agisce sui dati memorizzati al fine di ottimizzarne la fruizione[19], concludendo che i gestori delle piattaforme di

[17] È opportuno precisare che l'art. 14, c. 1, lett. *b)* della direttiva 2000/31/CE stabilisce invece che il *provider* non è responsabile delle informazioni memorizzate, sempreché, una volta al corrente del fatto che l'attività o l'informazione è illecita, egli «agisca immediatamente per rimuovere le informazioni o disabilitarne l'accesso».

[18] Per una breve panoramica di questi orientamenti R. Bocchini, *La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP*, in *Giur. it.*, 12, 2019, 2607-2608. È opportuno evidenziare che il modello di responsabilità del *provider* elaborato dalla giurisprudenza viene generalmente condiviso, sia pur con diverse sfumature, dalla dottrina: oltre all'Autore appena citato (2610 ss.), vd., *ex multis*, R. Panetta, *Il ruolo dell'*internet service provider, cit., 1019 ss.

[19] La nozione di "*host provider* attivo" è stata accolta da Cass. civ., sez. I, 21 febbraio 2019, n. 7708, in *Riv. dir. ind.*, 4-5, 2019, II, 201; fra i giudici di merito Trib. Roma, sez. XVII, 12 luglio 2019, n. 14757, in *Guida dir.*, 41, 2019, 49. Con riferimento invece alla giurisprudenza della Corte di Lussemburgo, vd. spec. CGUE, C-324/09, *L'Oréal SA e a. c. eBay Inernational AG e a.* (2011); è opportuno segnalare che l'orientamento secondo cui l'art. 14 della direttiva sul commercio elettronico si applica solo agli "*host provider* passivi" è stato recentemente avallato pure dalla Commissione europea, nella citata COM (2017) 555. Per completare il quadro, ricordiamo infine che il ridimensionamento del principio di neutralità del prestatore di servizi nella rete ha interessato anche l'attività dei motori di ricerca: nella nota pronuncia CGUE, C-131/2012, *Marjo Costela Gonzalez e AEPD c. Google Spain e Google Inc.* (2014), la Corte di Giustizia dell'Unione Europea ha riconosciuto in capo al *provider* l'obbligo, a determinate condizioni, di procedere alla cancellazione dei dati personali del richiedente, osservando che, «nella misura in cui l'attività di un motore di ricerca può incidere [...] sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca […] deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46». Questo principio è stato peraltro recepito dal regolamento UE 2016/679, che all'art. 17 disciplina il cosiddetto "diritto all'oblio".

social networking non possono beneficiare dei *safe harbours* previsti dalla direttiva[20]. Nella medesima prospettiva, ma in maniera meno radicale, un più recente indirizzo giurisprudenziale afferma che, a prescindere dalla sua natura, il *provider* ha l'obbligo di rimuovere i contenuti illeciti di cui sia venuto a conoscenza, senza che sia necessaria una formale richiesta dell'autorità giudiziaria[21]. A questo proposito si è infatti evidenziato che l'assetto definito dal d. lgs. 70/2003 è incapace di apprestare una tutela efficace a interessi di natura personale, come l'immagine o la reputazione, con riferimento ai quali ogni protrazione dell'illecito rischia di determinare un danno irreparabile[22]; si è così asserito che la richiesta del privato va ritenuta sufficiente a far scattare l'obbligo del prestatore di eliminare i contenuti oggetto di segnalazione, e conseguentemente a determinare l'insorgere di una responsabilità civile nel caso di loro intempestiva rimozione.

3. Il ruolo dell'amministratore del *blog* nella giurisprudenza penale: vecchi problemi...

Sul versante penale, negli ultimi anni la questione del ruolo dei gestori delle reti sociali è stata affrontata con esiti innovativi all'interno di due sentenze relative alla responsabilità dell'amministratore del *blog* per la mancata rimozione dei contenuti illeciti pubblicati dagli utenti. Tali pronunce devono essere attentamente esaminate perché, sebbene siano relative a uno specifico mezzo di comunicazione (il *blog*), esse contengono principi teoricamente suscettibili di trovare applicazione anche agli altri *social media*. In via preliminare è opportuno rammentare che, esclusa l'applicabilità dell'art. 57 c.p., l'opinione prevalente in dottrina e in giurisprudenza riconduceva l'attività del gestore del diario virtuale entro l'ambito di applicazione del d. lgs. 70/2003; in maniera coerente con questa impostazione, la responsabilità del *blogger* era dunque limitata ai casi di partecipazione attiva agli illeciti commessi dagli utenti[23]. Superando questa impostazione, la Suprema Corte ha invece ritenuto punibile per diffamazione il titolare della piattaforma che mantiene in rete i commenti offensivi pubblicati dai lettori. Poiché, peraltro, per approdare a questa conclusione i giudici di legittimità hanno seguito percorsi differenti, è opportuno esaminare partitamente le due decisioni; iniziamo dun-

[20] Così Trib. Milano, 9 settembre 2011, n. 10893, in *Riv. dir. ind.*, 6, 2011, II, 364 ss. e 7 giugno 2011, n. 7680; più di recente App. Milano, 7 gennaio 2015, in *Riv. dir. ind.*, 1, 2017, II, 4 ss.

[21] Così Trib. Roma, sez. IX, 15 febbraio 2019, n. 3512, in *Riv. dir. ind.*, 4-5. 2019, II, 296; App. Firenze, sez. II, 11 aprile 2018, n. 862; Trib. Napoli Nord, 3 novembre 2016, in *Dir. inf.*, 2, 2017, 243 ss.; Trib. Roma, sez. IX, 27 aprile 2016, n. 8437; Trib. Milano, 7 giugno 2011, n. 7680.

[22] Sul punto Trib. Napoli Nord, 3 novembre 2016, cit., ove si afferma che, «venendo in rilievo diritti della personalità (quali l'immagine, il decoro, la reputazione, la riservatezza), appare irrazionale dover attendere un ordine dell'autorità, il quale potrebbe intervenire quando oramai i diritti in questione sono irrimediabilmente pregiudicati e non più suscettibili di reintegrazione».

[23] In dottrina 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 s.; 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, 1076-1077; in giurisprudenza vd. invece Cass. pen., sez. V, 16 luglio 2010, n. 35511, in *Riv. it. dir. proc. pen.*, 4, 1604 ss.; cfr. Cass. pen., sez. V, 19 febbraio 2018, n. 16751, in *Cass. pen.*, 11, 2018, 3743 ss.

que trattando della prima e rimandiamo al paragrafo che segue l'esame della soluzione più recente.

Al fine di affermare la responsabilità dell'amministratore del *blog*, la Corte di Cassazione (Cass. pen., sez. V, 14 luglio 2016, n. 54946) nel suo primo arresto ha ritenuto decisiva la mancata adozione delle iniziative necessarie ad evitare la protrazione dell'altrui reato di diffamazione. Partendo dal presupposto che, una volta venuto a conoscenza del carattere illecito della pubblicazione, il gestore del sito sia obbligato a porre fine alla violazione, si è concluso che questi risponde come concorrente nell'altrui reato.

Una simile ricostruzione presta però il fianco a molteplici obiezioni. Anzitutto, infatti, la punibilità *ex* art. 110 c.p. si infrange dinanzi alla istantaneità del reato di diffamazione: fissata la consumazione nella immissione in rete del contenuto lesivo, il suo mantenimento nel *web* da parte del gestore del sito costituisce una condotta susseguente, che giocoforza fuoriesce dallo schema del concorso di persone[24]. Inoltre, la configurazione di una responsabilità per omesso impedimento del reato cozza con l'impossibilità di affermare l'esistenza nel nostro sistema di una posizione di garanzia in capo al *provider*: tralasciando la possibilità di ricavare, nell'ambito delle normative di settore, degli specifici obblighi di protezione[25], il d. lgs. 70/2003 da un lato esclude un generale dovere di controllo del prestatore di servizi nella rete, dall'altro costituisce 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[26].

Per la verità, alla prima annotazione si potrebbe opporre che nella diffamazione a mezzo *internet* non è del tutto infondato parlare di permanenza della violazione, dal momento che, in casi come quello in esame, il reo mantiene il dominio sul fatto anche dopo la pubblicazione del contenuto lesivo dell'onore[27]. Del resto, sulla scorta di un'analoga considerazione, un'autorevole dottrina ha in passato argomentato il prolungamento della consumazione nelle ipotesi di cosiddetta diffamazione "per espo-

[24] Così già S. Seminara, *La responsabilità penale degli operatori* su internet, in *Dir. inf.*, 4-5, 1998, 765 s.; più di recente A. Ingrassia, *Responsabilità penale degli* internet service provider*: attualità e prospettive*, in *Dir. pen. proc.*, 12, 2017, 1625. Aperture nei confronti della configurabilità di una responsabilità «per omesso impedimento di protrazione *ex post*» del reato in R. Bartoli, *Brevi considerazioni sulla responsabilità penale dell'*internet service provider, in *Dir. pen. proc.*, 5, 2013, 606.

[25] Sul punto R. Flor, Social networks *e violazioni penali*, cit., 679, secondo il quale «a fronte dell'assenza di un obbligo generale di sorveglianza o di controllo "preventivo", sono state introdotte nuove norme in settori specifici, come nella lotta alla pedopornografia *on-line*, che prevedono puntuali doveri in capo al *service provider*, suscettibili di essere posti a fondamento di una responsabilità omissiva, sia autonoma, *ex* art. 40 cpv. c.p., che concorsuale, *ex* art. 110 c.p.».

[26] Escludono l'esistenza di una posizione di garanzia in capo al *provider*, *ex multis*, A. Ingrassia, *Responsabilità penale degli* internet service provider, cit., 1626 s.; Id., *Il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?*, in *Dir. pen. cont.*, 8 novembre 2012, 26 ss.; S. Seminara, Internet, cit., 597-598; R. Bartoli, *Brevi considerazioni*, cit., 602-603. Diversamente F. Sgubbi, *Parere* pro veritate, in *Dir. inf.*, 4-5, 2009, 746; L. Picotti, *Art. 600*-ter, *III comma c.p.*, in Cadoppi (a cura di), *Commentario delle norme contro la violenza sessuale e contro la pedofilia*, Padova, 2006, 210 ss.

[27] Va peraltro evidenziato che la ricostruzione accolta dalla sentenza in esame è ambigua, giacché la Suprema Corte non afferma il carattere permanente del reato, bensì radica la responsabilità sull'«aver l'imputato mantenuto consapevolmente l'articolo sul sito, consentendo che lo stesso esercitasse l'efficacia diffamatoria»; sottolinea questo aspetto A. Ingrassia, *Responsabilità penale degli* internet service provider, cit., 1625 ss.

sizione"[28]; pertanto, si potrebbe sostenere che l'internauta risponde di diffamazione per tutto il tempo in cui non rimuove il *post* illecito pubblicato sul *blog*. Senonché una simile ricostruzione trascurerebbe di considerare che un'interpretazione estensiva del "dominio sul fatto" risulta poco aderente alla realtà della comunicazione digitale, in cui è già la stessa nozione di autore a perdere di consistenza[29]; soprattutto, l'idea della permanenza del reato, unita alla mancanza di finitezza spazio-temporale della rete, è in grado di determinare un completo stravolgimento degli istituti collegati alla consumazione[30]. In effetti, è sufficiente riflettere sulle conseguenze derivanti con riferimento al diritto di querela e alla prescrizione per rendersi conto della natura dirompente di tale soluzione[31]; in definitiva, bisogna ammettere che è preferibile l'interpretazione che fissa il disvalore del reato nella diffusione del contenuto lesivo e conseguentemente afferma la natura istantanea della violazione[32].

Concludendo, la configurabilità di una responsabilità a titolo di concorso di persone va rifiutata alla luce della impossibilità di ricavare dal diritto positivo un generale obbligo di protezione in capo al *provider*; anche sotto questo profilo, non è dunque possibile sostenere che l'amministratore del *blog* risponde per omesso impedimento dell'altrui reato di diffamazione.

4. (*segue*) ...e nuove soluzioni.

Alla luce delle considerazioni che precedono non sorprende che, tornando sul tema, la Suprema Corte abbia da ultimo accolto una diversa soluzione: in un recente arresto

[28] Si allude alla distinzione fra pubblicazione "per distribuzione" e "per esposizione" enucleata da T. Padovani, *Il momento consumativo nei reati commessi col mezzo della stampa*, in *Riv. it. dir. proc. pen.,* 1971, 800 ss.; in generale, nel senso della configurabilità in forma permanente del reato di diffamazione, A. Pecoraro Albani, *Del reato permanente*, in *Riv. it. dir. proc. pen*., 1960, 421, il quale fa l'esempio di colui che ha cura di «mantenere esposto per lungo tempo sul balcone, al fine di ingiuriare il suo dirimpettaio, un bel paio di corna». Si evidenzia inoltre che nella giurisprudenza civile è diffusa l'idea del carattere permanente degli illeciti commessi nella rete (così, *ex multis*, Cass. civ., sez. I, 21 febbraio 2019, n. 7708, cit.); tale interpretazione riflette però la confusione fra permanenza del reato e delle sue conseguenze.

[29] In generale, sulla dissoluzione del testo nell'era della comunicazione digitale R. De Simone, *Presi nella rete*, cit., 114.

[30] Il rapporto fra il concetto di consumazione e il reato commesso nel *cyberspace* è approfondito soprattutto da L. Picotti, *Diritto penale e tecnologie*, cit., 89 ss., il quale però giunge a un'opposta conclusione: premessa l'opportunità di ricorrere alla distinzione fra perfezione e consumazione/esaurimento del reato, l'Autore conclude che «il reato cibernetico non può dirsi "esaurito" nel periodo intermedio anche assai lungo che può intercorrere fra i due momenti, in cui "permane" e si approfondisce l'offesa». Per ulteriori riflessioni intorno alla consumazione del reato di diffamazione a mezzo *Internet* sia consentito rinviare a S. Braschi, *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, Milano, 2020, 259 ss.

[31] Va infatti considerato che, secondo la giurisprudenza, il diritto di querela può essere esercitato fino alla cessazione della permanenza (sul punto, per tutti, C. Mazzucato, *Art. 124*, in G. Forti-S. Seminara-G. Zuccalà (a cura di), *Commentario breve al codice penale*, Milano, 2017, 557); in ogni caso, nell'ipotesi di scoperta tardiva del reato, si potrebbe giungere al risultato paradossale di punire una diffamazione anche a molti anni di distanza dalla pubblicazione nella rete del *post* illecito.

[32] Sul punto, per tutti, S. Seminara, *La responsabilità penale*, cit., 765, secondo cui "i reati (di condotta) fondati su verbi modali come diffondere, divulgare ecc. si consumano nel momento in cui i contenuti illeciti sono resi accessibili da parte del loro autore».

(Cass. pen., sez. V, 8 novembre 2018, n. 12546) è stato affermato che l'amministratore del *blog*, il quale non elimina i commenti offensivi pubblicati dagli utenti, risponde di un autonomo reato di diffamazione.

Ad avviso dei giudici di legittimità, creando e gestendo una piattaforma di comunicazione, l'amministratore del *blog* tiene un comportamento positivo, che contribuisce alla circolazione del contenuto prodotto dall'utente; ne deriva che, nel caso in cui venga informato dalla natura illecita della pubblicazione, il gestore del sito può essere considerato responsabile di un nuovo reato di diffamazione. Rispetto alla precedente ricostruzione, la novità consiste dunque nell'inquadramento della condotta del *blogger* all'interno della responsabilità commissiva e nell'attribuzione ad essa di un'autonoma rilevanza penale; in questo modo si ritiene possibile aggirare l'obiezione secondo cui il diritto vigente non pone in capo al *provider* nessun obbligo di protezione, che giustifichi la configurazione di una responsabilità a titolo di concorso di persone.

Per la verità, la qualificazione in termini autonomi del comportamento dell'amministratore del sito, che non rimuove i contenuti pubblicati dagli utenti, non rappresenta un'assoluta novità; al contrario, essa trova un importante precedente giurisprudenziale nella sentenza relativa al caso noto come *Google vs Vividown*[33]. In quell'occasione, infatti, i giudici di legittimità sostennero che, una volta informato della illiceità dei contenuti ospitati sul proprio portale, il gestore della piattaforma di *video-sharing* acquisisce la qualifica di "responsabile del trattamento" e per questa ragione risponde del reato previsto dall'art. 167 d. lgs. 30 giugno 2006, n. 196. Peraltro, una simile ricostruzione sembra oggi confortata dal disposto dell'art. 17 della direttiva (UE) 2019/790, a norma del quale la condotta del *provider* che ospita un contenuto sul proprio portale deve essere trattata alla stregua di «un atto [positivo] di condivisione al pubblico»[34].

Nemmeno questa soluzione risulta però convincente.

Anzitutto si potrebbe obiettare che, dal punto di vista sistematico, non trova conferma l'obbligo dell'ISP di rimuovere i contenuti lesivi dell'onore, che siano oggetto di segnalazione da parte dell'utente. Per comprendere il significato di questa osservazione occorre considerare che gli artt. 14-*ter* e -*quater* l. 3 agosto 1998, n. 269, e l'art. 1, c. 2, d.l. 18 febbraio 2015, n. 7, stabiliscono che i siti contenenti materiale pedopornografico ovvero implicati nella commissione di reati di terrorismo siano inseriti in un apposito elenco presso il Ministero degli interni e oscurati su richiesta dell'autorità giudiziaria. Sembra dunque del tutto irragionevole che, proprio nei casi di diffamazione, in cui si rende necessario contemperare interessi di rango costituzionale, spetti invece interamente al gestore della piattaforma di comunicazione verificare l'esistenza del reato[35].

---

[33] Si tratta di Cass. pen., sez. III, 17 dicembre 2013, n. 5107, in *Riv. pen.*, 5, 2014, 495; va peraltro precisato che in quest'ultimo caso, a differenza che nella vicenda in esame, la Suprema Corte affermò la configurabilità di una responsabilità penale in capo al *provider* per la sua mancata attivazione, sul presupposto di una previa comunicazione da parte dell'autorità competente. Sul punto, per alcune brevi considerazioni, A. Ingrassia, *Responsabilità penale degli* internet service provider*,* cit., 1623 s.

[34] I contenuti essenziali della direttiva sono riportati *retro*, nt. 4.

[35] Invero, l'impostazione accolta dal d. lgs. 70/2003, che, come visto sopra, all'art. 16 subordina l'obbligo di attivazione del *provider* alla richiesta dell'autorità amministrativa o giudiziaria, risponde «allo scopo di rafforzare la determinatezza della fattispecie, evitando al *provider* l'onere di autonome iniziative con i connessi rischi di una responsabilità risarcitoria» (S. Seminara, Internet, cit., 603).

In secondo luogo, il ragionamento seguito dalla Corte di Cassazione appare fragile: non è infatti chiaro come mai, in assenza di un obbligo di rimozione, l'automatico, ininterrotto funzionamento dei meccanismi di diffusione dei dati nella rete possa acquisire un'autonoma tipicità penale[36]. A tacer del fatto che una simile ricostruzione svuota di significato il concetto di azione[37], essa è contraddetta dalla circostanza che, come visto, per sanzionare la mancata rimozione dei contenuti illeciti già oggetto di memorizzazione, il legislatore abbia avvertito la necessità di introdurre un apposito obbligo di attivazione (art. 16, c. 1, lett. *b)*, d. lgs. 70/2003). La verità è che la ricostruzione proposta dai giudici di legittimità costituisce un *escamotage* volto ad aggirare il principio secondo cui il dovere d'intervento del *provider* presuppone una comunicazione dell'autorità giudiziaria: in altri termini, la Suprema Corte ha cercato di trasferire sul piano penale l'orientamento accolto dalla giurisprudenza civile, secondo cui è sufficiente la segnalazione del privato perché scatti l'obbligo di eliminare le informazioni illecite memorizzate[38]. È chiaro, però, che una simile operazione cozza con l'art. 25 Cost., configurando una forma di responsabilità priva di fondamento legale; per questo motivo, la soluzione proposta dalla Cassazione non può essere accettata.

Giunti a questo punto, per completare il quadro sembra opportuna una breve riflessione sulla figura dell'"*host provider* attivo"; si è visto sopra che questa nozione viene utilizzata per individuare i fornitori di servizi nella rete che non svolgono attività meramente automatiche e passive e che perciò dovrebbero rimanere estranei all'ambito di applicazione del d. lgs. 70/2003. A tal proposito va premesso che lo scopo della costruzione è quello di ovviare ai limiti della disciplina vigente, adattando il modello di allocazione dei rischi connessi all'utilizzo di *internet* all'attuale realtà delle reti sociali: poiché, infatti, questi *provider* traggono profitto dalla elaborazione delle informazioni prodotte dagli utenti[39], si ritiene che essi siano tenuti anche a sostenere i costi derivanti dalla realizzazione di fatti pregiudizievoli per i fruitori[40]. Fatta questa precisazione,

[36] A tal proposito, la S.C. si limita ad affermare che «se […] il gestore del sito apprende che sono stati pubblicati da terzi contenuti obiettivamente denigratori e non si attiva tempestivamente a rimuovere tali contenuti, finisce per farli propri e quindi per porre in essere ulteriori condotte di diffamazione, che si sostanziano nell'aver consentito, proprio utilizzando il suo *web-log*, l'ulteriore divulgazione delle stesse notizie diffamatorie».

[37] Sul tema vd. le considerazioni di S. Seminara, Internet, cit., 570, secondo cui «la nozione di condotta […] richiede sempre un dominio dell'agente sul fatto, che preclude ogni sua dilatazione diretta a comprendere ulteriori effetti collegati al funzionamento di *Internet* e all'operato di ulteriori *server* o all'attività degli utenti».

[38] Considerazioni analoghe, con riferimento però alla sentenza esaminata nel paragrafo che precede, si rinvengono in R. Carbone, *Responsabilità del* blogger: *parziale* revirement *della Cassazione?*, in *Cass. pen.*, 7-8, 2017, 2787 s.

[39] Fermo restando quanto abbiamo evidenziato *supra* con riferimento alla estrema varietà dei *social network*, vd., per approfondimenti sul meccanismo di sfruttamento economico dei dati degli utenti da parte di siti come *Facebook*, S. Sica-G. Giannone Codiglione, Social network sites *e il "labirinto" delle responsabilità*, in *Giur. mer.*, 12, 2012, 2716 ss.; più in generale, per un'analisi critica del modello economico caratteristico del c.d. capitalismo dell'informazione C. Fuchs, *La politica economica dei* social media, cit., 74 ss.

[40] Così, sostanzialmente, R. Bocchini, *La responsabilità civile plurisoggettiva*, cit., 2608 ss.; sul punto, ampiamente, F. Di Ciommo, *Programmi-filtro e criteri di imputazione/esonero della responsabilità* on-line. *A proposito della sentenza Google/Vividown*, in *Dir. inf.*, 6, 2010, 853, secondo cui «in una situazione legislativa in cui ai *provider* non si chiede un controllo sui contenuti veicolati in *Internet* […] nessuno è incentivato

va evidenziato che un ragionamento non dissimile potrebbe trovare spazio anche in campo penale: poiché, infatti, la finalizzazione delle piattaforme sociali a uno scopo di profitto può porre queste in conflitto con le esigenze di protezione degli interessi degli utenti[41], appare tutt'altro che irragionevole imporre ai gestori dei siti obblighi di attivazione eventualmente presidiati dalla sanzione penale. Tuttavia, è chiaro che un simile discorso si inscrive in un orizzonte di politica criminale, mentre il ricorso alla nozione di "*host provider* attivo" non può giustificare l'applicazione di criteri d'imputazione *de iure condito* privi di fondamento legale: in mancanza di un intervento del legislatore, resta dunque necessario fare riferimento alle comuni regole in tema di concorso di persone, verificando alla luce della struttura della piattaforma sociale il contributo effettivamente apportato alla commissione del reato.

In conclusione, la ricostruzione offerta dalla Suprema Corte non può essere condivisa, giacché si pone in contrasto col diritto positivo, in base al quale il *provider* è tenuto a rimuovere i contenuti illeciti immessi nella rete previa richiesta dell'autorità giudiziaria. Fissato questo punto, occorre peraltro riconoscere che l'attuale sviluppo delle piattaforme sociali suggerisce di meditare sulla opportunità di riformare la disciplina vigente; come anticipato, in questa direzione si è già mosso il legislatore tedesco, approdando a una soluzione affatto originale, che è opportuno adesso esaminare.

5. Un possibile modello di disciplina? I contenuti della *Netzwerkdurch-setzungsgesetz*

Come accennato in apertura del lavoro, il tema del contrasto ai reati commessi nelle reti sociali è stato al centro di un recente intervento del legislatore tedesco, sfociato nell'adozione della *Netzwerkdurchsetzungsgesetz* (di seguito NetzDG). Scopo dichiarato della disciplina è quello di implementare la corretta interazione degli utenti nei *social network*, contrastando le forme più aggressive di comunicazione ovvero la diffusione di *fake news*[42]; la legge presenta però un ben più ampio raggio d'azione[43].

Procedendo a una sommaria esposizione dei suoi contenuti, bisogna anzitutto dire che la NetzDG trova applicazione ai *social network* con più di due milioni di utenti registrati

ad investire in *software* o strategie aziendali in grado, se non proprio di eliminare, di limitare il rischio costituito da illeciti commessi da utenti rimasti anonimi. […] Tutto ciò aumenta certamente le possibilità che in rete vengano commessi illeciti senza che nessuno risponda del relativo danno e, dunque, contribuisce ad aumentare la sensazione di deresponsabilizzazione che l'utente provoca mentre naviga».

[41] Esemplare in questo senso è la vicenda di Tiziana Cantone, giovane donna ritratta in alcuni video pornografici amatoriali successivamente diffusi nella rete: per ottenere la rimozione delle pagine che la rigurdavano, frattanto diventate di grande successo nella rete, la ragazza dovette affrontare una dura battaglia legale contro *Facebook*, la quale fu portata a termine dalla madre dopo il suo suicidio. Per un breve resoconto della storia e dei suoi risvolti a livello penale G. M. Caletti, *"Revenge porn" e tutela penale*, in *Dir. pen. cont.- Riv. trim.*, 3, 2018, 65 ss.

[42] BT-Drucksache 18/12356, 11 s. Per una panoramica del contesto nel quale si inscrive l'intervento normativo, per tutti, S. Müller-Franken, *Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Verfassungsrectliche Fragen*, in *Archiv für Presserecht*, 1, 2018, 1 ss.

[43] Per questa annotazione, con accento critico, vd. già le osservazioni della *Deutsche Gesellschaft für Recht und Informatik* (*Stellungnahme der DGRI zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG)*, in *Computer und Recht*, 2017, 311).

in Germania; è bene inoltre precisare che la legge accoglie una definizione ampia di *social network*, riferendosi ai «fornitori di servizi di telecomunicazione che per scopo di profitto gestiscono piattaforme *internet* progettate per permettere agli utenti di condividere qualunque tipo di contenuto o di renderlo accessibile al pubblico» (§ 1 NetzDG)[44].
A carico di questi *provider* vengono posti due obblighi fondamentali: da un lato, essi sono chiamati a svolgere un resoconto semestrale sull'attività di gestione delle segnalazioni effettuate dagli utenti con riferimento alla presenza di contenuti antigiuridici nella rete; dall'altro, devono adottare procedure trasparenti ed efficaci per la rimozione di tale materiale. Per individuare la nozione di "contenuti antigiuridici", la legge fa rimando ad alcune disposizioni del codice penale: senza pretesa di esaustività si possono ricordare i §§ 86 e 86a, relativi all'utilizzo di simboli e propaganda politica vietata, il § 111, che incrimina il pubblico incitamento alla violenza, i §§ 184b e 184d concernenti la pubblicazione e la detenzione di materiale pedopornografico, e i §§ 185-187, in tema di ingiuria e diffamazione. La violazione degli obblighi menzionati configura un illecito amministrativo punito con una sanzione pecuniaria, che nei casi più gravi può raggiungere l'importo di cinque milioni di euro; la legge trova applicazione anche agli illeciti commessi all'estero (§ 4 NetzDG)[45].
La scelta del legislatore tedesco è stata dunque quella di rendere obbligatoria l'adozione di misure di *notice and take down*, a tale scopo indicando alcuni principi generali che devono essere seguiti dai *provider*. Invero, la NetzDG stabilisce che i gestori delle reti sociali devono predisporre procedure di segnalazione e rimozione facilmente accessibili e tempestive; soffermandoci su quest'ultimo punto, la legge impone termini stringenti per la rimozione dei materiali oggetto di segnalazione: ventiquattro ore nelle ipotesi di illiceità manifesta, sette giorni negli altri casi. Essa inoltre stabilisce che, ogniqualvolta la liceità del contenuto dipende dalla veridicità di una dichiarazione, il *social network* può sollecitare la replica dell'autore (§ 3 NetzDG); per la soluzione dei casi più controversi la legge prevede infine che venga interpellato un organo di autoregolamentazione indipendente appositamente creato[46].
Come si vede, la NetzDG non interviene sulla responsabilità penale del gestore della rete sociale, la cui punibilità rimane dunque circoscritta ai casi di consapevole mancata rimozione dei contenuti illeciti oggetto di segnalazione, secondo quanto previsto dalla *Telemediengesetz*[47]; né essa intacca il principio secondo cui il *provider* non è tenuto ad effet-

[44] Vengono dunque esclusi i quotidiani *online* (per i quali vige un più severo regime di responsabilità penale) e le piattaforme di comunicazione individuale (si pensi a *Whatsapp*), mentre sono ricompresi, ad esempio, siti di *e-commerce* come *eBay*; sul punto G. Nolte, *Hate-Speech, Fake-News, das «Netzwerkdurchsetzungsgesetz» und Vielfaltsicherung durch Suchmaschinen*, in *Zeitschrif für Medienwissenschaft*, 2017, 555, il quale peraltro evidenzia la scarsa determinatezza della disposizione e il suo difetto di corrispondenza col linguaggio comune, presso il quale la nozione di *social network* assume un significato più circoscritto (sul punto *retro*, § 2).

[45] Con riferimento alle sanzioni occorre inoltre considerare che il § 30, c. 2, *Ordnungswidrigkeitengesetz* consente di aumentare fino a dieci volte l'importo massimo della sanzione pecuniaria prevista dalla legge.

[46] Sul punto vd. il § 3, c. 3, lett. *b)* e c. 6, ove sono specificati i requisiti necessari per l'accreditamento dell'organo di autoregolamentazione.

[47] Così chiaramente G. Nolte, *Hate-Speech*, cit., 553. Bisogna ricordare che l'attività del gestore del *social network* ricade all'interno del § 10 *Telemediengesetz*, il quale limita la punibilità dell'*host provider* ai casi

tuare alcun controllo preventivo sui contenuti pubblicati dagli utenti. La legge rafforza invece i doveri di intervento *ex post* dei gestori delle reti sociali, spostandoli dal campo dell'autoregolamentazione a quello della responsabilità amministrativa[48]; la notevole severità della sanzione dovrebbe assicurare il rispetto da parte dei *provider* delle prescrizioni stabilite dalla normativa.

Vero ciò, va peraltro considerato che, non di rado, la violazione degli obblighi che abbiamo riferito potrà emergere in occasione dei giudizi civili o penali concernenti i "contenuti antigiuridici" oggetto di segnalazione. Sotto questo profilo, il modello di responsabilità introdotto dalla NetzDG potrebbe essere accostato a quello previsto per gli enti dal § 30 *Ordnungswidrigkeitengesetz* (di seguito OWiG)[49]: anche nel caso in esame, infatti, la responsabilità amministrativa si salda con quella della persona fisica derivante dalla commissione di un reato. Inoltre, sul piano politico-criminale, si è già evidenziato che l'assoggettamento a sanzione dei gestori della rete sociale si fonda sulla considerazione che questi *provider* traggono profitto dall'attività svolta dai fruitori[50]; né si può trascurare che l'adozione di *policy* maggiormente restrittive nella rimozione dei contenuti illeciti è in grado, se non di eliminare, quantomeno di limitare significativamente le offese prodotte con le singole violazioni. Poiché, però, la responsabilità amministrativa regolata dal § 30 OWiG, a differenza di quella prevista dalla NetzDG, necessariamente presuppone la commissione di un reato e uno stretto collegamento fra la società e il suo autore, mentre un simile legame manca tra il fornitore del servizio di *social networking* e il singolo utente della rete, non è possibile spingere oltre il parallelismo fra i due meccanismi di imputazione.

6. (*segue*) e le sue criticità

Passando a valutare la bontà della disciplina che abbiamo illustrato, va detto che sin dalla presentazione del relativo progetto di legge, la NetzDG ha sollevato molteplici perplessità, essenzialmente dipendenti dalla sua asserita incompatibilità col diritto eurounitario e costituzionale[51].

in cui la mancata tempestiva rimozione del contenuto illecito è sorretta da dolo diretto; a differenza che nel nostro sistema, per la responsabilità del fornitore di servizi nella rete non è peraltro necessaria una segnalazione istituzionale della illiceità del contenuto. Per una panoramica sui presupposti della responsabilità dell'*host provider* in Germania, per tutti, J. Eisele, *vor § 184*, in A. Schönke-H. Schröder (a cura di), *Strafgesetzbuch Kommentar*, München, 2019, 1876 s., *Rn.* 84 ss.

[48] Evidenzia questo aspetto G. Nolte, *Hate-Speech, Fake-News*, cit., 555, secondo il quale sarebbe stato più opportuno intervenire rimanendo nel campo dell'autoregolamentazione. Con specifico riferimento al rapporto fra NetzDG e responsabilità civile del *provider* cfr. K. N. Peifer, *Fake News und Providerhaftung. Warum das NetzDG von Fake News die falschen Instrumente liefert*, in *Computer und Recht*, 12, 2017, 811 s.

[49] Per una sintetica illustrazione del sistema di responsabilità amministrativa degli enti in Germania e per ampi riferimenti bibliografici G. Heine/B. Weißer, *Vorbem. §§ 25 ff.*, in A. Schönke-H. Schröder, *Strafgesetzbuch Kommentar*, cit., 513 ss., *Rn.* 121 ss.; nella letteratura italiana V. Mongillo, *La responsabilità penale tra individuo ed ente collettivo*, Torino, 2018, 243 ss.

[50] Cfr., sul duplice scopo «preventivo-repressivo» e «di riequilibrio economico» del modello punitivo delineato dal § 30 OWiG, V. Mongillo, *La responsabilità penale*, cit., 246-247.

[51] Una panoramica completa dei profili di ritenuta illegittimità della NetzDG si rinviene in V. Claussen, Fake-news*, pluralismo informativo e responsabilità in rete*, in *questa Rivista*, 3, 2018, 119 ss.

Sotto il primo profilo, si è infatti sostenuto che la legge sarebbe contraria al principio della libera circolazione dei prestatori dei servizi dell'informazione, stabilito dall'art. 3 della direttiva 2000/31/CE; si è poi argomentato che la NetzDG contrasterebbe con l'art. 17 della stessa direttiva, secondo cui l'obbligo di rimozione presuppone una "conoscenza effettiva" della illiceità della comunicazione; infine, si è affermato che, individuando termini perentori per la rimozione dei contenuti, la nuova normativa violerebbe la regola secondo cui l'azione del *provider* è illecita (solo) se intempestiva[52].
Ancora più articolate le obiezioni relative alla conformità della normativa alla Costituzione, a proposito delle quali ci limitiamo ad alcuni brevi cenni. Le critiche principali riguardano il pericolo di una eccessiva compressione alla libertà di manifestazione del pensiero: si osserva infatti che la previsione di termini stringenti, unita alla prospettiva di incorrere in responsabilità per la mancata rimozione dei contenuti illeciti, non potrebbe che avere l'effetto di sollecitare l'adozione da parte dei *provider* di atteggiamenti fortemente censori[53]; inoltre, il sistema delineato dalla legge sarebbe discutibile anche sotto il profilo della cessione a soggetti privati del potere, di natura tipicamente pubblicistica, di accertare la liceità di una determinata comunicazione[54].
Iniziando dai dubbi relativi al diritto eurounitario, le obiezioni che abbiamo sinteticamente riferito sembrano superate alla luce degli orientamenti assunti dalla Commissione Europea, che con la raccomandazione approvata il 1° marzo 2018 ha invitato gli Stati membri e i *provider* a cooperare per l'adozione di procedure di *notice and take down* efficaci e trasparenti[55]; sotto questo profilo, si potrebbe persino affermare che la normativa tedesca si candida a rappresentare un modello per gli altri paesi dell'Unione.
Più delicata è, invece, la questione relativa ai rischi di un'eccessiva limitazione della libertà di espressione. Alle obiezioni che abbiamo riferito si potrebbe invero controbattere che la legge fonda la responsabilità del *social network* sulla mancata adozione di procedure efficaci e tempestive di segnalazione e rimozione dei contenuti antigiuridici, mentre prescinde dal giudizio relativo alla correttezza delle singole statuizioni; per questo motivo, non vi sarebbe alcun pericolo di un controllo pervasivo sulle comunicazioni[56]. Quanto poi all'attribuzione ai *provider* di prerogative tipiche del potere giudi-

[52] Per queste obiezioni vd. G. Spindler, *Internet Intermediary Liability Reloaded. The New German Act on Responsibility of Social Networks and its (In-)Compatibility with European Law*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2, 2017, 167 ss.

[53] S. Müller-Franken, *Netzwerkdurchsetzungsgesetz*, cit., 7 ss.; l'Autore punta il dito, fra l'altro, sul c.d. "*overblocking*", cioè sul possibile oscuramento di contenuti leciti, volto a minimizzare il rischio di incorrere in responsabilità. Per meglio comprendere le preoccupazioni alla base di queste obiezioni, possono riportarsi le considerazioni di E. Rosati - G. Sartor, Social networks *e responsabilità del* provider, cit., 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». Ampie considerazioni critiche in merito ai rischi di una eccessiva limitazione della libertà di manifestazione del pensiero si trovano anche in G. Nolte, *Hate-Speech, Fake-News*, cit., 557 ss.

[54] In proposito, per tutti, S. Müller-Franken, *Netzwerkdurchsetzungsgesetz*, cit., 5 ss.

[55] *Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online*, art. 1.

[56] A. Lang, *Netzwerkdurchsetzungsgesetz und Meinungsfreiheit. Zur Regulierung privater Internet-Intermediäre bei der Bekämpfung von Hassrede*, in *Archiv des Öffentlichen Recht*, 2, 2018, 227 ss., secondo cui la NetzDG realizza un bilanciamento ragionevole fra l'esigenza di assicurare la libertà d'espressione e quella di

ziario, la legge si limiterebbe a recepire un sistema oramai radicato nel mondo delle reti sociali, all'interno delle quali sono già da tempo operativi meccanismi di monitoraggio e rimozione dei contenuti pubblicati dagli utenti[57]; oltretutto, nel procedere in questa direzione, la NetzDG si sarebbe preoccupata di assicurare l'intervento dello Stato, prevedendo l'istituzione di un'apposita autorità indipendente chiamata a dirimere i casi più controversi.

Tali osservazioni sono indubbiamente ragionevoli. Vero ciò, va peraltro riconosciuto che la questione del ruolo dei *provider* nella individuazione della liceità delle comunicazioni "non manifestamente antigiuridiche" e in specie di quelle afferenti all'area della pubblica informazione chiama in causa problemi estremamente delicati di tutela dell'ordinamento democratico. Data la complessità della materia, a proposito della quale si registra una notevole diversità di opinioni anche presso la nostra letteratura costituzionale [58], è opportuno astenerci dal prendere una posizione sul punto. Volendo nondimeno stilare un bilancio conclusivo, si può affermare che la NetzDG sembra in grado di assicurare una tutela più effettiva dei diritti degli utenti della rete; quantomeno con riferimento alle ipotesi di manifesta antigiuridicità del contenuto, essa configura dunque un modello di disciplina meritevole di essere preso in considerazione anche nel nostro paese[59].

7. Cenni al fenomeno del *dark web* e le sue possibili implicazioni in campo penale

Prima di svolgere alcune riflessioni conclusive, per completare la nostra analisi intorno alla responsabilità dei *provider* sembra utile aprire una breve parentesi relativa al fenomeno del c.d. *dark web*. Invero, l'affermazione del *Web 2.0* sembra avere avuto come conseguenza collaterale l'espansione di quest'area della rete: l'avversione nei confronti del modello economico-sociale delle grandi piattaforme di *social networking*, unito all'insofferenza verso le relative *policy* in tema di trattamento dei dati personali, ha spinto molti utenti ad abbandonare il lato più "superficiale" del *web*[60]. A ciò si aggiunge che, al

tutelare i beni giuridici eventualmente aggrediti nella rete.

57 A. Lang, *Netzwerkdurchsetzungsgesetz*, cit., 237 ss.

58 Propone l'introduzione di «Istituzioni specializzate, terze e indipendenti (giudici o autorità indipendenti) che, sulla base di principi predefiniti, intervengano successivamente, su richiesta di parte e in tempi rapidi, per far rimuovere dalla rete quei contenuti che sono palesemente falsi o llegali o lesivi dei diritti fondamentali e della dignità umana» G. Pitruzzella, *La libetà di informazione*, cit., 26; decisamente critico nei riguardi dell'idea di istituire autorità indipendenti competenti ad accertare la veridicità delle informazioni diffuse nelle reti sociali, invece, N. Zanon, Fake-news *e diffusione dei* social media*: abbiamo bisogno di un'"Autorità Pubblica della Verità"?*, in *questa Rivista*, 2, 2018, 13 ss.

59 Ritiene che la NetzDG sia in grado di funzionare con riferimento ai reati d'odio e a fattispecie come la pornografia minorile, meglio di quanto non possa fare a proposito delle *fake news* K. N. Peifer, *Fake News und Providerhaftung*, cit., 811.

60 Così sostanzialmente R. Gehl, *Power/freedom on the dark web: a digital ethnography of the dark Web social Network*, in *New media & society*, 18, 2016, 3 ss. Sul punto vd. anche il *reportage* realizzato da C. Frediani, Deep web. *La rete oltre Google. Personaggi, storie, luoghi dell'*internet profonda, Genova, 2014, 56. L'Autrice intervista gli amministratori di alcune piattaforme attive nel *deep web*; fra le varie testimonianze, si segnala quella riportata nelle pp. 55-56, ove l'intervistato afferma: «È come tornare a prima dell'*internet* per idioti.

fine di contrastare i traffici illegali situati nel *dark web*, in Germania sono state avanzate due proposte di legge incentrate sulla incriminazione dei gestori delle piattaforme che operano in questa parte della rete; anche sotto il profilo politico-criminale, il tema appare dunque collegato all'oggetto delle nostre riflessioni.

In via preliminare sono opportune alcune informazioni tecniche relative al fenomeno di cui parliamo. Con l'espressione *dark web* s'intende usualmente indicare il complesso di siti presenti nel *deep web*, che sono utilizzati per la realizzazione di attività criminali; a sua volta il *deep web* corrisponde alla parte di *internet* che non può essere raggiunta con i comuni motori di ricerca, bensì tramite *browser* – il più famoso dei quali è TOR ("*The Onion Router*") – che assicurano il pieno anonimato degli utenti[61]. TOR consente infatti di nascondere l'identità di tutti i soggetti coinvolti nella comunicazione, criptando i relativi indirizzi IP; nella rete TOR non operano inoltre i comuni programmi di indicizzazione, sicché l'unico modo per raggiungere un determinato sito è quello di essere indirizzati dagli utenti che ne conoscono la "collocazione". Poiché, infine, nel *dark web* le operazioni commerciali vengono usualmente svolte con *bitcoin* o altre criptovalute, non è possibile risalire all'identità degli internauti nemmeno ricostruendo i relativi movimenti finanziari[62].

Alla luce delle annotazioni che precedono, non sorprende che il *dark web* costituisca un habitat particolarmente favorevole per la proliferazione di attività criminali, come la vendita di armi o di stupefacenti, lo scambio di materiale pedopornografico o l'offerta di servizi di *hacking*[63]. A titolo esemplificativo, possiamo ricordare il caso di *Silk Road*, sito attivo dal 2011 al 2014 e specializzato nella vendita internazionale di droga[64]; ma anche nel nostro paese sono stati recentemente scoperti mercati illegali che hanno luogo negli ambiti più reconditi della rete[65]. Poiché, peraltro, il fenomeno del *dark web* costituisce un'assoluta novità, difetta ancora una piena consapevolezza delle sue possibili implicazioni in campo penale[66].

[…] Prima della bolla speculativa, del *web 2.0*, dei markettari, dei *social*. Qui non hai la pappa pronta con motori che ti dicono cosa cercare. […] La Rete doveva essere un posto di liberazione per tutti […] ma quell'ideale si è perso».

[61] Per una breve – ma esaustiva – panoramica del fenomeno L. Greco, *Strafbarkeit des Unterhaltens einer Handels- und Diskussionplattform insbesondere im sog. Darknet*, in *Zeitschrift für Internationale Strafrechtsdogmatik*, 9, 2019, 436 ss.; per approfondimenti sul funzionamento tecnico della rete TOR, invece, R. Dingledine-N. Mathewson-P. Syverson, *Tor:_The_Second-Generation_Onion_Router*, 1 ss.

[62] Sul punto M. Bachmann-N. Arslan, *"Darknet"-Handelsplätze für kriminelle Waren und Dienstleistungen: ein Fall für den Strafgesetzgeber?*, in *Neue Zeitschrift für Strafrecht*, 7, 2019, 242.

[63] È necessario rimarcare la complessità della realtà di cui parliamo, all'interno della quale si rinvengono infatti anche *forum* destinati allo scambio di informazioni e al dibattito politico (vd. la letteratura citata nella nt. 61); significativo, sotto questo punto di vista, è il fatto che, in tempi recenti, testate giornalistiche di fama internazionale abbiano scelto di utilizzare il *dark web* per la divulgazione delle proprie notizie: *The New York Times is Now Available as a Tor Onion Service*, 27 ottobre 2017.

[64] Per approfondimenti sulla storia di *Silk Road*, C. Frediani, Deep web, 14 ss.; in proposito vd. anche L. Trautman, *Virtual currencies, Bitcoin & What Now After Liberty Reserve, Silk Road and Mt. Gox?*, in *Richmond Journal of Law and Technology*, 20, 2014, 91 ss.

[65] A conferma di ciò *Armi, droga, documenti falsi: bloccato «Berlusconi market», l'emporio italiano del* dark web, in *Il Sole 24 ore*, 7 novembre 2019.

[66] Nel nostro sistema, l'utilizzo della rete TOR o di altri *browser* equivalenti sembra assumere una specifica rilevanza in sede di commisurazione della pena: l'art. 602-*ter* c. 9 c.p. stabilisce infatti che

Soffermandoci brevemente sul punto, abbiamo già accennato al fatto che in Germania sono stati presentati ben due progetti di legge, i quali prevedono specifiche incriminazioni volte a sanzionare l'organizzazione e gestione di piattaforme dirette all'agevolazione di traffici criminali[67]. Più nel dettaglio, mentre una prima proposta fa riferimento esclusivo all'offerta di servizi all'interno del *dark web* ed è circoscritta ai siti che agevolano la commissione di determinate fattispecie relative alla vendita di merci illegali, il secondo disegno di legge mira invece a sanzionare anche le piattaforme attive nel *surface web* e non contempla limitazioni basate sulla tipologia dei reati oggetto di agevolazione[68].

In entrambi i casi, il fondamento delle proposte consiste nell'asserita difficoltà di punire a titolo di concorso di persone l'amministratore del sito ove si svolgono le attività criminose; con specifico riferimento al *dark web*, si ritiene che l'assoluta impossibilità di risalire all'identità degli internauti e all'oggetto delle relative comunicazioni non consenta di affermare la ricorrenza del dolo di partecipazione in capo a chi gestisce la piattaforma sociale. A questa considerazione si aggiunge inoltre che la stessa creazione di siti in cui l'incontro fra le parti avviene con la massima garanzia dell'anonimato avrebbe come effetto quello di incentivare la commissione di reati; donde l'opportunità di svincolare la punibilità del *provider* dal concorso nella commissione di specifici illeciti[69].

Così ricostruiti i lineamenti essenziali delle proposte, possiamo osservare che la creazione di un'autonoma fattispecie offre indubbi vantaggi sul piano probatorio; a un esame più approfondito, però, non sembra che essa configuri una soluzione convincente. Invero, nei casi di piattaforme come *Silk Road*, specializzate nella vendita di determinate merci illegali, la direzione finalistica delle condotte poste in essere dall'amministratore del sito consente di ritenere integrati i presupposti della responsabilità concorsuale nel reato commesso dagli utenti, essendo irrilevante l'ignoranza degli specifici contenuti delle singole transazioni; ne discende che colui che crea o gestisce una piattaforma di comunicazione diretta allo svolgimento di traffici criminali potrà rispondere come agevolatore delle singole violazioni poste in essere dagli internauti (ad esempio, traffico di sostanze stupefacenti *ex* art. 73 d.p.r. 9 ottobre 1990, n. 309). Come si vede, dun-

le sanzioni previste per i reati in materia di prostituzione e pornografia minorili siano aumentate «in misura non eccedente i due terzi» se i fatti sono «compiuti con l'utilizzo di mezzi atti ad impedire l'identificazione dei dati di accesso alle reti telematiche». È peraltro evidente che i problemi connessi al *dark web* non attengono unicamente al piano della severità della risposta punitiva.

[67] Per una panoramica sul contesto nel quale si inseriscono le due proposte di legge, la cui presentazione è stata incentivata dalla scoperta, successiva all'attentato commesso nel 2016 a Monaco di Baviera, dei legami fra *dark web* e terrorismo internazionale, L. Greco, *Strafbarkeit des Unterhaltens*, cit., 435.

[68] Nel dettaglio, la prima proposta, di iniziativa parlamentare, prevede l'introduzione di un nuovo §126a, volto a sanzionare «colui che offre servizi *internet*, l'accesso o il raggiungimento dei quali avviene mediante particolari misure tecniche di sicurezza e il cui scopo o la cui attività sono diretti a rendere possibile o a rafforzare la commissione di fatti antigiuridici»; individua inoltre la nozione di «fatti antigiuridici» richiamandosi ad alcune fattispecie in tema di vendita di sostanze stupefacenti, medicinali, armi ed esplosivi. Il secondo disegno di legge, invece, presentato dal Ministero degli interni, prende in considerazione la condotta di chi «mette a disposizione di terzi un servizio su *internet* il cui scopo o la cui attività è diretta a consentire, promuovere o agevolare la commissione di atti illeciti». Per un confronto fra le due proposte vd. M.A. Zöller, *Strafbarkeit und Strafverfolgung des Betreibens internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen*, in *Kriminalpolitische Zeitschrift*, 5, 2019, 277 ss.

[69] BR-Drs. 33/19, *Gesetzentwurf*, 4 ss.

que, in relazione a ipotesi come questa non è possibile affermare l'esistenza di lacune di tutela da colmare[70]. Le fattispecie contemplate nei summenzionati progetti di legge potrebbero assolvere invece a una vera e propria funzione di incriminazione nei casi in cui le piattaforme siano prive di una specifica connotazione criminale e nondimeno vengano utilizzate per la realizzazione di illeciti; poiché, però, con riferimento ai siti attivi nel *dark web* trovano applicazione i medesimi principi che governano la responsabilità dei *provider* che operano nella parte visibile della rete, non è possibile svincolare la punibilità dei gestori delle piattaforme dalla consapevole fornitura di un apporto attivo alla realizzazione di un reato[71]. In definitiva, la circostanza che un sito sia raggiungibile esclusivamente tramite TOR o altri programmi di criptazione dei dati, di per sé non giustifica l'applicazione di un diverso regime di responsabilità penale; deve dunque escludersi l'opportunità di fare propri i contenuti dei progetti di legge attualmente in discussione in Germania.

Concludendo, bisogna osservare che il fenomeno del *dark web* porta in primo piano un problema che, sebbene presente anche nella parte più visibile della rete[72], assume qua una portata decisiva: si tratta della estrema difficoltà di risalire all'identità dei responsabili delle singole violazioni[73]. A ben guardare, infatti, l'ineffettività della tutela penale non dipende tanto dall'esistenza di lacune sul piano del diritto sostanziale, bensì dalla mancanza di appropriati strumenti di indagine[74]. È chiaro, peraltro, che l'approfondimento di quest'ultimo tema comporterebbe una deviazione eccessiva dall'oggetto delle nostre riflessioni; pertanto, non resta adesso che chiudere la parentesi relativa al *dark*

---

[70] Così M. Bachmann-N. Arslan, *"Darknet"-Handelsplätze für kriminelle Waren*, 244; più ampiamente L. Greco, *Strafbarkeit des Unterhaltens*, cit., 443 ss. Una conferma di questa osservazione è offerta dai giudizi che hanno interessato i gestori delle piattaforme attive nel *dark web*, i quali si sono conclusi tutti con la pronuncia di sentenze di condanna (addirittura all'ergastolo, per il giovane creatore del sito *Silk Road*: *Ergastolo per il fondatore di* Silk Road*, il mercato nero del* web, in *la Repubblica*, 30 maggio 2015).

[71] Sul punto L. Greco, *Strafbarkeit des Unterhaltens*, cit., 440, il quale efficacemente nota: «offrire un'infrastruttura, nella quale acquirenti e venditori esercitano i loro commerci, non basta perché si possa parlare di complicità. Altrimenti anche il gestore di un club nel quale notoriamente si spaccia droga o di una stazione dove si esercita la prostituzione dovrebbe rispondere come concorrente».

[72] Il tema è troppo ampio per poter essere affrontato in questa sede. Sul punto ci limitiamo a osservare che alle criticità che generalmente affliggono la prova digitale (in proposito, per tutti, G. Di Paolo, *Prova informatica (diritto processuale penale)*, in *Enc. dir.*, Annali VI, 2013, 737 ss.), si aggiungono quelle derivanti dalla peculiare conformazione del mercato delle reti sociali: dal momento che i *server* dei grandi *provider* sono generalmente situati all'estero, il mezzo per ottenere i dati ivi contenuti consiste nella rogatoria internazionale; senonché il buon esito di questa procedura è condizionato dalla legislazione dello Stato in cui si trova il soggetto raggiunto dalla richiesta di informazioni e dal suo atteggiamento più o meno collaborativo. Sul punto e più in generale sulle indagini nell'ambito dei *social network*, C. Conti-M. Torre, *Spionaggio informatico nell'ambito dei* social network, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, 2014, 415 ss.

[73] Ad oggi, il modo più efficace per penetrare all'interno del *dark web* consiste nello svolgimento di indagini sotto copertura, a cui si aggiunge lo sfruttamento dei dati postali per localizzare i destinatari delle merci acquistate nei mercati illegali. Sul punto M. Bachmann-N. Arslan, *"Darknet"-Handelsplätze für kriminelle Waren*, cit., 244 s.; un resoconto delle indagini svolte dalla polizia americana nel caso *Silk Road* si trova invece in C. Frediani, Deep web, cit., 20 ss.

[74] Considerazioni analoghe in M. Bachmann-N. Arslan, *"Darknet"-Handelsplätze für kriminelle Waren*, cit., 246, secondo i quali le «parole-chiave» sono «personale specializzato, migliori attrezzature tecniche, formazione continua, cooperazione più forte a livello internazionale»; conf. M. A. Zöller, *Strafbarkeit und Strafverfolgung*, cit., 281.

web e passare ad abbozzare alcune riflessioni conclusive intorno al ruolo dei *provider* nell'ambito del *Web 2.0*.

8. Considerazioni conclusive

Volendo tracciare un bilancio conclusivo, bisogna anzitutto sottolineare che l'analisi svolta ha confermato il progressivo superamento dell'assetto normativo definito nei primi anni duemila: come efficacemente affermato da Rodotà, risulta oramai radicata l'idea secondo cui «il ricorso all'algoritmo non può divenire una forma di deresponsabilizzazione dei soggetti che lo adoperano»[75].

Più nel dettaglio, l'indagine ha consentito di fare luce sul cedimento nel nostro sistema del principio secondo cui l'*host provider* è tenuto a rimuovere le informazioni illecite solo in seguito alla comunicazione delle autorità competenti (art. 16 d. lgs. 70/2003)[76]; si è invero visto che la giurisprudenza civile e quella penale convergono nell'affermare la responsabilità del fornitore di servizi nella rete anche nei casi in cui ricorre la sola segnalazione del privato. Le ragioni alla base di questi orientamenti sono state illustrate: da un lato, l'enorme grado di diffusione della tecnologia digitale comporta che, a fronte della commissione di un illecito, sia essenziale un intervento tempestivo di rimozione dei materiali antigiuridici caricati nel *web*; dall'altro, la conformazione delle reti sociali, caratterizzate dallo sfruttamento economico dei contenuti prodotti dagli utenti, giustifica l'assegnazione in capo ad esse di più penetranti doveri di attivazione.

Al contempo, però, abbiamo osservato che una simile situazione rende imprescindibile un intervento del legislatore; a tacer d'altro, una volta che si riconosca la necessità di superare l'attuale disciplina, bisogna affrontare alcune importanti questioni. In primo luogo, infatti, occorre verificare se risulti ancora funzionale il tradizionale modello di imputazione incentrato sul paradigma partecipativo. Invero, la punibilità a titolo di concorso di persone deve fare i conti con la necessaria ricorrenza in capo al fornitore di servizi nella rete di requisiti di carattere soggettivo, il cui accertamento raramente è possibile nel caso dei grandi *provider* che operano in contesti essenzialmente legali; alla luce di tale considerazione, la soluzione, accolta dal legislatore tedesco, di fondare la responsabilità degli ISP sul mancato adempimento di obblighi strutturali aventi ad oggetto la predisposizione di procedure efficienti di segnalazione e rimozione dei contenuti illeciti pubblicati dagli utenti appare un'opzione tutt'altro che irragionevole.

Un secondo interrogativo riguarda la possibilità di una diversificazione della disciplina basata sulle finalità perseguite dalle singole piattaforme e sulle relative disponibilità economico-finanziarie[77]. Infine, bisogna stabilire se rimettere interamente al gestore

[75] S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, 403.

[76] Si è già accennato al fatto che tale previsione riflette una scelta del legislatore nazionale, limitandosi l'art. 14, c. 1, lett. *b)* della direttiva 2000/31/CE a richiedere la conoscenza da parte del *provider* della illiceità delle informazioni; sul punto *retro*, nt. 17.

[77] Come visto, tale è stata la scelta del legislatore tedesco. Sottolinea la necessità di distinguere "piccoli" e "grandi *provider*" F. Di Ciommo, *Oltre la direttiva 2000/31/Ce, o forse no. La responsabilità dei* provider *di* Internet *nell'incerta giurisprudenza europea*, in *Foro it.*, 1, 2019, 2072; invece, sulla possibilità di operare «differenziazioni a seconda che l'attività sia svolta o no a fini di lucro» vd., in termini dubitativi, S.

della rete la valutazione relativa alla liceità dei contenuti oggetto di segnalazione ovvero adottare l'impostazione accolta dal legislatore tedesco, che come visto ha stabilito l'intervento di un'autorità indipendente per la soluzione dei casi più difficili[78].

Ciò precisato, due ulteriori considerazioni sono necessarie. La prima concerne il ruolo sussidiario della responsabilità del fornitore di servizi nella rete: bisogna infatti evidenziare che l'unico modo per assicurare l'effettività della tutela penale consiste nella individuazione e punizione dell'autore principale del reato commesso nel *web*. Sotto questo profilo, il tema della punibilità del *provider* appare collegato a quello relativo ai poteri dell'autorità giudiziaria e si manifesta l'importanza di una riflessione aggiornata sugli strumenti a disposizione per il contrasto ai reati commessi su *internet*.

La seconda considerazione attiene invece alla necessità di un ripensamento della disciplina relativa ai doveri degli ISP anche in chiave eurounitaria. Se la strategia fino ad ora seguita, di aumentare i doveri dei *provider* in funzione del contrasto a specifici fenomeni illeciti, presenta un'indubbia razionalità politico-criminale, va nondimeno ribadito che la direttiva 2000/31/CE è diventata oramai incapace di regolare il mercato digitale; il riconoscimento della sua obsolescenza deve costituire il primo passo verso un rinnovamento della disciplina, al fine di assicurare la tutela dei diritti fondamentali degli utenti della rete e – con specifico riferimento al "salto in avanti" compiuto dal legislatore tedesco – di salvaguardare le esigenze di certezza e di armonizzazione del diritto all'interno dell'Unione.

Seminara, Internet, cit., 604.

[78] In questo senso vd. gli artt. 14 s. della Raccomandazione del 1° marzo 2018.

Neofeudalesimo digitale: Internet e l'emersione degli Stati privati*

Andrea Venanzoni

Abstract

La società digitale è da tempo punteggiata dalla emersione di soggetti privati che finiscono con il tracimare dalla loro dimensione societaria e iniziano a occupare spazi del reale. Lo fanno ricorrrendo alla innovazione tecnologica e con una gerarchia liquida, sempre più veloce e accelerata che gli Stati-nazione non riescono a regolare in maniera organica. In questo quadro di frantumazione giuridica e culturale, un processo iniziato nel cuore della globalizzazione, i poteri privati vanno atteggiandosi quali schemi neofeudali in cui meccanismi della conoscenza e della produzione sono uniti tra loro per colonizzare lo spazio reale. Gli Stati infatti hanno sempre più bisogno dei servizi, in alcuni casi esclusivi, offerti dagli OTT. Scopo del presente saggio è analizzare il concetto di neofeudalesimo per come emerso nel corso degli anni nei campi delle scienze sociali, verificare la struttura dei nuovi poteri in relazione ad esempi storici ben conosciuti come quello della British East India Company, mettere in luce le analogie tra società medioevale e cultura organizzativa degli OTT e offrire alcune parziali risposte di contrasto alla feudalizzazione dei rapporti politici e sociali.

The digital society has long been punctuated by the emerging power of private actors who end up overflowing from their corporate dimension and begin to occupy spaces of reality. They do so by resorting to technological innovation and with a liquid, increasingly fast and accelerated hierarchy that nation-states are unable to regulate organically. In this framework of legal and cultural shattering, a process that began at the heart of globalization, private powers are posing as neo-feudal schemes in which mechanisms of knowledge and production are united to colonize the real space. Indeed, countries are increasingly in need of the services, in some cases exclusive, offered by OTTs. The purpose of this essay is to analyze the concept of neo-feudalism as it has emerged over the years in the fields of social sciences, to verify the structure of the new powers in relation to well-known historical examples such as the British East India Company, to highlight the similarities between medieval society and the organizational culture of the OTT and to offer some partial responses to the feudalization of political and social relations.

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

Andrea Venanzoni

Sommario

Keywords

società digitale - neofeudalesimo - poteri privati - diritti fondamentali - over-the-Top

«Le grandi società della costa orientale avevano adottato per lungo tempo un approccio organizzativo di tipo feudale. C'erano sovrani e nobili, vassalli e uomini d'armi, chierici e servi della gleba, divisi tra di loro da un insieme di protocolli sociali e ostentazioni che operavano come simboli araldici, come poter esibire la macchina con autista. Fondare una compagnia, una start-up, divenne allora fondare prima di tutto una comunità, una comunità senza distinzioni di rango sociale in cui si poteva parcheggiare nello spiazzo aziendale nell'ordine di arrivo senza discriminazioni gerarchiche legate al ruolo occupato, e si supponeva che ciascuno interiorizzasse in maniera quasi metafisica gli scopi societari»

T. Wolfe, *The tinkerings of Robert Noyce*

1. Torri e piazze digitali: la piramide liquida della gerarchia nella società digitale

La recente pubblicazione del volume di Joel Kotkin, *The coming of Neo feudalism – a warning to the global middle class*[1], rappresenta senza dubbio occasione per una generale riflessione sulla connessione tra sfera digitale, *governance* dei poteri economici privati che dal digitale traggono forza e codici comunicativi, e rischio di una potenziale regressione delle garanzie incarnate e custodite dalla *figura* dello Stato costituzionale.

Nel saggio, Kotkin analizza come l'ordine mondiale sia ormai punteggiato da una ridefinizione strutturale degli assetti produttivi, sociali e culturali, da fenomeni di asimmetrie economiche sempre più ampie e palesi, propiziate e fatte deflagrare dalla grande convergenza tecnologica e dalle società private che monopolizzano il sistema del digitale[2].

Crisi sociali, stagnazione dei rapporti inter-personali dettata anche dalla drammatica pandemia da SARS Co-V 2, necessità di continuo adattamento selettivo alle nuove logiche e ai nuovi codici produttivi governati, o meglio egemonizzati, dagli OTT stanno facendo rifluire una parte considerevole del ceto medio in una condizione di

[1] J. Kotkin, *The Coming of Neo feudalism – a warning to the global middle class*, New York, 2020.

[2] Ivi, 41 ss., analizza gli Oligarchi della società neofeudale e si focalizza sugli OTT come cardini di costruzione dello spazio neofeudale.

soggezione rispetto alla ricchezza e alla capacità di adattività dei nuovi signori sovrani[3]. Il rischio della privatizzazione della sfera pubblica e dello sdilinquimento delle tipiche garanzie importate da un sistema di maturo costituzionalismo liberal-democratico, sotto le spinte convergenti di nuova globalizzazione e di digitalizzazione della società, ha portato una autorevole parte della dottrina a parlare di un rischio di neo-istituzionalismo medievale[4]: la a-territorialità della Rete, il suo travalicare ordinamenti e confini, presentando una dinamica costitutiva liminale e sfuggente alla regolazione pubblicistica e ingenerando una serie di reazioni da ordine sociale spontaneo[5] sono caratterizzazioni che tra loro cospiranti portano a intravedere, in penombra, delle similitudini non incidentali con l'esperienza giuridica medioevale, sia pure ricostruita in negativo.
Le metafore costituiscono da sempre una presenza irrinunciabile nella scienza sociale, e giuridica in particolare[6]. E Internet, senza alcun dubbio, ha dimostrato una indubbia

[3] E. Morozov, *Silicon Valley. I signori del Silicio*, Torino, 2016.

[4] Il riferimento è a S. Rodotà, *Il mondo nella rete*, Roma-Bari, 2014, 67, il quale rileva come a fronte di un potenziale ordinamento globale in molte nuove teorie sembri esservi carenza euristica di strumenti concettuali per analizzare e padroneggiare i veloci cambiamenti della società e degli ordinamenti. Anche G. Azzariti, *Internet e Costituzione*, in *Costituzionalismo.it, 3,* 2011, 4.
Il concetto di neo-istituzionalismo medievale risaliva a un precedente saggio di D. D'Andrea, *Oltre la sovranità. Lo spazio politico europeo tra post-modernità e nuovo medioevo,* in *Quaderni fiorentini per una storia del pensiero giuridico*, 1, 2002, 77 ss. Nel saggio in oggetto veniva decostruita la teorica degli spazi transnazionali come "società anarchica" determinata da interazioni da ordine sociale spontaneo, con una ampia disamina del pensiero di H. Bull su cui avremo modo di tornare.

[5] Una assai interessante ricostruzione dello spazio digitale ricorrendo, in ipotesi, alla costruzione teorica hayekiana dell'ordine spontaneo ci è offerta da R. Bifulco, *Intelligenza artificiale, internet e ordine spontaneo*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 394: l'A. sottolinea l'apparente paradosso di un ambiente come internet rappresentante al tempo stesso in certa misura una delle massime manifestazioni della progettualità umana e uno spazio dentro cui, secondo molti, la regolazione giuridica esterna non dovrebbe penetrare.
La formula fondante della auto-regolazione interna alla architettura della Rete, il *multi-stakeholderism*, ne rappresenterebbe il portato essenziale, il genuino ordinamento, composito e strutturato secondo dinamiche assommanti poteri pubblici, poteri privati, società civile. Ed in effetti si assiste e si è assistito a un processo di prima latente poi scoperta istituzionalizzazione degli incontri e dei summit e dei forum che punteggiano lo spazio digitale, come ad esempio il World Summit on the Information Society.
A ben vedere, rileva l'A., questo paradosso si risolve nella riproposizione di uno dei dualismi più arcaici del diritto, il contrasto tra *physei* e *nomos*.

[6] Sulla importanza esercitata dall'utilizzo delle metafore nella ricostruzione giudiziaria chiamata ad esprimersi e tutelare i diritti fondamentali nello spazio digitale, adottando un approccio costruito sulla base della argomentazioni della linguistica e delle scienze cognitive, è stato giustamente sottolineato come Internet rappresenti, anche in chiave giuridica, un ambito privilegiato per la emersione delle metafore, essendo un ambiente al tempo stesso virtuale e reale, capace di continue inferenze, e interferenze, tra realtà analogica e realtà digitale, 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*, 3, 2018, 3.
Riprendendo alcuni spunti formulati da George Lakoff nell'importante lavoro *Metaphors We Live By*, viene sviluppata l'idea secondo cui il linguaggio non rappresenta una costruzione autonoma rispetto alle altre attività cognitive, come ad esempio il ragionamento, e viene sviluppata una ampia disamina di come vi sia uno stretto legame tra significati e concetti. L'approccio teorico sotteso alla ricostruzione mira a mostrare come la metaforia sia pertanto più un aspetto del pensare piuttosto che del linguaggio. Vero è che le metafore nascono e si sviluppano mediante network mentali di associazioni, di idee, spunti, riflessioni, ricordi, opinioni, operando già in questo come un elemento assimilabile al funzionamento del web, ovvero come un protocollo operativo dialogico. L'approccio giuridico nei confronti delle metafore è ambivalente, come viene ricordato nel saggio riportando citazioni di Posner e di Cardozo estremamente critiche nei confronti della potenziale ambiguità della argomentazione giuridica intessuta di metafore, eppure sembra prestarsi, in termini euristici, anche alla ricostruzione giuridica quando essa

predisposizione strutturale ad approcci descrittivi di tipo metaforico.
La Rete è stata affrescata come un sistema cardiovascolare[7], come una rielaborazione digitale e perfezionata della macchina di Gutenberg[8] nel generale quadro della Riforma protestante, paragonata a un mercato delle idee, ad una autostrada della informazione[9].
Ma a ben vedere sono due le metafore che maggiormente occupano la linea d'orizzonte delle ricostruzioni offerte in dottrina[10]: quella sulla frontiera[11] americana, e il Medioevo appunto.
Chi scrive concorda con quella autorevole dottrina che avverte di essere cauti nell'adottare modelli dispersi nelle nebbie del tempo, facendone paradigmi epistemologici per l'oggi[12].

---

tocchi l'ambito della Rete, proprio per le motivazioni ricordate supra, ovvero la tendenziale matrice ibrida di Internet.

[7] T. Hardy, *Copyright Owners' Rights and Users' Privileges on the Internet: Computer RAM "Copies": A Hit or a Myth? Historical Perspectives on Caching as a Microcosm of Current Copyright Concerns*, in *Dayton Law Review*, 22, 1997, 436 ss.; A. Johnson-Laird, *The Anatomy of the Internet Meets the Body of the Law*, ivi, 469 ss.

[8] S. McGeady, *The Digital Reformation: Total Freedom, Risk, and Responsibility*, in *Harvard Journal of Law & Technology*, 10, 1996, 137 ss.

[9] C. Calvert, *Regulating Cyberspace: Metaphor, Rhetoric, Reality, and the Framing of Legal Options*, in *Hastings Comm. & Ent. Law Journal*, 20, 1998, 541 ss.

[10] La metafora del *marketplace of ideas* pertiene infatti, sia pure in una chiave privilegiata, a un aspetto funzionale della rete, quello dell'interscambio informativo, mentre qui si predilige il profilo ricostruttivo strutturale.

[11] A.P. Morriss, *Miners, Vigilantes, & Cattlemen: Overcoming Free Rider Problems in the Private Provision of Law*, in *Land & Water Law Review*, 33, 1998, 581 ss., spec. 687 ss.; S. Hetcher, *Climbing the Walls of Your Electronic Cage*, in *Michigan Law Review*, 98, 2000, 1916 ss.;A. P. Morriss, *The Wild West Meets Cyberspace*, in *The Freeman*, 48(7), 1998, 22, il quale sottolinea come l'ordine spontaneo della frontiera, capace di auto-regolarsi e in alcuni casi di essere co-regolato, non debba e non possa servire come metafora per reclamare un intervento dello Stato, posto che la frontiera rappresenta al contrario un orizzonte tendenzialmente capace di autoregolarsi. Una assai interessante ricostruzione della Frontiera americana come "impero della libertà" e come progetto emancipativo ci è è offerta da A. Buratti, *La frontiera americana. Una interpretazione costituzionale*, Verona, 2016, 40 ss. Vero è che l'ordine costituzionale della frontiera si basava su alcuni elementi che fuor di metafora è ancora oggi possibile trovare nella dinamica digitale: l'*homesteading*, inteso come appropriazione originaria e trasformazione in fatto sociale di un bene non appartenente a nessuno, la auto-regolazione dei conflitti, la emersione di norme sociali non originanti da meccanismi istituzionali, la valenza centrale e fondante della proprietà privata, la assoluta preminenza del diritto privato sul diritto pubblico.

[12] I modelli storici e culturali non rappresentano, come autorevolmente avverte Paolo Grossi, così P. Grossi, *Unità giuridica europea: un Medioevo prossimo futuro?,* in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, XXXI, 2002, spec. 41 ss., delle essenze da poter estrarre dal loro percorso logico-fattuale pensando, o forse coltivando l'illusione, di poterli trapiantare nel presente senza dover poi, dolentemente, registrare dei rigetti da un corpo sociale totalmente diverso e in alcuni casi antagonista rispetto a una essenza formatasi in un contesto del tutto *altro.*
Ci sono però due aspetti da sottolineare e che consigliano un approccio parzialmente diversificato: il primo è che questa avvertenza vale per la scienza, in cui le risultanze sono sempre determinate da un metodo, ma non sembrano valere per l'andamento, mai lineare, delle decisioni politiche ed economiche le quali seguono una loro logica diversa.
A me sembra che in molti casi esista, si manifesti, una volontà di ricostruire l'essenza del passato, di un passato magari vagheggiato o poco conosciuto ma potente nel suo incedere.
Le metafore che punteggiano, sin dalla sua comparsa nel teatro del progresso sociale e tecnologico, Internet sono un qualcosa che si situa oltre l'affabulazione semantica; sono ontologie profonde, che riproducono come una replica strutturale l'idea di un rafforzamento archetipico.
Non casualmente, per fare un esempio preciso, la evoluzione nel Web semantico si basa proprio sulla ricodificazione del messaggio in una prospettiva che però, pur scintillante e innovativa, è una lotta nel

Al tempo stesso, mi sembra dato non revocabile in dubbio che alcuni elementi progettuali della architettura della rete e delle relazioni sociali che da questa germinano, e soprattutto il ruolo sempre più egemone occupato dalle grandi piattaforme digitali, le quali hanno scalzato la questione della struttura stessa della rete per imporre una loro agenda giocata sui servizi e sulle dinamiche di interazione sociale[13], rimandino a un non incidentale aroma neo-feudale.

La lezione della storia, ha recentemente scritto Niall Ferguson, è che affidarsi alle reti per governare il mondo è una ricetta perfetta per l'anarchia[14]. La tentazione autoregolatoria della Rete propone sin dalla sua origine la grande contraddizione di una disciplina eterarchica, come quella della Rete, che però non gerarchica è solo in apparenza. È infatti evidente come ogni network sia governato da sue proprie razionalità che originano e si riproducono attraverso la struttura fondante, per come essa è pensata *ex ante*, modellata e fatta evolvere.

La apparente mancanza di normatività nella fisionomia della Rete, la quale viene percepita come uno spazio di libertà e in cui i servizi vengono offerti in maniera "gratuita", conduce al paradigma della citata anarchia, intesa come superamento della istituzione sociale e dell'ordinamento giuridico, per mutarsi in un ordine sociale ristrutturato: un passaggio funzionale per la costituzione di un ordine neofeudale il quale, come ogni ordine spontaneo, è *vuoto* di Costituzione.

Proprio per questo verrà in primo luogo chiarito cosa si intende per neo-feudalesimo, e successivamente si illustrerà la morfologia del neo-feudalesimo digitale.

2. Il neofeudalesimo nella scienza sociale: nascita di un concetto pericoloso

Thomas Carlyle, filosofo scozzese dallo stile corrosivo e dalle idee potenzialmente incendiarie, ebbe a scrivere che la democrazia di massa, all'epoca dei suoi scritti in realtà

e sul linguaggio che finisce per rammentare esperienze del passato, G.L. Conti, *Manifestazione del pensiero attraverso la rete e trasformazione della libertà di espressione: c'è ancora da ballare per strada*?, in *Rivista AIC*, 4, 2018, 219, il quale sottolinea la valenza cooperativistica e collaborativa del sistema del web semantico, contraddistinto dalla elaborazione di caratterizzazione delle informazioni in maniera tale che alla loro immissione consegua una organizzazione in termini razionali e un loro utilizzo più consapevole.

I linguisti e gli studiosi di semiotica quando si confrontano con il Web semantico e con il linguaggio dei social media ne traggono subito l'immagine vivida di un medioevo digitale; M. Arcangeli, *All'alba di un nuovo medioevo. Comunicazione e informazione al tempo di internet*, Roma, 2016, 109, ricorda come i metodi semantici di organizzazione strutturale del web riproducano fenomeni di "incastellamento", ovvero chiusure auto-referenziali legate a codici espressivi precisi che oscillano tra digitale e reale, incidendo spesso nella socialità, nella urbanistica, come ad esempio nel caso delle gated-communities, le comunità chiuse che riproducono dinamiche sociali e istituzionali da feudo nel cuore di città altamente tecnologizzate come Los Angeles, Tokyo, Singapore, città in cui la tecnologia aumenta esponenzialmente la performatività di alcune categorie sociali ma distanzia e reclude, fino alla nullificazione completa, altri strati della popolazione.

[13] G. Sartor, *Il diritto della rete globale*, in *Ciberspazio e diritto*, 1, 2003, 47 ss. come rispetto alla prima architettura del Ciberspazio si sia assistito col tempo, in maniera graduale ma inarrestabile, ad una autentica colonizzazione da parte delle logiche commerciali e dei propri attori che hanno inciso sulla fisionomia e sulla modulazione della architettura-codice del Ciberspazio medesimo.

[14] N. Ferguson, *La piazza e la torre*, Milano, 2018, 462.

una fantasmatica presenza concettuale agitata dagli scritti socialisti più che un dato fattuale, si sarebbe dovuta contrastare con la instaurazione di un ordine gerarchicamente governato da pochi individui la cui legittimazione sovrana sarebbe derivata dalla loro effettiva capacità di provvedere al sostentamento delle moltitudini[15].

La definizione di Carlyle era stata già individuata come primo elemento concettuale di un ordine neofeudale[16].

È importante rilevare come il dibattito sul neofeudalesimo, tra gli anni cinquanta e sessanta del XX Secolo, fosse indirizzato in chiave squisitamente polemica per svalutare le teoriche alla Kenneth Galbraith[17] e le dinamiche di interventismo statale in economia.

Solo successivamente ripresero a fronteggiarsi tra loro due distinte ricostruzioni teoriche: un Medioevo visto come epoca di potere autoritario, capace di legare e avvincere ricorrendo a regolamenti, procedure, sovranità regale discendente dal dato metafisico, utilizzata questa visione contro l'interventismo regolatorio dello Stato, e un Medioevo, all'opposto, concepito come uno spazio di auto-regolazione e di canoni privati, tendenzialmente quindi un momento storico di libertà.

È in questa prospettiva ricostruttiva che si situa, ad esempio, l'opzione teorica della *Lex informatica*[18], attualizzazione alla società digitale della *Lex mercatoria*.

Altrettanto significativo notare come mentre i polemisti che utilizzano la metafora del medioevo per attaccare l'autoritarismo, vero o presunto, degli interventi normativi di regolazione sulla società digitale citino esplicitamente il feudalesimo, le monarchie, il sacro Romano Impero, chi del medioevo vuole estrarre paradigmi concepiti come modelli di libertà si limita a un *cherrypicking* senza mai evocare *ex professo* quella che nell'immaginario collettivo continua ad essere percepita come una età oscura.

È d'altronde vero che «costrutti metaforici, nelle argomentazioni degli organi giudiziari, operano, per usare, ancora una volta, una metafora, come "veicoli" idonei a condurre verso aree concettuali e contesti valoriali diversi. Dietro ogni metafora c'è un mondo di concetti logicamente interrelati e la scelta di un mondo concettuale anziché di un altro è frutto di una precisa opzione assiologica del decisore»[19].

Ogni metafora scelta tradisce in certa misura, quasi fosse un letto di Procuste, le preferenze di chi sta decidendo, valutando, selezionando: si prende la quotidianità e la

---

15 Citato in J. Jones, *Carlyle, Whitman, and the Democratic Dilemma*, in *English Studies in Africa,* 3(2), 1960, 179.

16 J. L. Slater, *An Introduction to the Correspondence of Carlyle and Emerson*, New York, 1956, 112.

17 L'opera di John Kenneth Galbraith, *The Affluent Society*, Boston, 1958, venne duramente criticata negli ambienti anarco-libertari americani, proprio ricorrendo alla definizione di neo-feudale. Recensendo infatti il testo in questione, G. Reisman definì il pensiero di Galbraith: «una riedizione in chiave moderna di feudalesimo prussiano», G. Reisman, *Galbraith's Modern Brand of Feudalism*, in *Human Events*, 3 febbraio 1961.

Nello stesso anno l'aggettivo aveva punteggiato la ricostruzione teorica offerta in tema di responsabilità sociale delle imprese come modalità di istituzionalizzazione neofeudale, appunto, con tutti i difetti tipici di un sistema paternalistico e autocratico, T. Levitt, *The Danger of Social Responsibility*, in *Harvard Business Review*, 1958, 41 ss.

18 J. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in *Texas Law Review*, 1998, 553 ss.

19 A. Morelli - O. Pollicino, *Le metafore della Rete*, cit., 10.

si disseziona al fine di modificarla secondo l'ontologia del canone metaforico stesso.
Ciò non vale necessariamente soltanto per i giudici ma per chiunque sia investito del potere di assumere una decisione: politico, imprenditore, o appunto giudice.
Il passaggio dalla legge al contratto, dalle Costituzioni agli *standard* tecnici e ai *terms of use,* se da un lato rappresenta un elemento agevolato dalle dinamiche accelerate dello spazio globale[20], uno spazio cieco e vuoto dentro cui non va germinando una comune visione politica ma una razionalità originante dal peso della tecnica e della economia, fa comprendere come il medioevo digitale più che una opportunità di inventiva giuridica e di opzioni culturali rappresenti uno schema assiologico tendenzialmente assimilabile a quello paventato da Carlyle.
L'origine del concetto, aldilà degli accenti polemici, sembra riemergere ad opera degli OTT[21] proprio avendo riguardo ai poteri privati, nella declinazione di un nuovo feudalesimo come opportunità: maggiormente suadenti e adattivi rispetto a quelli della sfera pubblica, più capaci di governare le logiche non politiche della globalizzazione, non frenati né drenati dalle garanzie costituzionali e dai vincoli formali della legge, delle procedure parlamentari.
Le *start-up* del digitale sono state per lungo tempo considerate un fenomeno capace di incrinare un neofeudalesimo esibito legato a dinamiche capitalistiche da vecchia industria: l'idea di un canone intrinsecamente democratico, su base meritocratica, in cui ad

[20] Di Medioevo cibernetico, nel generale quadro della analisi della globalizzazione e di una potenziale fine dello Stato di diritto, parla A. Baldassarre, *Globalizzazione contro democrazia*, Roma-Bari, 2001, 249 ss.

[21] Nel suo intervento, *The education of a Libertarian*, apparso sul sito online del Cato Institute il 13 aprile 2009, P. Thiel, fondatore di PayPal, uno dei maggiori venture-capitalist della Silicon Valley, consigliere per gli affari tecnologici della Amministrazione Trump nonché uno dei maggiori finanziatori esterni di Facebook, ha chiaramente statuito come democrazia e libertà siano valori tra loro strutturalmente antitetici. Una parte rilevante del saggio è dedicata proprio al Ciberspazio, descritto, in riferimento alla creazione di una moneta alternativa a quelle statali e libera da influenze governative funzionale alla fine della sovranità monetaria, come una rete di connessioni per sperimentare modelli di libertà e di dissenso e di partecipazione politica non più mediati dalle formazioni sociali promananti dagli Stati-nazione.
Il pensiero di Thiel risente fortemente delle influenze anarco-libertarie statunitensi le quali vedono nel Governo centrale e nel potere pubblico in generale una influenza minacciosa, confidando invece nella matrice autoregolatoria delle dinamiche intrinseche del mercato.
È anche vero e va sottolineato con forza che l'anarco-libertarismo predicato da una parte della società digitale e che raccoglie le proprie posizioni teoriche attorno al citato Cato Institute sembra in qualche misura tradire lo spirito originario del pensiero *libertarian* e dei suoi maestri, come Murray N. Rothbard, ad oggi raccolto dal Mises Institute.
A differenza della parte *libertarian* degli OTT, gli anarco-capitalisti di osservanza rothbardiana sono fortemente critici del *big business* e della trasformazione semi-statale delle grandi società di capitali.
Per vero, come non si è mancato di sottolineare, il mercato in cui credono gli OTT non conosce concorrenza alcuna, ma semplicemente una visione imperiale di occupazione dell'intero spazio a disposizione, il che per altro spiega le ripetute acquisizioni di start-up, le integrazioni verticali, i progetti condivisi.
Le piattaforme digitali non sono tutte strutturalmente uguali: esattamente come i network finanziari tendono a intrecciarsi e ad embricarsi coprendo l'intero spettro del mercato, fino ad occuparlo del tutto, le piattaforme digitali si muovono secondo coordinate strategiche simili.
Google non è simile a Facebook, e Amazon non equivale a Twitter; eppure tra loro unite e cospiranti queste piattaforme finiscono per occupare ogni spazio. Per riprendere il celebre saggio di L.M. Khan, *Amazon's Antitrust Paradox*, in *Yale Law Journal,* 126, 2016, spec. 754 ss., è il paradosso anti-trust di queste grandi piattaforme che finiscono, pur apparentemente parlando il linguaggio della innovazione e della concorrenza, per colonizzare l'intero spazio, prima mercatorio poi politico, annichilendo ogni concorrenza e per divenire essi stessi, in prima battuta, il mercato.

essere riconosciute e premiate fossero le intuizioni, i progetti, le realizzazioni e non il mero *status* è stata per lungo tempo un *topos* irrinunciabile.
Potrebbe quindi apparire contraddittorio o paradossale dover inferire che gli stessi soggetti emersi sulla scena produttiva come potenzialmente, e radicalmente, antagonisti rispetto un modello iper-gerarchizzato di capitalismo siano andati costituendo essi stessi un modello neofeudale, ancor più pervasivo e pericoloso di quello precedente.
Nella scienza giuridica il neofeudalesimo è stato adottato come paradigma per descrivere, o tentare di descrivere, oltre ai ricordati profili delle *corporations* anche le forme composite di ordinamenti sovranazionali e di latente crisi della sovranità singolo-nazionale[22] nel prisma della globalizzazione.
In questa chiave di lettura, neo-feudalesimo diviene una pluralizzazione degli assetti sovrani e degli obblighi di fedeltà, secondo un canone de-formalizzato e de-istituzionalizzato che in chiave sociologica funzionalizza anche i poteri privati a servire come poteri pubblici[23].
La strada, nella chiave di lettura di una pluralizzazione parcellizzante e frammentaria, è senza dubbio stata aperta dalle istituzioni della globalizzazione e dai meccanismi regolatori dello spazio globale che hanno introiettato nel complessivo ordine economico globale una fluida *rule of law* molto spesso cesellata da soggetti privati[24].
L'aspetto più significativo che a mio avviso emerge da una ricostruzione neofeudale degli assetti di potere nel ventre della nuova globalizzazione e della società digitale è la scissione formale tra sovranità e Stato nazionale: non quindi una fine della sovranità, quanto una sua riallocazione pulviscolare in distinti centri e in diversi corpi tecnici, mediante riassetti e riassemblaggi che seguono le linee evanescenti del digitale e quelle fisiche, ma non più coincidenti con lo Stato-nazione, delle grandi macro-regioni commerciali.

3. La Lega anseatica digitale: verso gli Stati privati

La perdita di aderenza del territorio nella sua funzione di delimitazione di un ordine sociale e di un ordinamento giuridico, pulviscolarmente incistato in una ragnatela di relazioni, rapporti, scambi, cede il passo alla riaggregazione dei confini sotto forma di

[22] Il riferimento obbligato è qui al pensiero, già accennato in precedenza, di H. Bull, *The Anarchical Society*, Hampshire, 1977, 248 ss., il quale osserverà come i fenomeni di globalizzazione, colti all'epoca nella loro intersezione con i canoni della Guerra Fredda, avrebbero potuto ingenerare una dinamica di sostituzione della sovranità statale con un ordinamento sovra-nazionale composito, somigliante almeno in chiave funzionale al Sacro Romano Impero e a un insieme eterogeneo di città-regioni capaci di ricordare le Repubbliche marinare.

[23] R. Lippert - D. O'Connor, *Security intelligence Networks and the Transformation of Contract Private Security*, in *Policing & Society*, 16(1), 2006, 50 ss.

[24] Per una lucida e critica ricostruzione di come la *rule of law* della globalizzazione sia in realtà una legalità originante da razionalità private, U. Mattei - L. Nader, *Il saccheggio. Regime di legalità e trasformazioni globali*, Milano, 2010. Opportunamente gli Autori spiegano come sia più conforme a verità descrivere l'ordinamento globale come un reticolo di regimi parziali, generati da logiche private e cesellati da grandi studi legali e da agenzie sospese in una dimensione embricata tra potere pubblico e potere privato.
In questo quadro, i nuovi paradigmi essenziali divengono ottimizzazione, efficienza economica, profitto, mentre i diritti fondamentali acquistano una dimensione recessiva e minoritaria.

interessi[25] e alla coagulazione di nuovi soggetti che vanno via via assumendo sembianze semi-statali[26], pur originando da una forma chiaramente privata.

[25] Quando le reti e i mercati si allineano, come sta avvenendo ai giorni nostri, la disuguaglianza riesplode, perché i guadagni prodotti dalle reti finiscono in misura preponderante nelle mani di chi le possiede, così N. Ferguson, *La torre e la piazza*, cit., 440.

[26] Caso assolutamente paradigmatico, ma come vedremo non unico, la Compagnia delle Indie Orientali che il Barone Macauley, parlamentare e commentatore britannico, definì un mostro politico dalla doppia natura, per come citato in S. Gialdroni, *Gestire la ricchezza, arginare il sovrano: la lunga parabola della British East India Company*, in V. Mastroiacovo (a cura di), *Le sovranità nell'era della post globalizzazione*, Pisa, 2019, 154.
Vero è che la Compagnia sin dal lontano 1686, stando ai carteggi interni tra funzionari e dirigenti della stessa e alti esponenti militari della Corona, iniziava ad adombrare una propria coscienza strategica e politica, tanto da aver fatto parlare della necessità che la Compagnia si rendesse a tutti gli effetti uno Stato sovrano (*sovereign estate*), così Sir Josiah Child nella epistola citata rivolta al Presidente di Fort St. George, nel distretto indiano di Madras, e che invitava a instaurare la legge marziale della Compagnia per passare da una mera aliquota (*parcel*) di mercanti a un effettivo governo (*government*) marziale sull'India.
L'espressione *Estate* tende a ben riconnettere tra loro l'espressione del dominio proprietario terricolo e la sovranità come canone di dominio, secondo una linea concettuale che tende a sdilinquire la differenza e a fondere tra loro portato sovrano-politico e paradigma commerciale/finanziario.
L'idea di Child di superare una "aliquota" o un "branco" di mercanti organizzati tra loro solo in chiave funzionale ma non ancora politica rende evidente due aspetti: il suo utilizzo consapevole di canoni semantici riferibili alla sovranità, dal marziale al termine Stato, indicano che a fronte della originaria legittimazione infusa nella Compagnia dalla Corona, la Compagnia si fosse in certa misura emancipata divenendo stato di se stesso, S. Batthacharya, *The strange case of Lord Pigot*, Newcastle upon Thyne, 2013, 52.
Esattamente come la mandria elettronica che governerebbe i processi di globalizzazione attraverso la razionalità procedurale del mondo finanziario e dei network capitalistici, così il "branco" di mercanti incistati nei nodi connettivi della Compagnia iniziò a elaborare una propria coscienza politica.
L'espressione *mandria elettronica* si suole fa risalire a Tom Friedman e al suo classico studio *Le radici del futuro*, ad indicare speculatori e *venture-capitalist* che grazie alla globalizzazione e alla comunicazione digitale possono aggredire interi Paesi, costringendoli ad indossare camicie di forza istituzionali al fine di resistere a questi processi speculativi. Questa camicia di forza protettiva ingenera però una sensibile restrizione del politico a vantaggio dell'economico. Per una ampai disamina in tema, D. Rodrik, *La globalizzazione intelligente*, Roma-Bari, 2015, 269.
In fondo, l'ordinamento mobile del mare evocato da Schmitt è un ordinamento caotico e composito popolato, come soggetti egemoni, anche da *merchant-adventurers*: il mercante-avventuriero evocato dal giurista di Plettenberg smette di essere un soggetto puramente legittimato da una autorità a lui esterna e di questa funzione servente ed ancillare e date alcune condizioni prende a utilizzare quella iniziale legittimazione sovrana per autodeterminarsi nel processo di costruzione di un altro ordinamento, C. Schmitt, *Terra e mare*, Milano, 2002, 45.
Non mi sembra casuale che tanto nella ricostruzione storico-commerciale della Compagnia delle Indie quanto nell'affresco offertoci da Schmitt nella sua dinamica di sviluppo della talassocrazia ci siano due figure che finiscono per modellare una sorta di razionalità sovrana autonomizzatasi rispetto a quella della madrepatria: i già richiamati *merchant-adventurers* e i pirati.
Soggetti che si situano sul punto di confine, lungo la frontiera, che salda anarchia e sovranità.
Si pensi, come perfetta esemplificazione, a quanto avvenne alla Compagnia delle Indie Orientali nella sua conquista/compravendita del *diwani*, massimo organo di governo amministrativo indiano.
La presenza statale, sotto forma dell'Impero moghul, reagì al fine di imporre il ritorno del proprio dominio, mentre la Corona non si poneva la questione della auto-legittimazione della Compagnia, in quanto essa continuava ad essere comunque, almeno in apparenza, servente dei suoi interessi di espansione.
La Compagnia acquisì il *diwani* in totale autonomia rispetto alla Corona britannica, e non lo conquistò solo con la forza militare ma con una suadente opera commerciale e finanziaria: vennero offerti servizi, clonata la struttura governativa locale, messi gli uni contro gli altri i signori locali.
In questo delicato frangente storico si situa la piena compresenza di tutti gli elementi che ciclicamente tornano, in essenza, a riproporsi nella apertura di spazi, dalla globalizzazione al digitale: due poteri sovrani tra loro in conflitto, poteri privati che vanno espandendosi oscillando tra i due poteri sovrani,

I semi-Stati privati[27] non sono una novità nella storia della civiltà umana, e rappresentano lo strumento attraverso cui gli Stati hanno espanso il loro potere oltre i territori, al fine di occupare spazi[28].

soggetti privati che finiscono per costituire il popolo politico di questo nuovo spazio.
Nel caso di specie, Corona britannica e impero Moghul come poteri sovrani e indipendenti l'uno dall'altro, la Compagnia come potere privato, e i pirati e gli avventurieri come soggetti privati che popolando, non in senso meramente demografico ma politico, lo spazio annesso dalla Compagnia, ne divenivano l'ossatura portante. Questa sequenza è esemplificata dalla persona di Robert Clive, da molti ritenuto l'autentico fondatore dell'Impero britannico, S. Gialdroni, *Gestire la ricchezza, arginare il sovrano*, cit., 155.
Clive assommò tra loro potere della Corona, guidando una estesa spedizione militare contro i declinanti regni Maratha e le arti finanziarie e diplomatiche della Compagnia, portando a sintesi i due distinti aspetti. Giova rammentare che pur tra alcune perplessità dei direttori della Compagnia che temevano che questo processo di costruzione della Compagnia come soggetto semi-statale avrebbe importato una attrazione nell'alveo della sovranità nazionale britannica, da cui dimostravano chiaramente di sentirsi in parte separati, eppure fu a lui che continuarono ad affidare incarichi di prestigio e di crescente rilevanza, fino ad arrivare al culmine della presa del *diwani*, di cui abbiamo già avuto modo di occuparci.
Quell'evento venne salutato come il culmine e il raffinamento del processo di costruzione della sovranità autonomizzata della Compagnia, tanto da far parlare di *constituting the Company masters of a great Empire, in name and responsibility*, così J. Mill, *The history of British India,* (1817), Cambridge, 2010, 243.
La consapevolezza della auto-legittimazione sovrana della Compagnia divenne talmente evidente che essa fu al centro di un vasto dibattito parlamentare in Inghilterra, avvenuto il 10 Luglio 1833, durante il quale la Compagnia venne definita come un mostro dalla duplice natura, soggetto dell'autorità britannica nell' emisfero occidentale ma sovrano nell'altra parte del mondo, un fenomeno mai visto prima e mai affrontato in maniera analitica dal legislatore, dai giudici e dai commentatori.
Una delle notazioni che mi appaiono più interessanti ai fini del presente lavoro è quella secondo cui la natura ibrida della Compagnia, volutamente ambigua nel suo traslarsi dal piano privato al pubblico, avrebbe determinato lo sviluppo di questa natura e di questa coscienza politica, *Hansard's Parliamentary Debates*, Third Series, vol. XIX, London, 1833, 503 ss.

[27] Va tenuto presente che un indirizzo giurisprudenziale in seno alla Corte Suprema statunitense ritiene le c*orporations* come delle *persone*. Si badi, persone non nel senso metaforico di riduzione della complessità socio-tecnica ricondotta a razionalizzazione giuridica dalla *persona ficta* ma individui capaci di poter godere delle garanzie di cui al I e al XIV emendamento.
A far tempo dalla risalente ma ormai storica *Santa Clara City v. S. Pac. R. R. Co.*, 118 U.S. 394 (1886), con la quale la Corte Suprema inferì la applicabilità del XIV emendamento anche alle *corporations*, sul punto ampiamente M. J. Horwitz, *Santa Clara Revisited: The Development of Corporate Theory*, in *W.V. Law Review*, 173, 1985, 173 ss.
Successivamente, *Citizens United v. FEC*, 558 U.S. 310, 363 (2010), su cui ampiamente C. J. Mayer, *Persons and Organizations. Personalizing the Impersonal: Corporations and the Bill of Rights*, in *Harvard Law Journal*, 577, 1990, 41 ss.; K. Greenfield, *In Defense of Corporate Persons*, in *Const. Comm.*, 309, 2015, 30 ss.
In questo senso, come è stato rilevato, la società-persona inizia ad atteggiarsi come una entità separata rispetto allo spazio sovrano dello Stato, sfuggendo in maniera neo-feudale alla regolazione e alla sottoposizione all'ordinamento interno, racchiuso entro i confini statali. In questo senso è stata proposta una assai interessante teorica finalizzata ad una educazione ai diritti delle compagnie commerciali e delle grandi società di capitali, al fine di introiettare nel loro circuito vitale la conoscenza dei diritti fondamentali, così K. Greenfield, *Corporations are people too (and they should act like it*), Yale, 2018.
La *corporation* diventa un semi-Stato, munito di una propria quasi-sovranità, al pari delle gilde medioevali, delle aristocrazie terriere, dei centri universitari che pur essendo formalmente sottoposti alla autorità del sovrano godevano, in forza di un sistema di catene negoziali nutrito da reciproche obbligazioni e diritti, di autentici privilegi, così in D.J.H. Greenwood, *Neofeudalism: the surprising Foundations of Corporate Constitutional Rights*, in *Illinois University Law Review*, 1, 2017, 166.

[28] S. Pietropaoli, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in *Rivista di filosofia del diritto*, 2, 2019, 381, ricorda come Schmitt ritenesse essere stata l'Inghilterra a intuire – e a sfruttare – per prima le enormi potenzialità che scaturivano della nuova visione globale. Da isola essa si trasformò in pesce: come una nave o un pesce essa poteva raggiungere via mare qualsiasi altra parte del pianeta, centro mobile di un impero mondiale frammentariamente diffuso in

La Compagnia delle Indie orientali non fu un *unicum*[29]. La presenza nella storia umana di spazi d'altronde ha da sempre imposto la necessità di ricorrere a modelli inventivi e innovativi per rendere possibile la estensione della sovranità[30] a qualcosa che si situa ad una latitudine diversa rispetto ai concetti che informano la annessione o la conquista meramente territoriale.

Gran parte del Nord America, ancora sotto sovranità inglese, andò nel corso del XVII secolo punteggiandosi di compagnie private egemoni che formalmente investite del potere regio instaurarono un regime governativo privato capace come aveva già dimostrato la vicenda della Compagnia delle Indie Orientali (EIC) di autonomizzare la propria sovranità rispetto a quella della Corona[31].

La più nota e importante fu di certo la Virginia Company of London[32] che fu egemone sul territorio della Virginia, gettando una testa di ponte con omologhe compagnie private e finendo per ingenerare un sistema di sovranità a piramide liquida, in cui la funzione delimitativa del territorio era sostituita dalla comunanza di razionalità economica e di interessi, e in cui al cittadino come attore politico si era andato sostituendo il socio, secondo un meccanismo selettivo di accesso e di esclusione che replicava funzionalmente i meccanismi di cittadinanza, ma senza più alcuna legittimazione statale a monte.

La Compagnia, esattamente come avvenuto per la EIC, aveva ricevuto una prima legittimazione dalla sovranità regia, ma poi era andata modulando delle proprie dinamiche sovrane scisse dalla Corona: nata dalla Corona per impulso sovrano, aveva poi trovato la propria strada replicando la forma statale in una prospettiva puramente privata.

Il sistema delle Compagnie fu notevole per il successivo sviluppo della cultura economica e giuridica americana prima, e della globalizzazione poi.

In primo luogo, esse rappresentarono e rappresentano ancora oggi una forma perfezionata di Stato virtuale[33], in cui gli elementi costitutivi classici sono superati e rimodulati attorno al fulcro dell'interesse economico, considerato anche come ambiente

---

tutti i continenti.

[29] Sottolinea S. Cassese, *Lo spazio giuridico globale*, Roma-Bari, 2003, 22, come i due primi e storicamente più noti modelli di organizzazione a Rete siano stati costituiti dalla organizzazione corporativa medievale e dall'assetto di alcuni ordini imperiali a vocazione commerciale, come quello inglese. In questo senso è quindi possibile leggere la EIC come prodromo strutturale dei flussi della globalizzazione.

[30] D. C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, in *Mich. Telecom. & Tech. L, Rev.,* 69(4), 1998, 85, ritiene che il ciberspazio, con una innovativa ricostruzione teorica, sia simile agli altri spazi problematici del diritto, come lo spazio extra-terrestre e l'Antartide, separandolo pertanto dalla giurisdizione e dal potere degli Stati.

[31] Come è stato rilevato, la capacità di plasmarsi e atteggiarsi a quasi-Stato da parte della Compagnia, la quale nella sua prima fase di espansione territoriale e di virata da alcuni Stati asiatici al sub-continente indiano non solo non incontrò grandi aiuti da parte della madrepatria ma si trovò addirittura ostacolata mediante la concessione di privilegi finanziari a compagnie rivali, rese ben presto la Compagnia una società finanziaria con pretese sovrane; la Compagnia strutturò un proprio esercito, fece largo utilizzo delle sue disponibilità finanziarie e di metodi persuasivi e di ciò che oggi definiremmo *soft power* per intessere una autentica ragnatela-rete sociale, per riuscire ad autonomizzarsi rispetto alle pretese della madrepatria, G. Arrighi, *Il lungo XX secolo. Denaro, potere e le origini del nostro tempo*, Milano, 2016, 271 ss.

[32] G. Baars, *From the dutch East India Company to the corporate Bill of Rights: corporations and international laws*, in U. Mattei - J. Haskell, *Research Handbook on Political Economy and Law*, Cheltenham, 2015, 269 ss.

[33] Mutuo l'espressione da R. Rosencrance, *The rise of the Virtual State*, in *Foreign Affairs*, 75, 1996, 45 ss.

sociale e tecnico[34].

In secondo luogo, operarono come spinta propulsiva verso la definizione di uno Stato commerciante[35] in cui i traffici non seguivano necessariamente ed esclusivamente gli interessi dello Stato-nazione da cui le compagnie erano germogliate: essi seguivano molto spesso anche gli esclusivi interessi delle compagnie stesse le quali si atteggiavano a soggetti capaci di poter tenere proprie relazioni istituzionali, economiche e diplomatiche, con funzioni sovrane.

È indubbio che nel cuore della nuova globalizzazione le economie nazionali vadano somigliando sempre di più a confederazioni informali di economie regionali[36].

Dobbiamo a Immanuel Wallerstein la prima formulazione organica di un sistema mondo che va assommando una fisionomia frammentaria, e appunto neofeudale. Sottolinea Wallerstein come un sistema-mondo sia nei fatti un sistema sociale che ha propri confini, strutture, istituzioni, membri.

La sua esistenza è contraddistinta dai permanenti conflitti tra forze che sono tenute assieme da una tensione altrettanto permanente e dalle spinte che ogni insieme sociale infligge.

Presenta le caratteristiche di un organismo e nel corso della sua vita le sue parti essenziali sono soggette a modifiche, mutamenti, obsolescenza, ammaloramenti[37].

Il sistema globale tratteggiato da Wallerstein va componendosi in aree geografiche neofeudali popolate da una oligarchia baronale che detiene i nuovi mezzi di produzione, e dove la struttura gerarchica dipende dalla conoscenza informatica e dalla materiale disponibilità di alta tecnologia: i cardini di legittimazione di questo medioevo digitale finiscono per operare, autopoieticamente, mediante il ritorno a un concetto di gerarchia naturale, per cui l'investitura risulta *in re ipsa* nel dato informazionale[38].

Vero è che i sistemi di produzione e di scambio vanno sempre più configurandosi come prescindenti dalla fisionomia precisa e direttamente riconducibile allo Stato-nazione sovrano, acquisendo aspetti connessi a dimensioni transnazionali aggregate per interessi e per sistemi di produzione e per codici comunicativi autonomi[39].

---

[34] Al cittadino, sottolinea Parag Khanna, in contesti di forte crisi sociale e di confusione culturale, non importa quanto democratico sia uno Stato o una città, gli importano piuttosto la sicurezza, il benessere economico ed altri elementi tangibili, P. Khanna, *La rinascita delle Città-Stato*, Roma, 2017, 23.
È evidente che i grandi soggetti del digitale si presentano come ambiziosi risolutori di problematiche quotidiane, ne abbiamo avuto ennesima e fondamentale riprova nel cuore della pandemia, quando gran parte delle funzioni pubbliche, dalla istruzione alla sanità alla stessa comunicazione istituzionale, tendevano a passare attraverso piattaforme private.

[35] A. J. Scott, *Le regioni nell'economia mondiale*, Bologna, 2001, 34.

[36] In questo senso, molto chiaramente, A. Baldassarre, *Globalizzazione contro democrazia*, cit., 359 ss.

[37] I. Wallerstein, *The modern World System I: Capitalist Agriculture and the Origins of the European World-Economy in the Sixteenth Century*, New York, 1992, 347.

[38] I. Wallerstein, *Historical Capitalism with Capitalist Civilization*, London-New York, 1996, 162.

[39] R. Baldwin, *La grande convergenza. Tecnologia informatica, Web e nuova globalizzazione*, Bologna, 2017, 206, le ICT operano in maniera radicale sui fattori della organizzazione, mediante un processo di costruzione di nuove modalità di divergenza e convergenza. Richiedono crescente specializzazione per quanto concerne la fisionomia degli stadi produttivi più elevati, ma al tempo stesso si propongono e si atteggiano come alla portata di tutti.
Gli stadi più bassi del livello organizzativo e produttivo d'altronde richiedono costi minori per la società, ne consegue che le ICT importano continui processi di delocalizzazione e di iper-localizzazione.

È in questo momento che si situa la origine compiuta di ciò che ritengo di definire come *iper-territorio*[40], un mosaico globale composto da spazi iper-densi di popolazione, altamente tecnologizzati, funzionalmente inter-dipendenti gli uni dagli altri, contraddistinti da concentrazione della popolazione e dalla concentrazione dei mezzi produttivi e dei centri nevralgici del sistema economico che risponde non più a interessi pubblici bensì privati[41].

Come le Compagnie commerciali, anche questi schemi produttivi basati su dinamiche informazionali generano agglomerazione e coagulazione iper-localistica dei sistemi di produzione in densi complessi polarizzati sul territorio, i quali operano come attrattore e come snodo connettivo delle varie reti su scala globale[42].

Il digitale e gli snodi connettivi connessi a Internet rivestono un ruolo di primissimo piano nella emersione degli iper-territori: reputazione, valore, informazioni, linguaggi e codici tecnici tipologicamemente ascrivibili alla società digitale tra loro cospiranti determinano l'insorgere di un ambiente culturale economico distinto rispetto a quello della sfera pubblica[43].

Di più: il digitale è la architettura portante di questo nuovo eco-sistema che dopo la fase della de-territorializzazione e quella, contraria ma di eguale intensità, della ri-territorializzazione muta il portato ontologico del territorio, dei confini, delle barriere.

Il digitale ha ingenerato una dimensione altra, con una propria antropologia, una propria dimensione sociale e relazionale, proprie istituzioni e metodi di risoluzione delle controversie, ha soprattutto permesso la connessione tra spazi fisici e geolocalizzati arrivando a consistere della base, del codice, per dirla alla Lessig, che struttura, modella e definisce i confini dell'iper-territorio stesso[44].

---

[40] Di recente è stata avanzata anche l'ipotesi di poter parlare di iper-luoghi, in questo senso M. Lussault, *Iper-luoghi*, Milano, 2019, secondo il quale l'iper-luogo rappresenta la concentrazione localistica derivante dai moti accelerati della globalizzazione. Nel presente testo si preferisce l'espressione iper-territori per le conseguenze di ordine giuridico che questo fenomeno determina, alla luce del preciso riferimento costituzionalistico del lemma *territorio*, fermo restando che in termini descrittivi e strutturali vi è una profonda assonanza tra i due concetti.

[41] A. J. Scott, *Le regioni nella economia mondiale*, cit., 64.

[42] Ivi, 79.

[43] Ivi, 100-101.

[44] D.J.H. Greenwood, *Neofeudalism: the surprising Foundations of Corporate Consistutional Rights*, cit., 185, sottolinea come la impersonalità di una struttura societaria non significhi invisibilità e intangibilità: una società, come la Exxon o Amazon, si manifestano fisicamente non solo nei loro servizi ma nelle loro strutture, mediante i processi di venuta ad esistenza delle loro infrastrutture, delle loro sedi, della architettura e della razionalità con cui conquistano spazio nella dimensione fisica e territoriale. Influenzano le città, le regioni, punteggiando con le loro sedi e i loro metodi di occupazione del mercato lo spazio fisico.

Se *Code is Law*, nella ricostruzione di Lessig, possiamo dire che ora *Code is Space*. È solo il caso di rammentare che nel pensiero di Lawrence Lessig è l'architettura a rendere il Ciberspazio ciò che esso è, sottolineando come l'attenzione del giurista debba confrontarsi su come questa architettura-ordinamento finisca per incidere sulle libertà del singolo e della collettività.

La modellazione strutturale del Ciberspazio ne rappresenta in senso ordinale l'elemento istitutivo e fondazionale, e strutturalmente regolatorio, i poteri che incidono su di esso fino a modificarlo e alterarlo geneticamente, una volta sviluppata una propria *policy* politica, inizieranno ad operare in senso schiettamente costituzionale, incidendo sulle libertà e sui diritti costituzionali degli individui, L. Lessig, *Code 2*.0, New York, 2006, spec. 120 ss.

È quindi evidente che se il codice inizia a penetrare anche nell'ambiente e nello spazio fisico, lo spazio

Nascono quindi insiemi complessi meta-urbani legati tra loro dalla tecnologia utilizzata e dal dover rispondere nei loro codici costitutivi alla razionalità centrale, nuova vera sovranità privata, che quei codici conosce e detiene: agglomerazioni di città e di regioni e di aree geografiche pur culturalmente e giuridicamente diverse che sono tenute assieme da un potere che le pervade capillarmente.
In questo senso i detentori dei codici digitali rappresentano il cardine di coagulazione, l'ordine sociale e meta-normativo che va assemblandosi come un mosaico, simili a ciò che fu la Lega anseatica: regioni distinte che si uniscono nel nome appunto di una comune razionalità al fine di esercitare il monopolio informazionale e dei servizi digitali, in cui ciascun OTT diventa un singolo potere capace di tenere avvinte le regioni f*isiche*, ormai scisse dal loro canone sovrano singolo-nazionale.

4. L'istituzione neofeudale della società digitale

Le istituzioni medioevali si basavano essenzialmente su intricate relazioni di matrice negoziale. La *governance* di Internet, in questo, non fa differenza[45].
I contratti di feudo costituivano una ragnatela di rapporti su base delegatoria e parcellizzavano la sovranità rendendo evidente un gioco di conflitti e istanze di equilibrio disposti tutti su uno scosceso sistema di obbligazioni personali[46].
Tanto l'ICANN quanto gli OTT basano le loro dinamiche su sistemi concentrici di deleghe e di servizi resi in modalità circolare, seguendo una struttura a network.
Si trattava, nel medioevo, di un delicato sistema che nonostante l'accentramento del canone sovrano in capo al Re, permetteva a una serie di istituzioni sociali ed economiche, dalle Gilde commerciali alle Università, di reclamare loro autonomi spazi interstiziali di sovranità.
Qui si situa l'aspetto di maggiore interesse: le nicchie di potere privato si sono atteggiate nei confronti del potere pubblico come gli antichi vassalli che formalmente ossequiosi del potere costituito andavano assommando sempre nuove terre, nuovo potere, nuovi privilegi e diritti da opporre agli obblighi dedotti nell'assetto negoziale intercorso con il sovrano.
Facendo leva sull'oggettivo potere comunitario delle linee connettive del digitale[47] i po-

fisico verrà modellato dal codice stesso.

[45] Di struttura feudale della *governance* istituzionale di Internet parla B. Carotti, *Il sistema di governo di Internet*, Milano, 2016, 51 ss.

[46] C. Yen, *Western Frontier or Feudal Society? Metaphors and Perceptions in Cyberspace*, in *Berkeley Technology Law Journal,* 12, 2002, 1207 ss., spec. 1254, ha rilevato come la formulazione dei contratti di adesione ai servizi forniti dagli ISP ricordi la fisionomia delle obbligazioni personali intercorrenti tra signore e vassallo, giocate sul crinale del prendere o lasciare senza vero spazio per una contrattazione. Gli utenti autorizzano, consapevolmente o meno, ma legalmente, gli ISP all'utilizzo e al trattamento dei loro dati per collazionare e usare informazioni, strutturare codici di condotta, modificare unilateralmente gli accordi negoziali e cancellare gli account degli utenti senza previa notifica. Il che ricorda gli atti di lealtà e sottomissione dei vassalli nei confronti del sovrano, fino ad arrivare alla ipostatizzazione di una accettazione di una vita digitale in ossequio e al servizio dei Sovrani digitali.

[47] Il primo a parlare organicamente di comunità virtuali è stato H. Reinhgold, *The Virtual Community: Homesteading on the Electronic Frontier*, New York, 1993, 5, per una delle prime messe a fuoco organiche

teri privati del digitale si sono appiattiti sulle funzioni essenziali degli Stati, proponendo servizi che divenivano di volta in volta irrinunciabili per gli Stati stessi.
Nel medioevo si asssiste ad un processo di centralizzazione che si nutre e si rafforza con le prime assemblee ma che a ben vedere non cambia e non muta la possibilità prospettica della costruzione di contro-sovranità che pur sottoposte al Re, riescono a godere di ampia autonomia fino a produrre esse stesse dei contro-poteri.
Le assemblee rappresentano un organismo particolarmente importante perché esse continuano in certa misura a vantare una radice volontaristica. Dal punto di vista funzionale incarnano un momento di confronto utile per rendere edotto il sovrano delle richieste, delle istanze, delle informazioni sullo stato dei suoi possedimenti, sulle potenziali criticità, e sono al tempo stesso momenti di informazione promanante dal sovrano stesso alla nobiltà.
Nella società digitale, analogamente, è data la possibilità funzionale di un *multi-stakeholderism* per cui almeno in chiave formale ogni gruppo e sotto-gruppo, dai governi ai poteri privati passando per le ONG, possono trovare una propria voce nella miriade di consessi che popolano la modellazione della Rete, dall'ICANN passando per l'Internet Governance Forum e la Internet Engineering Task Force fino alla Internet Society e al World Wide Web Consortium.
Questa pluralizzazione non significa però, a ben vedere, unificazione o condivisione della sovranità. A restare sovrano, in questo caso, è chi detiene la possibilità di incidere sulla fisiologia morfologica del codice della Rete e sulla espansione virale e irrinunciabile dei servizi offerti.
La valenza di questi momenti assembleari, come quella dei "parlamenti" medioevali è, ovviamente, del tutto non paragonabile a quella esplicata nella modernità dai Parlamenti: il Parlamento moderno nasce e si rafforza come espressione della sovranità generale, sia essa incarnata nella locuzione-concetto di volontà generale, di sovranità della nazione, di sovranità popolare, al netto delle differenze incarnate poi da ogni singolo concetto nel suo rapporto, non sempre pacifico, con la rappresentanza.
L'assemblea medioevale al contrario è una cinghia di trasmissione delle decisioni del sovrano lungo la scala gerarchica dei suoi nobili e funzionari: sarebbe d'altronde irrealistico pensare che stanti anche i mezzi tecnici dell'epoca e la difficoltà di coprire le distanze[48], un sovrano potesse contare su differenti mezzi per rendere edotti i propri sudditi delle decisioni via via prese.
Con l'eccezione dei mezzi tecnici, oggi talmente sviluppati da consentire l'azzeramento delle distanze e la accelerazione del tempo, per il resto si scorgono delle sinuose ed ellittiche analogie[49].
Ed in effetti, anche nei consessi internazionali della società digitale la parola sovrana

sulla matrice comunitaria delle prime connessioni digitali.

[48] S. Pietropaoli, *Cyberspazio. Ultima frontiera dell'inimicizia?*, cit., 383, La rivoluzione spaziale che segna l'inizio della modernità trova una puntuale espressione nell'individuazione da parte delle potenze europee di nuove linee per dividere e ripartire il mondo al fine della demarcazione e ripartizione delle aree di conquista.

[49] F. Galgano, *Lex mercatoria*, Bologna, 2001, il quale iniziava dal medioevo per finire nel suo saggio con un neo-medioevo in cui le corporazioni medioevali erano soppiantate dalle *corporations*, e i processi decisionali delle gilde dai sistemi di democrazia azionaria interni alle società per azioni.

che viene tramandata è quella del detentore del codice[50].
La embricazione tra modulo negoziale, soggetti privati e torsione della forma di governo ogni tanto affiora all'aria, interrompendo l'apnea di un rapporto tra governanti e governati e tra poteri di governo che sembra rendersi sempre più granuloso.
Dopo essersi appiattiti sulla dimensione statale, avendone incarnato i servizi, e dopo aver funzionalizzato e polarizzato la popolazione secondo i propri schemi assiologici e strutturali, è lo spazio digitale egemonizzato dai poteri privati a traslarsi nel reale, terminando l'aggregazione assembleare di cui abbiamo detto e facendo emergere gli OTT come i nuovi Stati, capaci ora di godere anche di una loro fisicità: le infrastrutture, i palazzi, le città cablate.
Un mondo che esce dallo spazio dei bit per colonizzare, fisicamente e culturalmente, quello degli atomi.

5. *Code/Space*: neofeudalesimo digitale e territorio

Nel 2001, venne realizzata la prima cartografia essenziale del Ciberspazio[51].
La necessità di delimitare all'interno di un sistema grafico la spazialità geografica è prima di tutto una necessità di ordine politico e sociale[52], tanto ciò vero che come è stato autorevolmente osservato uno dei lasciti più severi della globalizzazione sarebbe stato importare non tanto la lamentata fine della storia quanto la fine della geografia[53].
Il punto che qui interessa è ben esemplificato dal volume *Code/Space*[54]: riprendendo la lezione di Lawrence Lessig sul codice strutturale di Internet come sistema intrinseco ordinamentale, gli autori si soffermano su come la struttura del digitale influenzi e pla-

[50] M. Zafirovski, *Neo-Feudalism in America? Conservatism in Relation to European Feudalism*, in *International Review of Sociology – Revue Internationale de Sociologie*, 17(3), 2007, 393, ha sottolineato come il sistema economico digitale connesso a una visione politica anarco-libertaria e conservatrice americana presenti una spiccata somiglianza con una visione di un passato feudale, mentre dall'altro lato negli USA si suole glorificare la mancanza di un passato feudale effettivo. Si tratta in effetti di un punto essenziale: l'idea neofeudale si atteggia come ologramma, come replica istituzionale strutturata secondo convenienza derivando da un assemblaggio di spunti ed elementi non necessariamente storici.

[51] M. Dodge - R. Kitchin, *The Atlas of Cyberspace*, Boston, 2001: si tratta di un volume di mappe dei vari angoli e spazi che tra loro cospiranti compongono il Cyberspazio, unitamente a una serie di interviste e di impressioni rilasciate da progettisti, ingegneri informatici, hacker, esperti di *digital media* in tema di immaginazione e territorio digitale.

[52] A. Tursi, *Cartografare contrade tecno-politiche*, in *Politica e società*, 1, 2018, 28. Con il termine ciberspazio, infatti, si offre un'immagine condensata di un *ambiente* in cui è possibile abitare e non tanto di uno *strumento*, come succede ancora utilizzando termini quali nuove tecnologie, nuovi media, internet, web.

[53] S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, 22.

[54] R. Kitchin - M. Dodge, *Code/Space: Software and Everyday Life*, Cambridge, 2011, 112, ricordano come le strutture algoritmiche finiscano per riprodurre nella architettura spaziale reale i loro codici. Nonostante molti codici sorgenti siano derivativi e scarsamente efficienti, alcuni risultano di grande impatto sugli ambienti del reale, dimostrando non solo una evidente adattatività e una altrettanto evidente performatività ma anche una capacità di incidere modellando e modificando il reale.
Negli ultimi anni i sistemi scolastici, gli aeroporti, gli edifici pubblici, gli ambiti urbani per poter accogliere la dimensione del digitale si sono conseguentemente modificati: si sono alterate le planimetrie, le dimensioni strutturali delle strade e degli edifici, si sono ridisposti il centro che non collima più con il passato storico ma con la razionalità della comunicazione digitale. Il nuovo centro ora è da dove l'assetto della rete origina, dove il segnale di trasmissione è più forte.

smi e permei la realtà, da quella sociale a quella architettonica.
La integrazione del dato tecnico digitale nella modellazione di edifici governativi, aziende, aeroporti, fabbriche, delinea un nuovo panorama, in cui se *Code is Law*, allora se ne dovrà logicamente inferire che *Code is Space*.
Ogni ordine per assumersi come tale deve godere di una estensione territoriale. Che poi questa sia reale o virtuale poco importa, ciò che davvero rileva è la possibile estensione del dominio sui profili di questo territorio.
La sua conquista e la sua, schmittiana, occupazione.
In questa prospettiva, alla luce dei fenomeni di de-territorializzazione e di re-territorializzazione, non conta più possedere materialmente il territorio, nel suo senso costitutivo dello Stato, quanto godere della capacità di influenzarlo, in senso ingegneristico, sin dalle proprie radici: detto in altri termini, lo Stato continuerà a detenere nel suo grembo il territorio come campo di delimitazione del proprio ordinamento e come elemento di validazione di una comunità politica ivi insediata, ma il codice strutturale e assiologico di quel territorio sarà modellato, in modalità esterna alla sovranità singolo-statale, da altri soggetti. I quali, lo si comprende agevolmente, ne saranno gli effettivi e reali detentori.
Nel medioevo d'altronde il potere era strettamente connesso alla terra: in una certa misura la estensione territoriale dei propri domini rappresentava un canone di legittimazione sovrana che consentiva a un dato vassallo di poter vantare e godere di autonomia più o meno marcata nei confronti del sovrano.
In questa chiave di lettura diveniva essenziale il riferimento perimetrico al territorio: ogni feudo implicava la razionalità di una data porzione, parcellizzata, di territorio su cui esercitare la sovranità regia e al contempo la sovranità del feudatario.
In questo senso è quindi evidente che a fronte della sovranità esercitata sul territorio da parte degli Stati-nazione, i grandi attori della società digitale si comportano come vassalli crescenti nel potere e nella influenza: dominano il campo del digitale, ove detengono la modellazione del codice, ma nel reale sono ancora almeno parzialmente sotto-ordinati.
La questione *Code/Space* diviene pertanto un cardine essenziale per performare il salto da una sovranità digitale a una che andrebbe facendosi anche latamente politica: dominando il campo del reale, dagli assetti regionali alle città interconnesse tra loro da sistemi algoritmici, i soggetti egemoni nel digitale perderebbero lo *status* di vassalli per divenire sovrani a tutti gli effetti.
Potendo essi godere di un vantaggio competitivo assoluto basato sui flussi di dati, informazioni, conoscenza e sulla essenzialità di molti dei servizi da loro prestati, in questo si assisterebbe a un radicale ribaltamento prospettico, con gli Stati ridotti, in molti casi, al vassallaggio.
Proprio per evitare questa deriva, diventa necessario propiziare una regolazione che impedisca la traslazione dal digitale al reale dei canoni sovrani privati, e per fare questo è necessario tornare a focalizzare il *focus* sull'organizzazione[55] dei contenuti e delle modalità espressive e strutturali: in questo senso, la normazione euro-unitaria, tanto sul

[55] Era già l'auspicio di C. Pinelli, *Il fattore tecnologico e le sue conseguenze*, in Aa. Vv., *Costituzionalismo e globalizzazione*, Napoli, 2014, 134.

versante della ridefinizione degli assetti anti-trust quanto sulla declinazione partecipativa con *focus group* e gruppi tecnici che rappresentino delle contro-razionalità rispetto a quelle dei grandi soggetti privati, deve essere implementata, anche ricorrendo alla fusione strategica di autorità garanti al fine di ingenerare organismi pubblici ad altissima specializzazione destinati solo al governo del digitale.

Divengono poi necessari la democratizzazione del canone digitale, da realizzarsi mediante investimenti mirati da parte dello Stato per produrre anche una propria innovazione tecnologica[56], una attività mirata di tutela dei diritti fondamentali da parte delle Corti, collegate esse stesse da network culturali prima ancora che giuridici, l'apertura di forum ibridi dentro cui razionalizzare le polarità latenti e i moti dissonanti della complessità sociale del digitale.

Non quindi organismi meramente consultivi ma eco-sistemi di rappresentanza della integrazione socio-tecnica tra biologico e digitale, politico e tecnico, introiettando e dando cittadinanza anche alle voci dissonanti e critiche, e valorizzando gli assetti sovra-nazionali posto che la limitazione spaziale e funzionale dei singoli Stati li rende nudi davanti ai grandi poteri del digitale.

[56] Il ripensamento organico e coerente delle Pubbliche amministrazioni è un elemento essenziale e irrinunciabile. Si pensi a quanto ci dice il Consiglio di Stato con il suo parere n. 343 del 2016, in riferimento alla riforma della pubblica amministrazione avvenuta con la legge 7 agosto 2015, n. 124: «la presa d'atto del mutato ruolo dello Stato, chiamato non solo a esercitare funzioni autoritative e gestionali, ma anche a promuovere crescita, sviluppo e competitività. Infatti, in tutti i maggiori paesi europei, le riforme amministrative del XXI secolo hanno tra gli obiettivi fondamentali sia il contenimento della spesa pubblica sia (soprattutto) quello della crescita economica e della protezione sociale. Si tratta, evidentemente, di obiettivi fortemente legati alla crisi economico-finanziaria (l'emersione del secondo accanto al primo deriva da una visione più ampia e completa del contesto), che hanno indotto gli Stati a rivedere profondamente le politiche pubbliche. Si registra una revisione del perimetro pubblico e dei processi decisionali, funzionali a rendere più efficiente la macchina amministrativa e a fluidificare i rapporti tra Stato e *stakeholders*».

L'idea che un concorso pubblico continui a selezionare in maniera ossificata, ricorrendo agli stessi schematismi attingenti a un formalismo burocratico che conosce solo poche differenze a seconda del posto messo a concorso o della pubblica amministrazione che indice il concorso, urta in maniera frontale con la idea di poter fronteggiare le strategie, i mezzi e la potenza delle piattaforme digitali, più adattive, fluide e meno cristallizzate nel loro incedere essendo "libere" dall'appesantimento importato da sistemi garantistici e da sovrastrutture come principio di legalità, riserva di legge, vincoli costituzionali legati alle libertà e ai diritti fondamentali, nonché dai passaggi tipici di una democrazia rappresentativa.

Questo *gap* che non può certo essere recuperato mandando al macero nel nome di concorrenzialità e innovazione il prisma garantistico del costituzionalismo, può essere recuperato, almeno parzialmente, da un processo di alta specializzazione delle amministrazioni pubbliche, tanto nel senso del personale quanto della stessa organizzazione e dalla ridefinizione di una latitudine strutturale del governo del digitale, ad esempio istituzionalizzando una integrazione tra dipartimenti di AGCOM e del Garante per la protezione dei dati personali funzionale al contrasto a derive di compressione di diritti costituzionali da parte dei poteri privati., penso al delicatissimo problema dei dati, mediante i poteri tipici della regolazione.

Utilizzo di *big data* nelle decisioni pubbliche tra innovazione e tutela della privacy*

Agostino Sola

Abstract

Il presente articolo muove dall'attuale contesto tecnologico per osservarne le possibili implicazioni sull'azione amministrativa. L'attenzione è focalizzata sui *big data* nel più ampio contesto del rapporto tra tecnologia e diritto. Dopo un quadro introduttivo si osservano le possibilità di utilizzo di *big data* nel generale contesto dell'intervento pubblico, con particolare attenzione al quadro normativo di riferimento, i suoi limiti e le sue limitazioni, onde dare maggior concretezza al tema. Da ultimo si osserva il portato pratico della riflessione condotta con riferimento al singolare caso della realizzazione di un'applicazione volta al tracciamento dei contagi da Covid-19.

This article moves from the current technological context to observe its possible implications on administrative action. Attention is focused on big data in the broader context of the relationship between technology and law. After an introductory framework, we observe the possibilities of using big data in the general context of public intervention, with particular attention to the reference regulatory framework, its limits and limitations, in order to give greater substance to the topic. Finally, the practical result of the reflection conducted with reference to the singular case of the implementation of an application aimed at tracing contagions from Covid-19 is observed.

Sommario

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

Keywords

big data - intelligenza artificiale - privacy - processi decisionali pubblici - utilizzo pubblico di *big data*

1. Introduzione. Intelligenza artificiale, *big data* e nuove tecnologie al servizio del diritto

1.1. L'avvento delle nuove tecnologie nella quarta rivoluzione industriale

L'attenzione per l'utilizzo delle nuove tecnologie è stata da sempre al centro del dibattito sociale, politico ed economico: attraverso l'utilizzo di strumenti innovativi si cerca di migliorare la produttività industriale e non[1]. La nozione di tecnologia è, d'altronde, molto ampia. La tecnologia, infatti, ha ad oggetto lo sviluppo e l'applicazione di strumenti tecnici - ossia di quanto è applicabile alla soluzione di problemi pratici, all'ottimizzazione di procedure, alla presa di decisioni, alla scelta di strategie finalizzate a dati obiettivi - sulla base di conoscenze scientifiche, matematiche e informatiche[2]. È chiaro, dunque, che la concezione del termine varia a seconda del periodo storico di riferimento: ciò che secoli fa costituiva un'importante applicazione tecnologica potrebbe non rivestire tale carattere in un'epoca successiva.

La rilevanza dell'avvento delle nuove tecnologie che connotano l'attuale contesto socioeconomico ha portato alla definizione della nostra epoca quale oggetto della cd. quarta rivoluzione industriale[3]. Tale rivoluzione si riferisce, in particolar modo, alla circostanza in base alla quale tutti gli ambiti della vita sociale ed economica sono influenzati, direttamente o indirettamente, dalle nuove tecnologie digitali che, con l'avvento e la diffusione di Internet, hanno determinato nuove modalità di comunicazione ed elaborazione dei dati ed una costante interconnessione della popolazione.

In tale contesto, poi, assume particolare rilievo anche l'alto grado di automazione raggiunto, l'incremento esponenziale della capacità di calcolo dell'informatica contemporanea e le sempre più frequenti applicazioni dell'intelligenza artificiale[4]. Sistemi,

[1] All'attenzione anche degli organismi sovranazionali, tra cui la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *L'Intelligenza Artificiale per l'Europa*, COM(2018)237 del 25 aprile 2018.

[2] Enciclopedia Treccani.it, *voce "Tecnologia"* in *treccani.it*.

[3] Secondo K. Schwab - P. Pyka, *Die Vierte Industrielle Revolution*, München, 2016, richiamato da A. Lalli, *Il sapere e la professionalità dell'amministrazione pubblica nell'era dei big data e dell'intelligenza artificiale*, relazione al Convegno AIPDA 2019. Ma anche l'Unione europea vede gli sviluppi dell'intelligenza artificiale quale elemento chiave nella strategia della Commissione per la digitalizzazione dell'industria (COM (2016) 180) e nella nuova strategia di politica industriale dell'UE (COM (2017) 479).

[4] Secondo la definizione di intelligenza artificiale proposta dal Consiglio d'Europa intesa quale «insieme di scienze, teorie e tecniche il cui scopo è quello di riprodurre, attraverso la macchina, le capacità cognitive di un essere umano». Disponibile sul *sito web* del Consiglio d'Europa. La creazione del termine si deve a John McCarthy durante una conferenza al Dartmouth College nel 1956.

software e dispositivi basati sull'intelligenza artificiale, infatti, sono in grado di fornire nuove e preziose soluzioni per affrontare i bisogni e le sfide in molti e differenti ambiti, quali la domotica, le smart cities, l'industria, la sanità e la prevenzione del crimine[5].

1.2. Le implicazioni sull'azione amministrativa

Indipendentemente dal più o meno elevato grado di innovazione, il diritto e l'evoluzione tecnologica sono da sempre fortemente connessi ed interdipendenti: se da un lato il sorgere di nuovi interessi e nuove dinamiche impone una tutela e regolamentazione delle situazioni create dal progresso[6]; dall'altro, allo stesso tempo, è anche il diritto ad utilizzare l'evoluzione tecnologica per il perseguimento dei propri fini[7]. Ed è proprio quest'ultimo che offre la possibilità di riconoscere le implicazioni per l'azione amministrativa derivanti dall'utilizzo delle nuove tecnologie, frutto della quarta rivoluzione industriale[8].

Nonostante l'attualità del dibattito sul tema, con particolare riferimento all'intelligenza artificiale ed all'utilizzo di sistemi *data driven*, l'attenzione per l'utilizzo delle tecnologie da parte della pubblica amministrazione, quale strumento funzionale al miglioramento dell'efficienza ed efficacia dell'azione azione amministrativa, è stato da sempre oggetto di analisi e studio: già nel giugno 1979 Massimo Severo Giannini osservava tale fenomeno nel Rapporto sui principali problemi dell'amministrazione dello Stato presentato alle Camere.

Si è, dunque, assistito ad una costante influenza tra l'evoluzione tecnologica e la disciplina procedimentale: la stessa costruzione originaria di attività procedimentale, in-

[5] L'intelligenza artificiale, ad esempio, può portare alla creazione di veicoli a guida autonoma, svolgere lavori pericolosi e usuranti, gestire in maniera razionale grandi quantità di dati e così via. Il libro bianco sull'intelligenza artificiale pubblicato dall'AGID, infatti, riporta un interessante calendario temporale basato su un'indagine, condotta da un gruppo di ricercatori dell'Università di Oxford, secondo cui le tecnologie controllate dall'intelligenza artificiale saranno in grado, ad esempio, nel 2026, di scrivere un tema di liceo, ovvero, nel 2053, di eseguire un intervento chirurgico (Fonte: *When Will AI Exceed Human Performance? Evidence from AI Experts*, Maggio 2017, Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, Owain Evans, Future of Humanity Institute, Università di Oxford).

[6] Il diritto è, infatti, una scienza sociale e, come tale, risente delle grandi direttrici di cambiamento della società. Si pensi alla crescente sensibilità maturata in ambito ecologico che ha portato ad un ripensamento del diritto ambientale, ad esempio.

[7] È evidente, allora, che il diritto – e non solo quello amministrativo – risenta della trasformazione in essere della società contemporanea derivante dallo sviluppo dell'informatica e dell'intelligenza artificiale.

[8] Proprio per tale motivo, dunque, la pubblica amministrazione si troverebbe già in una quarta fase di evoluzione: D.U. Galetta - J. G. Corvalàn*, Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto,* in *federalismi.it,* 3, 2019, 1 ss. Le precedenti fasi, secondo gli A. Sarebbero: la pubblica amministrazione 1.0, che corrisponde al classico modello di pubblica amministrazione del diciannovesimo secolo, caratterizzato dall'utilizzo di carta, stampa e macchina da scrivere. La pubblica amministrazione 2.0, che incorpora computer, processori di testo, stampante e fax. La pubblica amministrazione 3.0 verso cui, nel XXI secolo, il settore pubblico ha iniziato a migrare grazie all'uso di internet, dei portali digitali, delle applicazioni mobili e dei social network. Attualmente la pubblica amministrazione si trova, dunque, già in una quarta fase di evoluzione collegata alla quarta rivoluzione industriale ed ha come minimo comun denominatore un alto grado di automazione e di interconnessione. Si veda anche P. Otranto, *Decisione amministrativa e digitalizzazione della p.a.*, in *federalismi.it,* 2, 2018, 4.

fatti, si è immediatamente confrontata con l'applicazione dell'informatica all'azione amministrativa[9], anche relativamente all'uso delle tecnologie dell'informazione e della comunicazione (ICT) nell'attività amministrativa.

In un primo momento, infatti, si è osservata una mera "dematerializzazione" dei documenti amministrativi, realizzata mediante l'utilizzo sempre maggiore dello strumento computer che, in tale fervore efficientistico, non sarà più usato semplicemente quale moderna macchina da scrivere ma sarà individuato quale strumento di connessione nei rapporti con il cittadino e tra le pubbliche amministrazioni[10], oltre che di ricerca e catalogazione dei dati.

Tale informatizzazione[11], che ha condotto ad una progressiva digitalizzazione del procedimento e dell'attività amministrativa, è divenuta[12], poi, parte di un più ampio ed ambizioso disegno di costruzione di un'amministrazione pubblica che svolga la propria azione mediante l'utilizzo della tecnologia secondo i principi dell'*eGovernment*[13], cristallizzati nel Codice dell'Amministrazione Digitale (CAD), d.lgs. 82/2005[14], ed accolti anche a livello sovranazionale con grande entusiasmo[15].

Grazie alle continue evoluzioni scientifico-tecnologiche, anche in tema di intelligenza artificiale, poi, si deve osservare il passaggio alla cd. fase del "computer-funzionario"[16]

---

[9] Sono state infatti introdotte discipline relative alla modalità ed alla validità dell'uso del telefax (art. 6, c. 2, l. 30 dicembre 1991, n. 412), alla necessità di una rete di collegamento per il trasporto dei dati tra le pubbliche amministrazioni (art. 15, c. 1, l. 13 marzo 1997, n. 59), sono stati successivamente definiti i contenuti tecnologici del documento informatico e della firma elettronica (d.P.R. 10 novembre 1997, n. 513), del protocollo informatico (d.P.R. 20 ottobre 1998, n. 428), nonché le modalità di trasmissione telematica dei documenti elettronici (d.P.R. n. 513/1997).

[10] Rivoluzionando, in tal senso, sia le attività di *front-office*, quali le relazioni dell'amministrazione con i cittadini-utenti, sia le attività di *back-office*, quali le attività di istruttoria procedimentale proprie dell'amministrazione.

[11] Sul punto si veda G. Sartor, *Le applicazioni giuridiche dell'intelligenza artificiale*, Milano, 1990.

[12] Da ultimo codificata nel principio del cd. *digital first* nell'art. 1, c. 1, lett. *b*), della legge Madia, n. 124/2015. Sul punto, si veda G. Pesce, *Digital first*, Napoli, 2018, 49 ss.

[13] Quale «uso delle tecnologie dell'informazione e della comunicazione (ITC) nelle pubbliche amministrazioni, coniugato modifiche organizzative e all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostegno alle politiche pubbliche», in COM(2003)567 del 29 marzo 2003, § 3, 8. Come si vede, dunque, tale nozione non si esaurisce solamente nell'amministrazione digitale.

[14] A titolo esemplificativo si potrebbe richiamare l'art. 41 CAD, per mezzo del quale si disciplina l'adozione nei procedimenti amministrativi degli strumenti informatici; l'art. 3 CAD, sul diritto del cittadino a comunicare per via elettronica con l'amministrazione; ed ancora, gli artt. 2, 3, 4, 5, 7, 12, 13, 15, 17, 22, 23, 40, 43, 50, 73, 80. In particolare, l'art. 12 dispone che «le pubbliche amministrazioni, nell'organizzare autonomamente la propria attività, utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione», nonché per la garanzia dei diritti digitali dei cittadini e delle imprese; l'art. 41 prevede che «le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente».

[15] Nella Comunicazione della Commissione europea COM(2003)567 del 29 marzo 2003 si evidenzia la rilevanza strategica del ruolo dell'*eGovernment* per il futuro dell'Europa. Si veda anche il Piano d'azione dell'UE per l'*eGovernment* 2016-2020, contenuto nella COM(2016)179. Sempre sul tema, senza alcune pretesa di esaustività, COM(2010)245 del 19 maggio 2010, con la quale è stata varata l'Agenda digitale europea; COM(2002)263 del 28 maggio 2002, tra i primi documenti sul tema.

[16] Espressione di A. Masucci, *L'atto amministrativo informatico. Primi lineamenti di una ricostruzion*e, Napoli,

nella quale sulla digitalizzazione del procedimento amministrativo si viene ad innestare l'utilizzo di strumenti informatici idonei a determinare anche il contenuto dell'atto amministrativo, e non più solamente ad influenzarne la forma[17]: in tal senso, allora, ben si può affermare che l'automatizzazione del provvedimento, e, necessariamente, del procedimento, rappresenta una terza fase del processo evolutivo dell'attività amministrativa: dalla digitalizzazione del provvedimento e dalla teleamministrazione[18] si approda all'automatizzazione dell'attività amministrativa[19].

Attualmente, dunque, lo sviluppo degli studi circa l'utilizzo delle nuove tecnologie da parte delle pubbliche amministrazioni prosegue nel senso di riconoscerla quale possibilità di potenziare con adeguati automatismi molti procedimenti, per offrire ai cittadini la possibilità di relazionarsi con lo Stato in maniera più agile, efficace e personalizzata[20]. Nonostante gli interessi pubblici e, quindi, le attribuzioni delle pubbliche amministrazioni, rimangano sostanzialmente gli stessi, l'influenza della nuova rivoluzione tecnologica e la comparsa di nuove tecnologie determina un nuovo paradigma di pubblica amministrazione che ne colpisce le classiche, e più rilevanti, modalità d'azione, come il procedimento amministrativo. Potenzialmente, dunque, si potrebbe assistere ad un vero e proprio punto di svolta nell'evoluzione del settore pubblico: perché, per la prima volta, si potrebbe avviare un percorso di digitalizzazione (tramite gestione di dati e documenti, e non solo) finalizzato ad automatizzare il processo decisionale applicando l'intelligenza artificiale a vaste aree di attività.

L'utilizzo delle nuove tecnologie nel mondo del diritto amministrativo ha una rilevanza globale e le singole esperienze nazionali, influenzate da una maggiore o minore propensione culturale a convivere con lo sviluppo della tecnica[21], offrono risposte diverse e mostrano una differente permeabilità al fenomeno in questione[22]. L'attuale

1993, 13 e Id. *Atto amministrativo informatico*, in *Encicl. dir.,* Milano, 1997, vol. I, 221, § 1 che cita, al proposito, J. Frayssinet, *La bureaucratique: l'administration française face à l'informatique*, Paris, 1981, 15; la definizione francese di *bureaucratique*, riferita ai «procedimenti di automazione del lavoro d'ufficio (bureau), ...(e) definit(a) come la produzione, la riproduzione, il trattamento e la comunicazione di informazioni testuali o numeriche, che abbiano un supporto scritto, vocale o visivo, necessarie alla amministrazione ed alla gestione delle unità di produzione dei beni e dei servizi» è stata tradotta in burotica (poi divenuta teleburotica per i processi importanti anche l'impiego delle telecomunicazioni) da V. Frosini, *Telematica e informatica giuridica*, in *Encicl. dir.*, Milano, 1992, vol. XLIV, 60, § 3.

[17] Si consolida l'atto amministrativo in forma elettronica la cui sola redazione, quale contenitore, avviene mediante l'utilizzo di strumenti informatici. In tal senso, dunque, vengono superate le originarie diffidenze circa la possibilità di riconoscere la validità giuridica del documento amministrativo informatico, connesse, soprattutto, all'imputabilità ed all'integrità del documento così redatto.

[18] L'utilizzo della telematica nella realtà amministrativa ha reso possibile la circolazione *online* dei documenti amministrativi elettronici, garantendo un'interconnessione perenne con il cittadino e con le altre pubbliche amministrazioni, costituendo una vera e propria rivoluzione nella rivoluzione (A. Masucci, *Procedimento amministrativo e nuove tecnologie*, Torino, 2011, 4).

[19] Nella quale si perviene ad una decisione amministrativa automatizzata. Con tale definizione si identificano tutti quegli atti amministrativi il cui contenuto viene determinato mediante l'utilizzo di *software* o algoritmi che sostituiscono l'attività umana.

[20] Libro Bianco sull'Intelligenza Artificiale al servizio del Cittadino, marzo 2018, 27.

[21] L'intuizione è di A. Lalli, *Il sapere e la professionalità dell amministrazione pubblica nell'era dei big data e dell'intelligenza artificiale,* cit., 18.

[22] In tale panorama, l'Italia si caratterizza per un bassissimo indice di digitalizzazione dell'economia e della società (*Indice DESI*) che la trova al 25° posto in Europa. Corollario di ciò, è un'inevitabile scarsa

evoluzione tecnologica, e le possibilità che offre, unitamente alla grande disponibilità di dati[23] e le tecniche di corretta utilizzazione[24], concretizzano interessanti prospettive evolutive di possibili applicazioni anche per la pubblica amministrazione[25].

1.3. I *big data*

La disponibilità e la possibilità di analisi di dati prende il nome di *big data* ed è suscettibile di numerose applicazioni[26]: tra queste, nonostante siano ipotesi ancora remote nel nostro ordinamento[27], vi è quella di ricorrere a sistemi complessi di intelligenza artifi-

propensione all'accoglimento delle nuove spinte tecnologiche offerte.

[23] I dati e la loro *governance* sono «l'ossigeno dell'automazione e la base stessa per l'applicazione dei sistemi di Intelligenza Artificiale» poiché rappresentano il mezzo attraverso il quale l'algoritmo apprende e interagisce con il suo ambiente. L'espressione in corsivo è di D. U. Galetta - J. G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?,* cit., 12. La raccolta di dati e informazioni è da sempre utilizzata per una miglior gestione e conoscenza, già gli Egizi o i Romani utilizzavano i dati per consolidare il proprio dominio; attualmente, l'avvento di Internet e la raccolta delle "tracce digitali" che ciascuno di noi vi lascia, unitamente alle inimmaginabili capacità di calcolo ed estrazione, hanno contribuito alla formazione dell'epoca dei *big data.* Sul tema, P. Savona, *Administrative Decision-Making after the Big Data Revolution*, in *federalismi.it*, 19, 2018, 2 ss.
Occorre osservare anche che i dati e le informazioni crescono ad una velocità vertiginosa tale da creare un ambiente saturo di dati, in tal senso D.U. Galetta, *La pubblica amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?,* in *Ciberspazio e diritto,* 3, 2018, 327 riporta alcuni dati in tema di aumento del volume delle informazioni disponibili. Si pensi alla possibilità di acquisire informazioni su un numero indefinito ed elevatissimo di persone e situazioni attingendo alle fonti più disparate, sotto molteplici formati con una velocità di acquisizione ed elaborazione in tempo reale, (navigazione su Internet, utilizzo dei social network, posta elettronica, mappatura dei movimenti attraverso la geolocalizzazione).

[24] Senza adeguata tecnologia, infatti, l'acquisizione di grandi quantità di dati – inintelligibili alla conoscenza umana - rimarrebbe fine a se stessa e priva di qualsiasi utilità pratica e, quindi, di rilevanza economica.

[25] Invero già applicati da parte delle *administrative agencies* americane, sul punto: C. Coglianese - D. Lehr, *Regulating by Robot: Administrative Decision Making in the Machine-Learning Era*, in *The Georgetown Law Journal Online*, 105(5), 2017 1147; P. Savona, *Administrative Decision-Making after the Big Data Revolution*, cit., 10 ss.

[26] Le applicazioni concrete dell'analisi dei dati divengono sempre più numerose nella vita economica, specialmente nel settore privato con finalità commerciali di tipo predittivo (proposte e suggerimenti di acquisto di beni o servizi basati sulla profilazione del consumatore e sui precedenti dati di acquisto o anche dai dati della navigazione *online*). Fermo restando che, comunque, non esistono piattaforme analoghe a quelle dell'*e-commerce* nei rapporti con le pubbliche amministrazioni. I poteri pubblici stentano, ad oggi, a contrastare e controllare lo strapotere dei detentori, soggetti privati e pubblici, dei *big data* e a fornire adeguate tutele in termini di *privacy*. A. Lalli, *Il sapere e la professionalità dell'amministrazione pubblica nell'era dei big data e dell'intelligenza artificiale,* cit., 2, cita a tal proposito il caso paradigmatico dello scandalo di Cambridge Analytica. In disparte le eventuali considerazioni sugli effetti inevitabili quanto alla declinazione del rapporto tra libertà individuali e autorità e sulla struttura ed organizzazione dello Stato.
Le amministrazioni pubbliche sono, comunque, i più grandi gestori di dati ed informazioni personali, in tal senso F. Costantino, *Intelligenza artificiale e decisioni amministrative,* in *Riv. It. Sc. Giur.,* 8, 2017, 358.

[27] Altrove sono già realtà. A. Lalli, *Il sapere e la professionalità dell'amministrazione pubblica nell'era dei big data e dell'intelligenza artificiale,* cit., 7, richiama l'esempio del Sistema di Credito Sociale in Cina per classificare la reputazione dei cittadini, sulla base del rilevamento delle loro abitudini e dei comportamenti, cui segue un meccanismo di attribuzione di un punteggio: positivo per i comportamenti ritenuti socialmente apprezzabili e negativo per quelli che saranno considerati antisociali. Il punteggio sarà il presupposto per realizzare un apparato premiale, ma anche sanzionatorio.

ciale, caratterizzanti la "quarta rivoluzione industriale", di cui non è possibile escludere *a priori* un'apprezzabile utilità nella vita giuridica[28].

Per intelligenza artificiale deve intendersi quell'insieme di processi, realizzati artificialmente mediante algoritmi e consistenti nella raccolta e organizzazione di grandi masse di dati disponibili e nella individuazione, sulla base della predetta elaborazione, di concordanze e connessioni (*data matching),* che fanno emergere apporti conoscitivi nuovi, non esistenti in precedenza[29]. I sistemi di intelligenza artificiale utilizzano computer, algoritmi e varie tecniche per elaborare informazioni e risolvere problemi o prendere decisioni che in precedenza potevano essere prese solo dall'uomo[30].

L'aspetto più interessante è la capacità di autoapprendimento[31] di tali sistemi di intelligenza artificiale (*machine learning* ovvero *deep learning*), basata sull'elaborazione dei dati forniti e sulla costante identificazione di nuovi schemi (*pattern*) attraverso la lettura e l'analisi dei dati[32] e la successiva applicazione di questa conoscenza ai dati nuovi. Tali sistemi funzionano secondo il modello delle reti neurali e, riuscendo a sviluppare risultati sconosciuti al momento dell'elaborazione dell'algoritmo di base, possono adottare scelte imprevedibili anche per chi ha impostato l'algoritmo originario[33]. Queste tecnologie, basandosi sull'osservazione dei dati, consentono di sviluppare modelli predittivi[34] dei possibili sviluppi della società che consentirebbero, tra tutti, di identificare in via prioritaria i bisogni della pubblica amministrazione e, quindi, di rendere possibile automatizzare l'intera attività amministrativa ed implementare le procedure decisorie

[28] Il tema è stato già osservato a livello comunitario: nelle sue comunicazioni del 25 aprile 2018 e del 7 dicembre 2018, la Commissione europea ha definito la sua visione per l'intelligenza artificiale da realizzare in Europa, i cui caratteri siano l'etica, la sicurezza e l'avanguardia. Sul tema, P. Savona, *Administrative Decision-Making after the Big Data Revolution*, cit., 3; F. Costantino, *Intelligenza artificiale e decisioni amministrative,* cit., 360.

[29] A. Lalli, *Il sapere e la professionalità dell'amministrazione pubblica nell'era dei big data e dell'intelligenza artificiale,* cit., 14. La Commissione europea definisce l'intelligenza artificiale quale «*sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*» nella comunicazione *L'Intelligenza Artificiale per l'Europa*, COM(2018)237 del 25 aprile 2018.

[30] D. U. Galetta - J. G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?,* cit., 7.

[31] L'apprendimento automatico è una tecnica di intelligenza artificiale che, in una spiegazione molto elementare e rudimentale, può essere concettualizzata nel modo seguente: uno o più algoritmi rilevano molti dati al fine di stabilire dei modelli, che vengono poi tradotti in previsioni, sulla base di alcuni criteri statistici. L'utilizzo dei dati diviene, dunque, una modalità di "allenamento" per i sistemi di intelligenza artificiale più avanzati. Con ogni conseguenza in tema di predizioni errate poiché basate su determinati dati appartenenti ad una determinata categoria (ad esempio, un modello basato su dati che si riferiscono alla popolazione adulta potrebbe portare a risultati errati ove applicato alla popolazione adolescente).

[32] Quale l'estrazione di informazioni da grandi quantità di dati grezzi di per sé insignificanti, il cd. *data mining*. Quanto più è grande il set di dati, tanto più accurata sarà l'individuazione delle relazioni anche impercettibili tra i dati.

[33] Secondo il modello della cd. *black box* che sarebbe il vero problema connesso all'implementazione dei sistemi di algoritmi nel contesto dell'attività amministrativa. Si tratta della circostanza per la quale in alcuni casi è praticamente impossibile stabilire in che modo l'algoritmo di *machine learning* sia giunto ad un certo risultato o identificare quali siano i fattori precisi che hanno condotto ad un determinato risultato. Sul tema, D. U. Galetta - J. G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?,* cit., 15; P. Savona, *Administrative Decision-Making after the Big Data Revolution,* cit., 24 ss.

[34] Non si affronterà la possibile evoluzione dell'automazione nell'attività predittiva, con tutti i suoi rischi e tutte le sue enormi potenzialità, nonostante la presenza di alcuni rilevanti esempi sul tema.

automatizzate [35].

2. L'utilizzo pubblico di *big data*

L'utilizzo di *big data* è stato da sempre osservato con particolare riferimento a modelli economici privati, tipici delle cd. economie *data driven*[36] la cui rilevanza è tale da aver portato alla creazione di modelli di *business* concentrati unicamente nella raccolta e analisi di *big data*.

Il rapporto tra istituzioni e *big data* viene osservato in chiave regolatoria sull'idea che sia necessario un intervento pubblico che possa garantire i benefici di un'economia *data driven*, mitigandone i rischi:[37] in tal senso, se ne sono osservate le implicazioni concorrenziali,[38] la possibile sovrapposizione con le istanze di tutela della privacy[39] e l'approccio delle autorità di regolazione a livello nazionale e sovranazionale[40].

Il rapporto tra istituzioni e *big data* che si vuole osservare in questa sede riguarda, invece, attiene alla possibilità che i *big data* trovino un ulteriore campo di applicazione nell'utilizzo da parte delle pubbliche amministrazioni nell'offerta di nuovi servizi pubblici ovvero nell'individuazione di inedite modalità di perseguimento dell'interesse

[35] I sistemi più avanzati di intelligenza artificiale basati sull'analisi di questi dati possono essere variamente e largamente utilizzati a sostegno della decisione pubblica al fine di, ad esempio, ottimizzare la programmazione del trasporto pubblico locale in base alle concrete esigenze degli utenti ovvero l'allocazione dei fondi pubblici ovvero se si analizzassero i dati che riportano il tasso di incidenti e l'indice di mortalità di una determinata strada, unitamente ad altri dati, sarebbe possibile individuare le zone dove intensificare i controlli di polizia stradale. Secondo M. Finck, *Automated Decision-Making and Administrative Law,* in *Max Planck Institute for Innovation & Competition Research Paper No 19-10,* 2, in *ssrn. com,* i benefici per il processo decisionale pubblico derivanti dall'analisi dei dati disponibili sono tre: velocità, efficienza e la possibilità di individuazione di correlazioni tra dati altrimenti impossibili.

[36] Identificabili, in via di prima approssimazione, per l'utilizzo di *big data* – quale complessa serie di passaggi, dalla raccolta all'estrazione ed all'accumulo di ingenti quantità di dati (personali e non) – destinati ad essere processati tramite algoritmi per trarne informazioni nuove e rilevanti, tendenze e/o modelli predittivi utili per contribuire all'efficienza e alla qualità di processi produttivi tradizionali ovvero qualificare in termini di innovazione e di personalizzazione l'offerta di beni e servizi, digitali e non (*data driven innovation,* OECD 2015).

[37] M.E. Stucke - A.P. Grunes, *Big data and competition policy*, Oxford, 2016. Utili strumenti per comprendere l'evoluzione del fenomeno sono i documenti redatti a livello nazionale e sovranazionale nel corso degli anni, tra i quali si richiamano l'indagine conoscitiva sui *big data* del febbraio 2020 condotta da AGCom, AGCM e Garante per la protezione dei dati personali e le Linee guida e raccomandazioni di *policy* contenute al loro interno; OCSE (2018), *Quality Considerations in Digital-Zero Price Markets*, *Background note by the Secretariat*, Parigi.

[38] M. Maggiolino, *I Big data e il diritto antitrust*, Milano, , 2018; V. Falce - G. Ghidini - G. Olivieri (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2018.

[39] Per evidenziarne le preoccupazioni percepite anche a livello politico si segnala la risoluzione del Parlamento Europeo del 14 marzo 2017 "sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto" (2016/2225(INI)); ma anche l'International Working Group on Data Protection in telecommunications (IWGDPT), *Working paper on Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics*, 5-6 May 2014.

[40] S. Gobbato, *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo,* in *questa Rivista,* 3, 2019, 148 ss.

pubblico[41].

Nel percorso che si intende sviluppare è necessario chiarire che con riferimento ai *big data* si considerano le tecniche di estrazione, analisi e sfruttamento di dati mediante algoritmi ai fini dell'elaborazione di decisioni pubbliche – più o meno automatizzate[42]. Queste tecnologie, basandosi sull'osservazione dei dati, consentono di sviluppare modelli predittivi[43] dei possibili sviluppi della società che consentirebbero, tra tutti, di identificare in via prioritaria i bisogni della pubblica amministrazione e, quindi, di rendere possibile automatizzare l'intera attività amministrativa ed implementare le procedure decisorie automatizzate [44].

Le pubbliche amministrazioni, in effetti, come è stato più volte notato, godono di un'ampia disponibilità di dati acquisibili *ex lege*, sia d'ufficio che su impulso del cittadino[45]. L'ostacolo maggiore ad un loro proficuo utilizzo in termini di maggior efficacia ed efficienza della pubblica amministrazione è stato individuato dalla dottrina nella difficoltà di interconnessione delle banche dati pubbliche e dei servizi,[46] oltre alle questioni legate alla formazione del personale[47].

---

[41] Nella stessa direzione, sono allo studio ipotesi di condivisione dei dati tra le imprese e il settore pubblico. In questo senso si devono ricordare le direttive europee in materia di "*Public Sector Information*". In tal senso anche la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Verso uno spazio comune europeo dei dati*, Bruxelles, 25.4.2018, COM(2018) 232 final.

[42] Il fenomeno dell'automatizzazione dell'azione amministrativa, infatti, è stato solo recentemente al centro del dibattito giuridico a partire dalla nota sentenza del Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270, che definisce la previsione di modelli procedimentali senza la presenza dell'uomo e mediante il ricorso ad elaboratori elettronici quale «doveros[a] declinazion[e] dell'art. 97 Cost. coerenti con l'attuale evoluzione tecnologica». Si veda G. Fasano, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica* in *questa Rivista,* 3, 2019, 234 ss.; A. Sola, *La giurisprudenza e la sfida dell'utilizzo di algoritmi nel procedimento amministrativo* in *Giustamm.it,* 2, 2020.

[43] Non si affronterà la possibile evoluzione dell'automazione nell'attività predittiva, con tutti i suoi rischi e tutte le sue enormi potenzialità, nonostante la presenza di alcuni rilevanti esempi sul tema.

[44] I sistemi più avanzati di intelligenza artificiale basati sull'analisi di questi dati possono essere variamente e largamente utilizzati a sostegno della decisione pubblica al fine di, ad esempio, ottimizzare la programmazione del trasporto pubblico locale in base alle concrete esigenze degli utenti ovvero l'allocazione dei fondi pubblici ovvero se si analizzassero i dati che riportano il tasso di incidenti e l'indice di mortalità di una determinata strada, unitamente ad altri dati, sarebbe possibile individuare le zone dove intensificare i controlli di polizia stradale. Si pensi ad esempio ad un ente locale, piuttosto che a un polo museale, che voglia analizzare sui social le opinioni dei cittadini su una nuova iniziativa, oppure ad un ospedale che decida di raccogliere dati provenienti dai cosiddetti *wearable devices*. Secondo M. Finck, *Automated Decision-Making and Administrative Law,* cit., 2, i benefici per il processo decisionale pubblico derivanti dall'analisi dei dati disponibili sono tre: velocità, efficienza e la possibilità di individuazione di correlazioni tra dati altrimenti impossibili.

[45] Osserva la direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico che «il settore pubblico degli Stati membri raccoglie, produce, riproduce e diffonde un'ampia gamma di informazioni in molti settori di attività, per esempio informazioni di tipo sociale, politico, economico, giuridico, geografico, ambientale, meteorologico, sismico, turistico, informazioni in materia di affari, di brevetti e di istruzione».

[46] F. Costantino, *Intelligenza artificiale e decisioni amministrative,* cit., 360, nota 12; G. Carullo, *Big data e pubblica amministrazione,* in *Concorrenza e Mercato,* 23, 2016, *passim.*

[47] Che, da un lato, sconta un'età media superiore ai cinquanta anni, dall'altro, come osservano D.U. Galetta - J.C. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?,* cit., 14, nonostante l'art. 13, d.lgs. 82/2005 preveda espressamente che si attuino anche «politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione», non vi è

Nonostante ciò, comunque, si segnalano buone prassi già poste in essere da alcune amministrazioni pubbliche[48].

Individuati in termini generali i possibili sviluppi del rapporto tra tecnologia e diritto, occorre soffermarsi sulla risposta del legislatore alle possibilità di utilizzo delle nuove tecnologie dell'informatica e dell'intelligenza artificiale nelle attività giuridiche.

Da un lato, *big data* ed intelligenza artificiale possono svolgere mere funzioni di supporto all'azione amministrativa[49], ma, dall'altro, possono essere individuate, in un nuovo ruolo "attivo" di automatizzazione e sostituzione dell'attività umana[50]: le applicazioni della tecnologia, infatti, possono essere distinte in documentarie e metadocumentarie[51].

L'applicazione documentaria della tecnologia, tanto dell'intelligenza artificiale quanto dei *big data* – non è idonea a determinare uno stravolgimento delle modalità procedimentali classiche: il procedimento, cioè, si sostanzierà nelle fasi dell'iniziativa, istruttoria e decisoria. La fase che maggiormente risente dell'applicazione documentaria

un corrispondente stanziamento di risorse finanziarie *ad hoc* per questa formazione.

[48] Ad esempio, il sistema informativo dell'INPS realizzato fin dal 2000 a supporto delle decisioni strategiche dell'Istituto. Si veda F. Costantino, *Intelligenza artificiale e decisioni amministrative,* cit., 360, per ulteriori esempi; ma anche M. Falcone, *Big data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Riv. trim. dir. pubbl.*, 3, 2017, 603 ss.

[49] Ad esempio, nell'esercizio delle proprie funzioni di controllo, di regolazione o di gestione dei servizi pubblici.

È stato osservato come le pubbliche amministrazioni, sfruttando i dati in loro possesso, integrandoli e selezionandoli, sono in grado di costituire delle "basi di dati" che poi analizzano attraverso modelli e griglie predeterminate, utili per rilevare alcune tipologie di irregolarità amministrative, come quelle fiscali. Sulla base di queste rilevazioni, poi, avviano i tradizionali procedimenti amministrativi di accertamento individuale ed emanano i relativi provvedimenti. È il caso del *British Connect system*, che ha permesso al *British HM Revenue and Customs Office*, l'agenzia fiscale britannica, di recuperare moltissime risorse evase o eluse al fisco, come ha osservato M. Falcone, *Big data e pubbliche amministrazioni*, cit., 618 ss.

È anche il caso dell'amministrazione fiscale e doganale francese che è stata recentemente autorizzata dall'art. 154 della Legge Finanziaria francese per il 2020 (Loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020) a raccogliere ed elaborare, in via automatizzata, le informazioni pubblicate dagli utenti sui propri profili *social* per intercettare attività non dichiarate, verificare la corretta domiciliazione fiscale dei soggetti, come anche per portare alla luce illeciti specifici quali, ad esempio, il traffico e la compravendita illegale di tabacco, alcolici o metalli preziosi.

[50] D'altronde già in passato gli sviluppi tecnologici hanno già modificato l'attività amministrativa, le relazioni con i privati e le forme di esercizio del potere pubblico (si pensi all'utilizzazione di cd. *chatbot* in grado di rispondere a domande preimpostate ed indirizzare, in questo modo, l'utente).

[51] La distinzione è di M. D'Angelosante*, La consistenza del modello dell'amministrazione 'invisibile' nell'età della tecnificazione: dalla formazione delle decisioni alla responsabilità per le decisioni,* in S. Civitarese Matteucci - L. Torchia (a cura di*), La tecnificazione,* vol. IV*,* Firenze, 2017, 156-157. Le applicazioni documentarie riguardano il fenomeno dell'applicazione delle tecnologie dell'informazione e della comunicazione (ICT) nell'attività amministrativa in tema di forma degli atti amministrativi, organizzazione dei dati quali derivanti dall'utilizzo di computer e della telematica. Quanto alle applicazioni metadocumentarie, invece, ci si riferisce al passaggio, già segnalato dalla dottrina, alla fase del "computer-funzionario" (L'espressione è di A. Masucci, *L'atto amministrativo informatico. Primi lineamenti di una ricostruzion*e, Napoli, 1993, 13 e Id., *Atto amministrativo informatico*, in *Encicl. dir.,* Milano, 1997, vol. I, 221, § 1.) nella quale le tecnologie vengono utilizzate per la riproduzione automatica di processi mentali nell'attività amministrativa. Il modello metadocumentario, dunque, non fa riferimento all'utilizzo di strumenti informatici per l'esercizio delle funzioni amministrative secondo modalità tradizionali, ma a fenomeni di standardizzazione e spersonalizzazione dei processi decisionali nei quali la tecnologia informatica non viene usata per la redazione dell'atto o la sua conservazione o trasmissione, bensì per la determinazione del contenuto mediante l'esecuzione di operazioni logiche.

della tecnologia è quella istruttoria. A livello istruttorio, infatti, forte dell'art. 3-*bis,* l. 241/1990, l'Amministrazione procedente si avvarrà delle tecnologie che riterrà opportune per il miglior perseguimento dell'interesse pubblico e potrà, quindi, estrarre dati utili e metterli in relazione tra loro per il raggiungimento di una decisione pubblica maggiormente efficiente[52].

Diverso è, invece, il caso dell'utilizzo della tecnologia nell'azione amministrativa, finalizzato all'automatizzazione della stessa[53]. Il legislatore, infatti, si è concentrato principalmente sull'influenza dei precedenti sviluppi tecnologici che hanno portato ad un processo di informatizzazione e digitalizzazione dell'azione amministrativa[54] senza affrontare la possibilità di una sua, totale o parziale, automatizzazione.

3. Il contesto normativo di riferimento per l'utilizzo di *big data* ed intelligenza artificiale

Se si escludono gli interventi puntuali e disomogenei contenuti in singole disposizioni normative, il primo testo organico in materia di innovazione tecnologica nella pubblica amministrazione[55] deve individuarsi nel d.lgs. 82/2005 – il Codice dell'Ammi-

[52] M. Falcone, *Big data e pubbliche amministrazioni,* cit., 620 osserva analiticamente le possibili interazioni tra procedimento amministrativo e *big data*: prima ne evidenzia il carattere statistico-matematici ed i relativi elementi di incertezza per poi riconoscere la necessità di «circondarne l'utilizzo con una rete di garanzie adeguate». Quali la «sindacabilità sulle finalità, sull'appropriatezza e sulla proporzionalità dell'utilizzo stesso di algoritmi matematici e statistici», «garanzie organizzative», «garanzie di trasparenza sul funzionamento degli strumenti di elaborazione e di imparzialità del loro utilizzo» e «garanzie procedimentali, legate alla considerazione di questi risultati come semplici elementi di fatto (e non come presupposti di fatto), come presunzioni semplici, che possono soltanto concorrere alla compongono il quadro istruttorio».

Pertinente, sul tema, è anche il richiamo al *caveat* del Consiglio di Stato, sez. VI, 4 febbraio 2020, n. 881 sulla pretesa di neutralità dell'utilizzo di algoritmi per l'analisi di dati nel procedimento amministrativo: «le decisioni prese dall'algoritmo assumono così un'aura di neutralità, frutto di asettici calcoli razionali basati su dati [...] l'impiego di tali strumenti comporta in realtà una serie di scelte e di assunzioni tutt'altro che neutre: l'adozione di modelli predittivi e di criteri in base ai quali i dati sono raccolti, selezionati, sistematizzati, ordinati e messi insieme, la loro interpretazione e la conseguente formulazione di giudizi sono tutte operazioni frutto di precise scelte e di valori, consapevoli o inconsapevoli; da ciò ne consegue che tali strumenti sono chiamati ad operano una serie di scelte, le quali dipendono in gran parte dai criteri utilizzati e dai dati di riferimento utilizzati, in merito ai quali è apparso spesso difficile ottenere la necessaria trasparenza».

[53] Dove nel nostro ordinamento si osserva, a differenza di altre esperienze giuridiche estere, una sostanziale carenza normativa nonostante la crescente attenzione (e, in alcuni casi, preoccupazione) sociale ed accademica per il crescente utilizzo di algoritmi nelle decisioni pubbliche.

[54] Gli sviluppi tecnologici, infatti, hanno già modificato, come visto, in precedenza, le forme dell'attività amministrativa, le relazioni con i privati e le modalità di esercizio del potere pubblico. Si veda, ad esempio, il risalente d.lgs. 39/1993 con il quale si prevede che gli atti amministrativi siano predisposti tramite i sistemi informativi automatizzati (art. 3, c. 1), ossia l'elaborazione documentale dell'atto amministrativo mediante computer.

[55] Occorre, tuttavia, ricordare che la prima disposizione di carattere generale in tema di automazione e "dematerializzazione" dell'attività amministrativa è l'art. 3, d.lgs. 39/1993 recante "Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera mm, della legge 23 ottobre 1992, n. 421". Fra queste norme di partenza ed il CAD digitale si inseriscono: la direttiva del Parlamento europeo e del Consiglio 13 dicembre 1999, n. 1999/93/CE, relativa ad un quadro comunitario per le firme elettroniche; il Testo Unico di cui al d.P.R. 445/2000, che recepisce il

nistrazione Digitale[56], deputato a disciplinare l'intera materia, pur non costituendone l'approdo definitivo. Il riconoscimento e l'incentivo all'utilizzo delle tecnologie in capo alla p.A. si ha, invece, nel precedente art. 3-*bis* della l. 241/1990 – introdotto con la l. 15/2005 di riforma.

In generale, dunque, si ha un quadro normativo nel quale l'utilizzo della telematica, e, quindi, la digitalizzazione della p.A. in senso lato, costituiscono un principio dell'azione amministrativa, *ex* art. 3-*bis,* l. 241/1990, volto al miglioramento della stessa ed è poi espressamente riconosciuto anche dall'art. 12, d.lgs. 82/2005[57].

In dottrina, poi, l'evoluzione naturale del fenomeno viene individuata nell'automatizzazione dell'azione amministrativa[58]; tendenza accolta dalla giurisprudenza e ricondotta quale applicazione concreta ed attuale dell'art. 97 Cost. poiché suscettibile di implementare le tecniche di buon andamento attraverso cui la p.A. opera secondo i criteri di efficienza, efficacia ed economicità.

In un contesto di generale attenzione verso la digitalizzazione dell'azione amministrativa, rinnovato a seguito della codificazione del principio del *digital first*[59] da estendere anche all'organizzazione dell'amministrazione, il passaggio all'automatizzazione stenta ancora a trovare un'adeguata cornice normativa, nonostante, come si vedrà, non manchino esempi di decisioni amministrative automatizzate.

Non vi è, infatti, alcun riferimento specifico, all'interno del CAD, all'uso di tecnologie (*software,* algoritmi ed intelligenza artificiale) ai fini di una successiva automatizzazione dell'attività amministrativa.

In un contesto normativo, come visto, ancora da delineare, si segnala, sul piano delle forme di disciplina non vincolanti di cd. *soft law* o, meglio, di *pre-law*[60], la presentazione da parte dell'Agenzia per l'Italia Digitale (AgID)[61] di un Libro Bianco sull'intelligen-

d.P.R. 513/1997; ed ancora, le modifiche al testo unico operate dal d.lgs. 10/2002, di attuazione della direttiva del 1999, e poi dal d.P.R. 137/2003. Successivamente, si muove dalla l. 223/2009 il cui art. 10 contiene rilevanti deleghe relative al documento informatico, alle firme elettroniche, ai servizi resi in via telematica, al procedimento amministrativo ed all'accesso alle banche dati. Sulla base di tali deleghe è stato emanato il CAD.

[56] Sebbene sia stato costantemente oggetto di modifiche ed integrazioni normative, da ultimo ad opera della l. 124/2015 (legge Madia). Il Codice viene, proprio per questi motivi, viene individuato quale esempio del paradosso della "nave di Teseo", raccontato da Plutarco. La metafora è di D. Marongiu, *Mutamenti dell'amministrazione digitale. Riflessioni a posteriori,* in D. Marongiu - I. Martìn Delgado, *Diritto amministrativo e innovazione. Scritti in ricordo di Luis Ortega*, Napoli, 2016, 30.

[57] «Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione […]».

[58] Secondo A. Masucci, *Procedimento amministrativo e nuove tecnologie,* Torino, 2011, 81, l'automatizzazione dell'attività amministrativa rappresenterebbe «la conclusione naturale» dell'evoluzione tecnologica e giuridica che sta caratterizzando l'organizzazione amministrativa di molti Paesi.

[59] Per un'analisi del principio nel contesto di riferimento, si rinvia a G. Pesce, *Digital first*, Napoli, 2018, 49 ss.

[60] All'interno del più ampio concetto di *soft law* è possibile individuare negli strumenti preparatori di atti giuridici vincolanti - Libri bianchi, Libri verdi programmi di azioni, comunicazioni istituzionali – forme di *pre law.*

[61] Istituita con il d.l. 83/2012 con lo scopo, tra gli altri, di dare attuazione agli obiettivi dell'Agenda digitale italiana per la promozione e la diffusione delle tecnologie digitali nel Paese.

za artificiale al servizio del Cittadino[62] con interessanti riferimenti e possibili risvolti in tema di automatizzazione dell'attività amministrativa con l'utilizzo dell'intelligenza artificiale nel miglioramento dei servizi pubblici e del rapporto tra pubblica amministrazione e cittadini[63].
Sul tema ha già avuto modo di pronunciarsi la giurisprudenza amministrativa, peraltro in maniera non sempre uniforme: la questione dà piena evidenza del fatto che l'automatizzazione della decisione amministrativa non sia un fenomeno che riguarda solamente l'amministrazione ma, al contrario, è destinata ad impattare anche con l'esercizio del potere giurisdizionale, dovendo il Giudice valutarne la legittimità[64].

3.1 In Europa e nel mondo

L'analisi del fenomeno che si intende osservare non può limitarsi al solo piano interno ma deve necessariamente osservare le modalità con cui viene, se viene, disciplinato negli altri ordinamenti giuridici nei quali, in generale, si può osservare una maggior attenzione per l'utilizzazione delle tecnologie dell'informatica e dell'intelligenza artificiale. Nonostante ciò, comunque, la reazione dell'ordinamento giuridico europeo si è limitata all'enunciazione di principi generali senza prevedere adeguate garanzie per la protezione dei cittadini innanzi all'automatizzazione delle decisioni pubbliche[65].
È solamente nel regolamento (UE) 2016/679 (GDPR)[66] che viene osservato il fenomeno dell'automatizzazione delle decisioni (anche) amministrative. In tal senso, infatti,

[62] Con riferimento ai contenuti, il *Libro Bianco* offre una completa ricostruzione dello stato dell'arte dei servizi digitali in Italia, ed illustra poi, più nello specifico, l'attuale stadio di sviluppo dell'intelligenza artificiale, i principali ambiti del suo impiego, nonché le prospettive aperte dal ricorso a tali strumenti da parte delle pubbliche amministrazioni.

[63] Per un'analisi puntuale del documento si rinvia a M. Tresca, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale* in *questa Rivista,* 3, 2018, 240 ss.

[64] La presente affermazione riposa sulle pronunce che si sono alternate nel corso degli ultimi anni sul tema, con posizioni non sempre coincidenti. Se ne darà atto nel corso dell'elaborato con riferimento alle singole questioni controverse. La questione dà piena evidenza del fatto che l'automatizzazione della decisione amministrativa non sia un fenomeno che riguarda solamente l'amministrazione ma, al contrario, è destinata ad impattare anche sull'esercizio del potere giurisdizionale, chiamato a valutarne la legittimità ed a dotarsi di tutti gli strumenti necessari per una piena conoscenza. Singolare, sul punto, una recentissima pronuncia del TAR Lazio, sez. II ter, 27 gennaio 2020, n. 1077, dove, in tema di tassazione delle nuove monete digitali (nel caso si trattava di *Bitcoin*) nel respingere il ricorso il TAR ha liquidato le spese, in una cifra piuttosto elevata, ponendole a carico del ricorrente soccombente, «nella misura che tiene conto … dello sforzo difensivo che è stato richiesto all'Avvocatura». Un precedente interessante – e preoccupante per i professionisti del libero foro - per le nuove frontiere del diritto amministrativo.

[65] I principali interventi dell'Unione europea sul tema, senza pretesa di esaustività, si possono individuare nell'emanazione di *linee guida in materia di intelligenza artificiale e protezione dei dati*, di *orientamenti etici per un'intelligenza artificiale affidabile* e di una Comunicazione della Commissione europea sull'intelligenza artificiale (COM(2018) 237 final "*Comunicazione della commissione comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni*".

[66] Come si vedrà, i sistemi, più o meno avanzati, di intelligenza artificiale necessitano di dati, anche personali. Proprio per questo motivo il richiamato regolamento in materia di *privacy* pone particolare attenzione al trattamento automatizzato dei dati personali e, più in generale, al loro utilizzo. In tal senso, infatti, si afferma che «la protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali» (considerando 15).

l'art. 22 introduce il diritto a che l'interessato non venga sottoposto – e, quindi, il relativo diritto ad opporsi[67] - ad una decisione basata unicamente sul trattamento automatizzato dei dati - compresa la profilazione[68] - che produca effetti giuridici[69] che lo riguardano o che incida allo stesso modo significativamente sulla sua persona[70].
In tema, tuttavia, è necessario osservare come l'applicazione concreta di tale diritto incontri due ordini di limitazioni. Da un lato, infatti, lo stesso art. 22 ammette la possibilità di ricorrere a decisioni automatizzate qualora necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento – ipotesi tipica dei rapporti privatistici; ovvero qualora autorizzata dal diritto dell'Unione o dello Stato membro – previa individuazione delle misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato ovvero qualora basata sul consenso esplicito dell'interessato. Ed ancora, poi, l'art. 23 ammette la possibilità di ricorrere a decisioni automatizzate, nel rispetto dell'essenza dei diritti e delle libertà fondamentali, qualora sia una misura necessaria e proporzionata per la salvaguardia dei numerosi interessi

[67] Da svilupparsi nelle modalità previste dall'art. 12.

[68] Sono trattamenti largamente diffusi, specialmente nel settore privato, ma che, come si vedrà, sono suscettibili di una vasta portata applicativa anche per le pubbliche amministrazioni. Le "Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679" (WP251) evidenziano i rapporti tra la profilazione e le decisioni automatizzate: da una parte, infatti, le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere svolta senza che vengano prese decisioni automatizzate. Tuttavia, la profilazione e il processo decisionale automatizzato non sono necessariamente attività separate. Qualcosa che inizia come un semplice processo decisionale automatizzato potrebbe diventare un processo basato sulla profilazione, a seconda delle modalità di utilizzo dei dati. L'esempio riportato è quello di una multa per eccesso di velocità: decisione totalmente automatizzata ove comminata esclusivamente sulla base delle prove fornite dall'autovelox, senza necessità di profilazione; si farebbe riferimento alla profilazione ove la multa fosse determinata in base alle personali abitudini di guida, già monitorate in precedenza, coinvolgendo altri fattori quali l'eventuale recidiva di eccesso di velocità o l'eventuale recente violazione di altre disposizioni del codice della strada.

[69] Il Regolamento non definisce i concetti di "giuridico" o "in modo analogo significativi". Sul tema, però, nuovamente occorre fare riferimento alle citate linee guida WP251 secondo cui un "effetto giuridico" possa riferirsi a tutte quelle decisioni, basate unicamente su un trattamento automatico, che incidano sui diritti giuridici di una persona, quali la libertà di associarsi ad altre persone, di votare nel contesto di un'elezione o di intraprendere azioni legali ovvero che possano sullo *status* giuridico di una persona o sui suoi diritti ai sensi di un contratto. Quanto agli "effetti analoghi", invece, si deve ritenere che il Regolamento faccia riferimento all'impatto significativo delle decisioni automatizzate che, pur non coinvolgendo diritti umani, colpiscano significativamente altri interessi: le linee guida riportano, ad esempio, decisioni che negano a una persona un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio.

[70] Si veda anche il considerando 71, in base al quale «l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona». Disposizioni analoghe erano già contenute all'art. 15 della direttiva 95/46/CE, recepito dall'art. 14 del d.lgs. 196/2003.

pubblici elencati[71].

Come visto, dunque, si rendono, di fatto, sempre ammissibili i trattamenti automatizzati da parte di amministrazioni pubbliche[72].

Le richiamate disposizioni normative, dunque, vietano l'adozione di decisioni prese senza il coinvolgimento di un essere umano che possa influenzare e/o modificare il risultato cui perviene l'algoritmo: in tal senso, infatti, deve intendersi l'utilizzo della parola "unicamente" nel dettato normativo, così manifestando la volontà di escludere un sistema decisionale puramente automatizzato ma, allo stesso tempo, ammettendo un sistema di supporto decisionale in cui il decisore finale sia ancora un essere umano il cui apporto non risulti essere meramente formale[73].

Come efficacemente osservato[74], le richiamate disposizioni europee vengono spesso individuate, in assenza di concrete alternative normative, quale parametro di legittimità dell'attività amministrativa automatizzata, nonostante non siano state introdotte per il riconoscimento di garanzie e tutele per i cittadini nei confronti del corretto esercizio di poteri pubblici con algoritmi e programmi automatizzati quanto piuttosto per l'indivi-

---

[71] Quali a) la sicurezza nazionale; b) la difesa; c) la sicurezza pubblica; d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g); i) la tutela dell'interessato o dei diritti e delle libertà altrui; j) l'esecuzione delle azioni civili.

[72] In tal senso, D.U. Galetta - J. G. Corvalàn, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0?,* cit., 17, secondo cui «i trattamenti automatizzati da parte di amministrazioni pubbliche sono ammissibili sempre: purché siano basati su specifiche previsioni normative (principio di legalità) e purché rispettino il principio di proporzionalità, inteso nei termini classici di idoneità, necessarietà e proporzionalità in senso stretto del trattamento rispetto alla tutela dell'interesse pubblico in concreto perseguito dal titolare del trattamento».

Con riferimento al secondo paragrafo, lett. *b*), dell'art. 22, A. Boix Palop, *Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones,* in *Teoría y Método. Revista de Derecho Público,* 1, 2020, 28, osserva che tale disposizione consente a qualsiasi previsione normativa che autorizzi processi decisionali automatizzati di derogare alla disciplina in materia di protezione dei dati personali, senza la preventiva necessità di ottenere il consenso degli interessati, ad esempio.

[73] Venendo così a determinare il "principio di non esclusività della decisione algoritmica" in base al quale, come osservato, è necessario che la macchina interagisca con l'essere umano per produrre il suo risultato. G. Pesce, *Il Consiglio di Stato ed il vizio della opacità dell'algoritmo tra diritto interno e diritto sovranazionale,* in *giustizia-amministrativa.it*, 2020, 9, ricorda come tale modello sia utilizzato in ambito matematico ed informatico e definito quale *HITL* (*human in the loop*). Secondo l'A., ancora, il richiamo al principio di non esclusività risentirebbe, innegabilmente, dell'influenza dei riferimenti etici che devono governare l'impiego della IA nel settore pubblico. Sul punto, allora, pare di interesse ricorda che, nelle sue comunicazioni del 25 aprile 2018 e del 7 dicembre 2018, la Commissione europea ha definito la sua visione a sostegno di un'intelligenza artificiale che «etica, sicura e all'avanguardia realizzata in Europa». Ed ancora, nello "*Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems"* presentato alla Commissione dall'*European Group on Ethics in Science and New Technologies*, sono individuati nove "principi etici e requisiti pre-democratici" che dovrebbero fornire una guida futura per legislatori, regolatori e giudici: dignità umana; autonomia; responsabilità; giustizia, equità e solidarietà; democrazia; «*rule of law and accountability*»; sicurezza, integrità fisica e mentale; protezione dei dati e privacy; sostenibilità.

[74] A. Boix Palop, *Los algoritmos son reglamentos,* cit.

duazione delle sole garanzie dell'individuo a non essere sottoposto a forme decisionali, pubbliche ma specialmente private, automatizzate, a meno che non ricorrano determinate condizioni[75].

4. La filiera pubblica di *big data* e possibili limiti derivanti dall'utilizzo di dati personali

Indipendentemente dagli sviluppi, più o meno possibili, dell'azione amministrativa in termini di automatizzazione della stessa, osservato come l'utilizzo di *big data* per aumentare l'efficienza pubblica debba essere incentivato e, comunque, non trovi divieti normativi espressi, ci si deve concentrare ora sulle possibili limitazioni.

La premessa iniziale è utile per richiamare la filiera di *big data* che si articola (con ogni possibile ricaduta sul piano giuridico) in tre ordini principali di attività: i) la raccolta, che a sua volta si articola in generazione, acquisizione e memorizzazione, ii) l'elaborazione, che coinvolge attività di estrazione, integrazione e analisi, iii) l'interpretazione e l'utilizzo.[76] I dati raccolti, elaborati ed interpretati possono avere natura personale o non personale e tale distinzione rileva ai fini del trattamento dei dati sotto il profilo regolamentare e sulle conseguenti possibili limitazioni[77].

La prima fase di raccolta ha inizio con la generazione di dati derivante dall'attività degli utenti/fruitori o dall'attività di strumenti di rilevazione di dati ambientali, geografici e logistici. I dati generati sono poi raccolti e memorizzati. La seconda fase è finalizzata all'elaborazione dei dati raccolti: attività centrale nell'intera filiera dei *big data* atteso che il possesso di grandi quantità di dati grezzi, non strutturati in informazioni suscettibili di pratica applicazione, è priva di utilità. In linea generale, le tecniche di analisi consistono per lo più in algoritmi di interrogazione e di apprendimento. La terza ed ultima fase, invece, si inserisce nei processi decisionali, contribuendone ad implementare l'efficienza e la qualità ovvero qualificare in termini di innovazione e di personalizzazione l'offerta di beni e servizi, digitali e non, secondo il paradigma della *data driven innovation.* In altri termini, le decisioni – sia pubbliche che private – vengono prese direttamente sulla base dei dati e della loro correlazione.

La raccolta di dati non rappresenta *ex se* un'attività illecita, né quando è posta in essere da soggetti privati né tantomeno quando è posta in essere da soggetti pubblici. La rac-

[75] S. Civitarese Matteucci, *"Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità,* in *Diritto pubblico,* 1, 2019, 23.

[76] Indagine conoscitiva sui *Big Data*, rapporto finale di AGCom, AGCM e Garante Privacy, 2020, 8.

[77] Per dato personale si intende «qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale»; si considera identificabile «la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Particolare attenzione, e una maggiore protezione, sono rivolte ai dati sensibili, cioè ai dati personali «idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale».

colta di dati aventi natura non personale[78], poi, si può ritenere sostanzialmente libera e non soggetta a limitazioni di sorta – poiché difficilmente si potrebbe immaginare la lesione di un interesse meritevole di tutela contrapposto alla loro raccolta ed utilizzazione.

Le questioni sorgono, però, qualora la raccolta – e l'elaborazione - abbia ad oggetto dati personali la cui protezione è pacificamente riconosciuta anche a livello sovranazionale determinando un trattamento dei dati che agisca per finalità determinate ed in base al consenso dell'interessato[79].

Le amministrazioni pubbliche ottengono dati personali, anche sensibili, nello svolgimento delle loro finalità istituzionali: dall'amministrazione finanziaria al servizio sanitario. I dati raccolti confluiscono poi in apposite banche dati pubbliche.

Anche per le pubbliche amministrazioni si pongono gli stessi obblighi finalizzati a garantire i diritti fondamentali dell'individuo in tema di protezione dei dati personali. Si consideri anche come la cooperazione tra autorità nazionali, anche mediante lo scambio di dati personali, è incoraggiata (*recte*, imposta) ove finalizzata allo svolgimento delle rispettive funzioni[80].

L'utilizzo dei dati personali da parte delle autorità pubbliche è accompagnato da una "presunzione di liceità" qualora sia finalizzato alla salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica ovvero quando necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri[81]. L'individuazione di un interesse pubblico da perseguire mediante l'utilizzo di dati personali, ancora, vale anche a definire la finalità del trattamento, fermo restando la possibilità di prevedere apposite disposizioni normative per determinare on maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto[82].

Le finalità pubbliche, in ragione della loro necessità, non sembrano dover essere assistite dal consenso dell'interessato, diversamente opinando si avrebbe la possibilità che allo Stato sia impedito il perseguimento dei superiori interessi pubblici per il mancato consenso del cittadino al trattamento dei propri dati personali (nella misura in cui detto trattamento sia lecito e legittimo)[83].

---

[78] Quali, ad esempio, i dati geografici e di localizzazione prodotti dai Geographic Information System (GIS).

[79] La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'art. 8 della Carta dei diritti fondamentali dell'Unione europea e l'art. 16 del Trattato sul Funzionamento dell'Unione europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

[80] Considerando 5, regolamento 2016/679/UE, regolamento del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (anche GDPR).

[81] Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione (considerando 46, GDPR).

[82] Fermo restando che il GDPR non impone che vi sia un atto legislativo specifico per ogni singolo trattamento.

[83] G. Carullo, *Big data e pubblica amministrazione,* cit.*,* 192 ss., il quale osserva le differenze nei rapporti tra privati e nel rapporto con l'autorità laddove, infatti, «gli interessati vedono di fatto annullata

Non solo, per motivi di interesse pubblico rilevante è consentito il trattamento dei dati cd. sensibili, purché proporzionato alla finalità perseguita e nel rispetto del diritto alla protezione dei dati. Resta salva la tutela che il GDPR riconosce al soggetto i cui dati siano stati raccolti e siano oggetto di trattamento.

Da ultimo, il quadro normativo di riferimento si completa con la previsione contenuta nell'art. 23 del GDPR dove si chiarisce la possibilità di derogare, mediante specifiche misure legislative, la portata di alcuni fondamentali obblighi e diritti degli interessati qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare tra gli altri: la sicurezza nazionale; la difesa; la sicurezza pubblica; la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari.

Ai fini della presente trattazione non si affronteranno gli obblighi a carattere organizzativo connessi al trattamento di dati personali i capo alle pubbliche autorità, quali l'individuazione di figure responsabili del trattamento, il cd. *data protection officer* (DPO)[84] ovvero l'adozione del registro dei trattamenti, né alle questioni attinenti al bilanciamento tra diritto di accesso, trasparenza e protezione dei dati personali.

In conclusione, dunque, le disposizioni normative a tutela della privacy non limitano le possibilità d'azione delle autorità pubbliche ma, anzi, confermano la primazia dell'interesse pubblico rilevante. La tutela della privacy, dunque, lungi dall'essere privata di efficacia, si conforma e si adatta al miglior perseguimento dell'interesse pubblico. Nell'attuale contesto tecnologico, unitamente ad un'interpretazione d'avanguardia del principio generale, *ex* art. 3-*bis*, l. 241/1990, il miglioramento dell'azione amministrativa muove necessariamente da queste spinte innovative. L'utilizzo di tecnologie – anche in termini di automatizzazione del procedimento - viene accolto con entusiasmo dalla giurisprudenza e ricondotto quale applicazione concreta ed attuale dell'art. 97 Cost.

---

la loro capacità di autodeterminazione in merito al trattamento dei dati». Sono poi individuate tre diverse possibili "ordini di situazioni" di questo rapporto: acquisizione di dati connaturata all'attività amministrativa svolta (ad esempio, i dati relativi alla posizione fiscale dei privati); acquisizione di dati volontaria ma obbligatoria per la fruizione di una prestazione pubblica (ad esempio, iscrizione di un minore alla scuola primaria); acquisizione di dati volontaria ma irrinunciabile (ad esempio, nei rapporti con il servizio sanitario nazionale).

[84] La designazione di un DPO da parte del Titolare (art. 37 GDPR) è obbligatoria solo in casi specifici ed, in generale, i soggetti pubblici devono sistematicamente nominare un DPO, ad eccezione delle autorità giurisdizionali quando esercitano la funzione giurisdizionale. per tutti gli altri soggetti, la designazione è obbligatoria quando le "attività principali del Titolare", considerati i caratteri del trattamento, "richiedono il monitoraggio regolare e sistematico degli interessati su larga scala" oppure quando consistono nel trattamento, su larga scala, di categorie particolari di dati sensibili, di cui all'art. 9, o di dati relativi a condanne penali e reati di cui all'art. 10. Il DPO è designato in funzione delle qualità professionali ed è tenuto ad una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati; può essere un dipendente del Titolare o del Responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi; i dati di contatto del DPO devono essere comunicati al Garante dal Titolare/Responsabile del trattamento.

poiché suscettibile di implementare, secondo i criteri di efficienza, efficacia ed economicità, le tecniche di buon andamento attraverso cui la pubblica amministrazione opera. Si pensi, ad esempio, all'utilizzo dei dati per la creazione di *smart cities*, in cui i cittadini attraverso un'applicazione presente nei propri smartphones hanno accesso in tempo reale ai dati sul traffico, sui parcheggi disponibili, sulla qualità dell'aria, sui tempi di attesa dei mezzi pubblici, sulle farmacie di turno aperte, sul numero di pazienti presenti nei pronto soccorso. Tutto ciò grazie a sensori interconnessi, i quali trasmettono le proprie rilevazioni ad un server centrale che elabora e rende disponibili le informazioni ai propri utenti.

4.1. Il ruolo privacy (e dell'Autorità Garante) nella creazione di un'applicazione volta al tracciamento dei contagi da COVID-19

Un interessante banco di prova dell'utilizzo di *big data* concernenti dati personali (e non solo) è sicuramente offerto dall'utilizzo di un'applicazione volta al tracciamento dei contagi da Covid-19.

L'idea non è nuova ma origina dalla Cina[85]. Il funzionamento di tale applicazione è relativamente semplice: tracciare gli spostamenti della popolazione per metterli in relazione tra loro onde avvisare gli utenti circa la possibilità che siano entrati in contatto, non necessariamente in maniera volontaria, con un soggetto risultato positivo al Covid-19.

Nel rispetto dei principi della "*privacy by design"* e "*by default*,"[86] l'Autorità Garante per la protezione dei dati personali ha sin da subito ricoperto un ruolo di primaria importanza nella possibilità di prevedere un'applicazione volta al tracciamento dei contagi da COVID-19.

Nonostante, però, come visto, la normativa in tema di dati personali contenga già al

[85] *Un'app per "geolocalizzare" i malati di Covid-19: l'idea della Cina per rallentare il contagio*, in *Huffington Post*, 9 marzo 2020 ; *La Cina lancia un'app statale per controllare il rischio contagio da coronavirus*, in *La Stampa*, 14 febbraio 2020.

[86] Il principio della *privacy by design* implica che la protezione dei dati sia considerata sin dalla progettazione di una data tecnologia, servizio o procedimento che dovranno realizzarsi, quindi, avendo presente, sin dal principio - by design, appunto - la riservatezza dell'utente finale e la protezione dei suoi dati personali, con tutte le necessarie applicazioni di supporto (informatiche e non). Diverso, ma complementare in un'ottica di massima protezione efficiente dei dati, è quello della *privacy by default*, il quale implica che i dati vengano raccolti nella minore misura possibile e che le finalità del trattamento siano quanto più possibile limitate. Si tratta, in altre parole, della summa dei principi di "minimizzazione dei dati" e di "limitazione della finalità" (da cui discende a sua volta il principio della "limitazione della conservazione", il quale impone di limitare nel tempo quanto più possibile il trattamento e l'archiviazione dei dati raccolti). Corollario di tali principi è una minimizzazione dei dati ed una limitazione della finalità e della conservazione dei dati. Tali misure, poi, potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, nel consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati, i produttori, dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni. In questi termini il considerando 78, GDPR. L'art. 25, GDPR, rappresenta il fulcro normativo dei predetti principi. In tema, G. D'Acquisto - M. Naldi *Big data e privacy by design: anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017; S. Calzolaio, "*Protezione dei dati personali*", voce in *Digesto, Dir. Pubblico,* 2017.

suo interno regole che consentono di trattare anche i dati più delicati - quali sono quelli sul contagio – ove detto trattamento serva realmente a tutelare la salute dei singoli o della collettività,[87] si è inteso fornire un'inedita base normativa alla previsione della richiamata applicazione in conformità ai principi di proporzionalità, necessità, ragionevolezza.

Si osservano ora alcuni dei profili di interesse giuridico relativi all'applicazione per il tracciamento dei contagi da Covid-19 sulla base della recente introduzione dell'art. 6 "*Sistema di allerta Covid-19*", d.l. 30 aprile 2020, n. 28.

Preliminarmente si dà atto che la liceità del trattamento dei dati in un'applicazione simile non si può individuare nel consenso dell'interessato poiché viene ricondotta all'esecuzione di un compito di interesse pubblico, rispetto al quale è comunque prevista la volontarietà di adesione da parte dell'interessato[88]. Si ritiene che il trattamento dei dati sarebbe stato comunque lecito anche in assenza della volontarietà di adesione in ragione del fatto che il trattamento dei dati personali risponde a rilevanti motivi di interesse pubblico[89].

La base giuridica del trattamento dei dati, costituendo un *unicum* nel panorama legislativo nazionale e non essendo desumibile in alcuna disposizione vigente, è stata elaborata *ex novo*[90].

La base normativa, infatti, trattandosi di dati personali sensibili[91], oltre a dover specificare la finalità perseguita e limitare il trattamento al perdurare dello stato di emergenza[92], precisando che i dati personali dovranno essere in ogni caso cancellati una volta raggiunto lo scopo per il quale sono stati raccolti e non potranno essere utilizzati per

[87] «Il trattamento di dati personali dovrebbe essere […] considerato lecito […] necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. […] Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana» (considerando 46, GDPR) ed anche «Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche» (considerando 54, GDPR).

[88] «…. è istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile» (art. 6 "Sistema di allerta Covid-19", d.l. 30 aprile 2020, n. 28).

[89] In disparte gli ulteriori profili legati all'eventuale obbligatorietà, quali, ad esempio, l'effettivo controllo e la possibilità di coazione all'installazione dell'applicazione. La decisione di non rendere obbligatoria l'installazione dell'applicazione è, tuttavia, condivisibile in un contesto di ancora maggiore trasparenza e fiducia nelle istituzioni anche in ragione del rilevante impatto individuale del tracciamento. Né il mancato utilizzo dell'applicazione comporterà conseguenze in ordine all'esercizio dei diritti fondamentali dei soggetti interessati nel rispetto del principio di parità di trattamento (art. 6, c. 4, d.l. 28/2020).

[90] Dando così attuazione ai richiamati principi della *privacy by design* e *by default*.

[91] Il cui trattamento «deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato» (art. 9, par. 2, lett. *g*), GDPR).

[92] Il c. 6 dell'articolo chiarisce che ogni trattamento di dati personali dovrà cessare al termine del periodo di emergenza, e comunque non oltre il 31 dicembre 2020, con conseguente cancellazione dei dati trattati.

finalità diverse e ulteriori[93], rispetto a quelle stabilite dalla norma e rese note all'interessato, deve anche prevedere misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato anche in termini di selettività e minimizzazione dei dati[94].
In tal senso, dunque, si dovranno osservare le disposizioni normative introdotte, in attesa della concreta attuazione da parte del Ministero.

5. Conclusioni. Effettività delle politiche pubbliche *data driven.*

Il fenomeno non è tuttavia così semplice come si è tentato di descrivere. I *big data* pongono questioni molto rilevanti per il diritto pubblico e privato, portando alla luce fenomeni inediti e determinando un generale ripensamento (forse) degli istituti giuridici classici. Si pensi al controllo dei dati quale strumento di garanzia dell'indipendenza esterna degli Stati[95], al controllo dei dati per inedite forme di spionaggio e di attività di intelligence, al ripensamento delle categorie giuridiche classiche[96], degli strumenti regolatori antitrust[97], alla stessa insufficienza di forme di regolazione scoordinate tra loro[98].
L'utilizzo di *big data* è un fattore determinante nel perseguimento degli interessi (economici) delle imprese: è il fenomeno delle cd. *economie data driven*. Nel settore pubblico, invece, se si escludono casi più o meno isolati - ove non dettati dall'emergenza, come

[93] Il c. 3 prevede che i dati raccolti attraverso l'applicazione non possono essere utilizzati per finalità diverse da quelle fine di prevenzione e tutela della salute, salvo in forma aggregata o anonima per finalità scientifiche o statistiche.

[94] È stato precisato nel parere n. 79 del 29 aprile 2020 dell'Autorità garante per la protezione dei dati personali che «i dati raccolti devono poter tracciare i contatti stretti e non i movimenti o l'ubicazione del soggetto. Devono essere raccolti solo i dati strettamente necessari ai fini della individuazione dei possibili contagi, con tecniche di anonimizzazione e pseudonimizzazione affidabili. Anche la conservazione deve limitarsi al periodo strettamente necessario, da valutarsi sulla base delle decisioni dell'autorità sanitaria su parametri oggettivi come il periodo di incubazione». Recepito poi dal c. 2 dell'art. 6, d.l. 28/2020 nel senso di prevedere che i dati personali raccolti dall'applicazione siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al Covid-19, individuati secondo criteri stabiliti dal Ministero della salute; il trattamento effettuato per il tracciamento dei contatti sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati, con esclusione di ogni forma di geolocalizzazione dei singoli utenti; siano garantite su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento; i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo, stabilito dal Ministero della salute, strettamente necessario al tracciamento e cancellati in modo automatico alla scadenza del termine; i diritti degli interessati di cui agli artt. da 15 a 22 del regolamento possano essere esercitati anche con modalità semplificate.

[95] In tema, ad esempio, si veda G. Resta - V. Zeno Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour principles" al "privacy shield"*, Roma, 2016.

[96] In tema, ad esempio, si veda G. De Minico, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria,* in *Diritto Pubblico*, 1, 2019, 89 ss.

[97] In tema, ad esempio, si veda M. Maggiolino, *I Big data e il diritto antitrust*, cit.

[98] In tema, ad esempio, si veda V. Falce - G. Ghidini - G. Olivieri (a cura di), *Informazione e big data tra innovazione e concorrenza*, cit.; S. Gobbato, *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo,* cit.

visto -, il fenomeno, nonostante le potenzialità, ha una portata applicativa veramente ridotta.

L'utilizzo di *big data* da parte delle autorità pubbliche, mosse dal solo perseguimento di interessi collettivi, qualora coinvolga dati personali non è sempre accolto, a parere di scrive, con lo stesso entusiasmo (o, forse, superficialità) con cui si accetta di cedere (più o meno inconsapevolmente) i propri dati, i propri interessi, le proprie opinioni, in favore di società mosse solo da fini egoistici.

Vi è però un giusto compromesso tra scenari orwelliani ed un'autorità pubblica che non utilizzi pienamente gli strumenti di una rivoluzione, tecnologica ed industriale, in atto.

Un'autorità pubblica che orienti le proprie scelte anche, e non solo, sui risultati osservati tra le interazioni dei dati in proprio possesso è in grado di recuperare margini di efficienza tali da muovere un percorso virtuoso di sviluppo economico ed innovazione, fondamentale per il rilancio della competitività del Paese.

L'amministrazione pubblica detiene una grande quantità di dati che, ove utilizzati adeguatamente nei processi decisionali, ingenera due distinti effetti: da una parte, il ricorso a tecniche di *Data Analysis* garantirebbe una migliore allocazione delle risorse, sicuramente più efficiente, in grado di aumentare il benessere collettivo, la prosperità economica e la sicurezza pubblica; dall'altra, una pubblica amministrazione che sfrutti gli strumenti e le potenzialità dell'economia digitale orienterà il mercato con le proprie rinnovate richieste di figure professionali inedite e necessità di approvvigionamenti informatici e tecnologici tali da sviluppare l'offerta di tali servizi, a vantaggio, di nuovo, della competitività del Paese.

La recente, ed allo stato, ancora attuale, emergenza sanitaria ha mostrato come sia possibile aumentare l'efficacia e l'efficienza pubblica sfruttando i *big data* ma ha mostrato le gravi lacune tecnologiche della pubblica amministrazione (impossibilità di accesso al sito e violazione della *privacy* degli utenti per l'erogazione di sussidi per i lavoratori autonomi).

Pur nel suo contesto tragico, la necessità di individuare metodi efficaci, innovativi ed anche alternativi, di azione pubblica su larga scala ci ha mostrato un nuovo cammino: non resta che fare di necessità, virtù.

L'impiego di termocamere ad infrarossi nei locali aziendali: un'analisi sulle implicazioni giuridiche delle misure per il contrasto al "SARS-CoV-2" in ambito privacy e nel diritto del lavoro*

Elena Kaiser - Sofia Monici

Abstract

La crisi sanitaria dovuta alla diffusione della malattia COVID-19 ha sollevato diverse problematiche relative alla protezione dei dati personali, derivanti soprattutto dalle misure di sicurezza adottate (anche in ambito lavorativo) per prevenire la diffusione del contagio. Il presente articolo vuole analizzare, in particolare, se (ed a quali condizioni) l'uso di termocamere ad infrarossi all'ingresso dei locali aziendali sia compatibile con la normativa, di matrice europea, a tutela della privacy (il c.d. GDPR) e in particolare con le limitazioni alla raccolta ed al trattamento di dati "particolari", come quelli relativi alla salute. Al contempo, l'esigenza di impiegare tali strumenti richiede di esaminare le disposizioni normative che, in Italia, vietano il compimento di accertamenti ed indagini sullo stato di salute dei lavoratori e che regolano, a particolari condizioni, l'installazione di impianti di videosorveglianza nei luoghi di lavoro.

The crisis caused by the outbreak of the COVID-19 pandemic has raised several issues concerning the protection of personal data, deriving above all from the security measures adopted (also in the workplace) to prevent the spread of the infection.
This article wants to analyze, in particular, if (and under what conditions) the use of infrared thermal cameras at the entrance of company premises is compatible with the GDPR and in particular with the limitations on the collection and processing of "particular" data, such as those relating to health.
At the same time, the need to use these tools requires an analysis of the national (Ita-

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

lian) legal framework which prohibits carrying out checks and investigations on the workers' health and which, under particular conditions, regulates the installation of video surveillance systems in workplaces.

Sommario

Keywords

GDPR - Covid-19 – obblighi datore di lavoro – termocamere - privacy

1. Premessa

L'attuale emergenza sanitaria dovuta alla diffusione del virus "SARS-Cov-2"[1] - identificato come la causa della malattia respiratoria chiamata "COVID-19"[2] - e la conseguente necessità di contrastare l'ulteriore propagazione della pandemia[3] hanno sollevato diverse questioni giuridiche legate al problematico bilanciamento tra il diritto alla salute e il diritto[4] alla protezione dei dati personali[5].

Il presente articolo affronta, in particolare, il tema del trattamento dei dati personali

[1] Acronimo inglese per "*Severe Acute Respiratory Syndrome* - Coronavirus – 2", per distinguerlo dal virus responsabile dell'epidemia del 2002 in Cina.

[2] Acronimo inglese per "*Corona Virus Disease 2019*".

[3] L'ufficializzazione dello *status* di "pandemia" è avvenuto l'11 febbraio 2020. V. la dichiarazione del direttore generale dell'Organizzazione mondiale della sanità (OMS), Tedros Adhanom Ghebreyesus "*WHO Director-General's opening remarks at the media briefing on COVID-19*".

[4] Come noto, la Carta dei diritti fondamentali dell'Unione europea (in *G.U.C.E.* 364 del 18 dicembre 2000) ed il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (in *G.U.U.E.* L 119 del 4 maggio 2016), riconoscono la tutela dei dati personali come un diritto fondamentale dell'individuo.

[5] Ad esempio, è ormai noto l'accesso dibattito legato alle applicazioni di tracciamento del virus tramite servizi di localizzazione degli utenti.

e specialmente dei dati sanitari - considerati, come si vedrà, categorie speciali di dati ai sensi dell'art. 9 del regolamento (UE) 2016/679 (anche noto come "*General Data Protection Regulation"* o GDPR) - nell'ambito dei rapporti di lavoro, in questo periodo di emergenza[6].

L'art. 2087 c.c. pone, come noto, a carico dell'imprenditore l'obbligo di tutelare l'integrità psicofisica dei propri dipendenti, dal quale deriva l'esigenza di predisporre all'interno degli ambienti di lavoro le necessarie e potenzialmente invasive misure di prevenzione dal contagio.

Al riguardo, più nello specifico, ci si domanda a che condizioni ed in quale misura le imprese possano fare ricorso - al fine di rilevare temperature sospette della presenza della patologia COVID-19 - a telecamere termografiche che misurino la temperatura dei dipendenti e visitatori all'ingresso sul luogo di lavoro.

Un'ulteriore questione giuridica oggetto di approfondimento è quella relativa alle particolari garanzie che devono assistere l'installazione di impianti di videosorveglianza nei luoghi di lavoro, tanto alla luce delle "linee-guida" elaborate nel contesto europeo quanto alla luce delle norme nazionali. Infine, sempre tenuto conto della natura dei dati sanitari, verranno esaminati i limiti dettati dalla normativa interna circa l'esecuzione di accertamenti sanitari sui luoghi di lavoro e, in particolare, le condizioni per la richiesta di esami e per la raccolta di dati relativi allo stato di salute dei dipendenti.

2. Le misure di contrasto al virus "SARS-COV-2" nei luoghi di lavoro

Prima di esaminare le questioni giuridiche sottese all'impiego della termografia in ambito lavorativo, occorre fare un passo indietro per comprendere come l'esigenza della rilevazione della temperatura corporea si collochi nel quadro delle misure varate dalle autorità in questo periodo di emergenza.

Tra il 9 marzo ed il 18 maggio 2020, nell'ambito degli interventi volti a contenere il grave rischio sanitario dovuto appunto alla diffusione del virus "SARS-CoV-2", il Governo Italiano (come quasi ogni altro Paese[7]) ha adottato una serie di misure volte ad introdurre importanti limitazioni agli spostamenti ed alla circolazione delle persone nonché allo svolgimento delle attività lavorative[8].

---

[6] A livello nazionale "lo stato di emergenza" è stato dichiarato, inizialmente per sei mesi, dal Consiglio dei Ministri con delibera del 31 gennaio 2020 (pubblicata in *G.U.R.I.* Serie Generale n. 26 dell'1 febbraio 2020) ai sensi dell'art. 24 d.lgs. 2 gennaio 2018, n. 1 (Codice della Protezione Civile, pubblicato in *G.U.R.I.* Serie Generale n. 17 del 22 gennaio 2018).-Ritenuta la persistenza della situazione emergenziale, il Consiglio dei Ministri ha successivamente prorogato lo "stato di emergenza" con delibera del 29 luglio 2020 e, poi, con delibera del 7 ottobre 2020, fino al 31 gennaio 2021.

[7] È rimasta isolata la reazione della Svezia che ha stabilito di non introdurre misure di c.d. *lockdown.*

[8] Facendo ampio ricorso allo strumento del Decreto del Presidente del Consiglio dei Ministri (*breviter* DPCM) - sulla base di una sorta di "delega in bianco" contenuta dapprima nel d.l. 23 febbraio 2020, n. 6 (in *G.U.R.I.* Serie Generale n. 45 del 23 febbraio 2020), convertito con l. 5 marzo 2020, n. 13 (in *G.U.R.I.* n. 61 del 9 marzo 2020) e successivamente del d.l. 25 marzo 2020, n. 19 (in *G.U.R.I.* Serie Generale n. 79 del 25 marzo 2020) convertito con l. 22 maggio 2020, n. 35 (in *G.U.R.I.* n. 132 del 23 marzo 2020). - per comprimere, «con un'intensità senza precedenti» (cfr. in dottrina L. Cuocolo, *I diritti*

Più in particolare, nell'ottica di ridurre al minimo i contatti interpersonali per frenare la propagazione del contagio, - con una serie di provvedimenti che si sono avvicendati a far data dall'11 marzo 2020 (DPCM 11 marzo 2020[9], DPCM 22 marzo 2020[10], DPCM 10 aprile 2020[11], DPCM 26 aprile 2020[12] e DPCM 17maggio 2020[13]) - il Governo ha parzialmente sospeso le attività produttive, commerciali e professionali, consentendo la prosecuzione delle attività lavorative limitatamente ai soli settori necessari per fornire un servizio reputato essenziale per la popolazione[14].

In tale periodo, la prosecuzione dell'attività lavorativa nell'ambito dei settori di attività consentiti è stata, inoltre, subordinata all'attuazione di specifici protocolli di sicurezza c.d. anticontagio (art. 1, punto 7, lett. *d*), DPCM 11 marzo 2020), ossia alla condizione che venissero messe in atto, da parte delle imprese, - in attuazione dell'obbligo sulle stesse incombente ai sensi del citato art. 2087 c.c. - specifiche misure e procedure volte a salvaguardare la salute dei lavoratori, così come dei terzi (fornitori e clienti) aventi accesso ai locali aziendali[15].

Relativamente alla definizione dei contenuti di tali protocolli di sicurezza, l'art. 1, c. 1, punto n. 9 del DPCM 11 marzo 2020 ha espressamente manifestato l'intenzione del Governo di favorire l'adozione di intese tra le organizzazioni dei datori di lavoro e dei lavoratori ossia tra le associazioni portatrici degli interessi delle parti direttamente riguardate dalle misure, evidentemente con l'auspicio che venissero individuate delle soluzioni idonee a contemperare le istanze di sicurezza provenienti dai lavoratori con le esigenze organizzative e produttive dell'impresa.

Su invito del Governo, pertanto, il 14 marzo 2020 le parti sociali hanno sottoscritto il documento denominato "Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro" (di seguito, per brevità, "Protocollo condiviso"). Al punto n. 2, rubricato "Modalità di ingresso in azienda", le stesse hanno espressamente previsto la facoltà del datore di lavoro di sottoporre il personale, prima dell'accesso ai locali aziendali, al controllo della temperatura corporea al fine di verificare la presenza di un eventuale stato febbrile (temperatura superiore alla soglia di 37,5° centigradi) per procedere con l'immediato isolamento ed allontanamento dal posto di lavoro. Il punto. n. 3 ha inoltre indicato che le stesse procedure di accesso in azienda debbano essere applicate anche

costituzionali di fronte all'emergenza COVID-19: la reazione italiana, in *federalismi.it*, Osservatorio emergenza COVID-19, 13 ss.), diritti e libertà di rango costituzionale, tra cui la libertà personale (art. 13 Cost.), la libertà di circolazione e di soggiorno (art. 16 Cost.), il diritto al lavoro (art. 4 Cost.), il libero esercizio dell'attività di impresa (art. 41 Cost.).

[9] DPCM 11 marzo 2020, pubblicato in *G.U.R.I.* Serie Generale n. 64 del 11 marzo 2020.

[10] DPCM 22 marzo 2020, pubblicato in *G.U.R.I.* Serie Generale n. 76 del 22 marzo 2020.

[11] DPCM 10 aprile 2020, pubblicato in *G.U.R.I.* Serie Generale n. 97 del 11 aprile 2020.

[12] DPCM 26 aprile 2020, pubblicato in *G.U.R.I.* Serie Generale n.108 del 27 aprile 2020.

[13] DPCM 17 maggio 2020, pubblicato in *G.U.R.I.* Serie Generale n. 126 del 17 maggio 2020.

[14] La limitazione all'attività imprenditoriale trova, invero, già a livello costituzionale, una sua giustificazione nel secondo comma dell'art. 41 Cost. ai sensi del quale la stessa «non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana».

[15] Fermo restando, comunque, l'invito a favorire – ove possibile – il ricorso al lavoro agile, a ferie e permessi, ovvero agli ammortizzatori sociali.

nei confronti di utenti esterni, visitatori e clienti nonché fornitori.
Come risulta dalla relativa "premessa", il Protocollo condiviso è stato elaborato per fornire semplici "linee-guida" e "raccomandazioni", non obblighi. Nondimeno, con il successivo DPCM 10 aprile 2020, l'adozione delle misure del Protocollo è stata espressamente prevista come condizione per la prosecuzione dell'attività[16], con la precisazione che «la mancata attuazione dei protocolli che non assicuri adeguati livelli di protezione determina la sospensione dell'attività fino al ripristino delle condizioni di sicurezza»[17].
La decisione di attribuire natura vincolante - e non meramente programmatica – al Protocollo condiviso (nel frattempo integrato e perfezionato in data 24 aprile) è stata riconfermata anche dal successivo DPCM 26 aprile 2020[18] che ha inaugurato quella che è stata definita la c.d. "fase 2"[19], nonché dagli ulteriori provvedimenti emanati dopo tale data.
Inoltre, tenuto conto della specificità di alcuni settori di attività, quali quello logistico e dell'edilizia, che prevedono più limitate possibilità di attuare il distanziamento sociale, sono stati elaborati – rispettivamente a fine marzo ed a fine aprile 2020 - due ulteriori protocolli "speciali", anch'essi resi obbligatori per tutte le imprese rimaste o ritornate operative[20]. Tra le misure ivi contenute figura anche l'obbligo (e non già la semplice facoltà) di rilevare la temperatura all'ingresso dei cantieri[21].
Infine, il d.l. 33 del 2020[22] ha ulteriormente integrato le condizioni per la riapertura dei settori di attività sospesi, prevedendo l'adozione – sempre a pena di sospensione

[16] Cfr. art. 1, c. 6: «Le imprese le cui attività non sono sospese rispettano i contenuti del protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro sottoscritto il 24 aprile 2020 tra il Governo e le parti sociali [..], nonché, per i rispettivi ambiti di competenza» gli ulteriori adottati dalle parti sociali».

[17] Al riguardo, l'Ispettorato Nazionale del Lavoro (INL) chiamato a fornire alle proprie articolazioni a livello territoriale le indicazioni per supportare le Prefetture nell'ambito delle verifiche circa la ricorrenza delle condizioni previste per la prosecuzione (ove consentita) delle attività produttive, industriali e commerciali, con la propria nota n. 149 del 20 aprile 2020, ha infatti fornito ai propri Ispettori una "*Check list*" che ricalca pedissequamente i contenuti del Protocollo condiviso.

[18] Anche se l'adozione delle misure di sicurezza previste dai menzionati Protocolli non fosse stata resa espressamente vincolante dalla normativa emergenziale, l'attuazione di ogni misura necessaria a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro – «secondo la particolarità del lavoro, l'esperienza e la tecnica» – fa parte degli obblighi che gravano su ciascun datore ai sensi dell'art. 2087 c.c., unitamente a quelli previsti dal d.lgs. 81/2008. Questa è la ragione per cui, ove richiesto dalle circostanze, ciascun datore di lavoro è tenuto ad adottare, oltre alle procedure previste espressamente dal protocollo, ogni altra misura che si renda eventualmente necessaria alla luce delle specifiche modalità di organizzazione del lavoro.

[19] Per "Fase 2" si intende il periodo di progressiva riduzione delle misure di *lockdown*.

[20] Cfr. il Protocollo condiviso di regolamentazione per il contenimento della diffusione del COVID-19 nei cantieri, sottoscritto il 24 aprile 2020 fra il Ministro delle infrastrutture e dei trasporti, il Ministero del lavoro e delle politiche sociali e le parti sociali, nonché il Protocollo condiviso di regolamentazione per il contenimento della diffusione del COVID-19 nel settore del trasporto e della logistica sottoscritto il 20 marzo 2020.

[21] Cfr. p. 3 del Protocollo: «il personale, prima dell'accesso al cantiere dovrà essere sottoposto al controllo della temperatura corporea. Se tale temperatura risulterà superiore ai 37,5°, non sarà consentito l'accesso al cantiere».

[22] Pubblicato in *G.U.R.I.* Serie Generale n. 125 del 16 maggio 2020, convertito con modificazioni dalla l. 14 luglio 2020, n. 74 (in *G.U.R.I.* 15 luglio 2020, n. 177).

dell'attività[23] - di ulteriori «protocolli e linee guida [..], adottati dalle regioni o dalla Conferenza delle regioni e delle province autonome", contenenti indirizzi specifici per alcuni settori di attività[24]. Questi ultimi «riprendendo le misure di prevenzione e contenimento riconosciute a livello scientifico»[25], hanno confermato l'opportunità di effettuare la rilevazione della temperatura corporea del personale e dei terzi visitatori. Anche nell'ambito della c.d. "fase 3" dell'emergenza (tutt'ora in corso), che ha visto la riapertura – con decorrenza dal 15 giugno 2020 – di buona parte delle attività ancora sospese ed un ulteriore "allentamento" delle misure varate, il Governo[26] ha continuato a ribadire la necessaria applicazione delle raccomandazioni contenute nel Protocollo condiviso con sindacati ed imprese, nonché delle linee guida elaborate dalle Regioni o dalla Conferenza delle Regioni e delle province autonome limitatamente a specifici settori di attività.

Vale la pena sottolineare che, proprio a livello Regionale, la normativa ha introdotto in alcuni casi un vero e proprio obbligo (e non già una mera facoltà) di misurazione della temperatura corporea del personale. Ciò è accaduto in particolare in Lombardia – in assoluto la regione più colpita dal virus – che ha scelto espressamente di imporre (e non soltanto facoltizzare) la misurazione della temperatura corporea, sia prima dell'accesso sul luogo di lavoro, che durante l'attività lavorativa[27].

3. L'utilizzo della termografia nella prevenzione e controllo delle epidemie: dai termometri ad infrarossi alle termocamere

Non è una novità che tra i sistemi di contenimento delle epidemie venga utilizzato il metodo della rilevazione sistematica della temperatura corporea. L'esperienza delle epidemie "Mers" e "SARS" nei Paesi asiatici e l'"Ebola" in Africa, infatti, ci ha insegnato l'importanza dei controlli atti a verificare, in tempi rapidi, la presenza di una sintomatologia compatibile con l'infezione, allo scopo di individuare ed isolare tempestivamente i soggetti potenzialmente "positivi" al virus. Un sintomo che può

[23] Art. 1, c. 15, d.l. 33/2020.

[24] Cfr. art. 1, c. 14, d.l. 33/2020. Si badi che in assenza di quelli regionali, è espressamente previsto che trovino applicazione i protocolli o le linee guida adottati a livello nazionale.

[25] Cfr. Linee Guida per la riapertura delle Attività economiche e Produttive, 16 maggio 2020, aggiornate in data 25 maggio.

[26] V. art. 2 e allegati da 12 a 14 del DPCM 11 giugno 2020 (in *G.U.R.I.* 11 giugno 2020, n. 147), nonché il DPCM 14 luglio 2020 (in *G.U.R.I.* 14 luglio 2020, n.176) che ha prorogato le misure disposte dal precedente DPCM 11 giugno aggiornando, all'allegato 1, le "linee guida Linee guida per la riapertura delle Attività Economiche, Produttive e Ricreative". V. altresì l'art. 2 e gli allegati 9, 12, 13 e 14 del DPCM 7 agosto 2020 (in *G.U.R.I.* 7 agosto 2020, n. 198) le cui misure sono state poi prorogate dal DPCM 7 settembre 2020 (in *G.U.R.I.*, 7 settembre 2020, n. 222). Infine, nelle more dell'adozione di un nuovo DPCM, l'art. 5 del d.l. 7 ottobre 2020, n. 125 (in *G.U.R.I.*, 7 ottobre 2020, n. 248, in vigore alla data di redazione del presente contributo) ha disposto l'ultrattività del DPCM 7 settembre 2020 fino al 15 ottobre 2020.

[27] V. le ordinanze della Regione Lombardia n. 546 del 13 maggio 2020, n. 547 del 17 maggio 2020, n. 555 del 29 maggio 2020. Da ultimo, l'ordinanza n. 604 del 10 settembre 2020.

essere verificato in modo immediato è, naturalmente, la presenza di un eventuale stato febbrile. Pertanto, nelle citate esperienze, la rilevazione della temperatura corporea è risultata fondamentale per rallentare la crescita del contagio.

Già all'epoca, sono apparsi inadeguati gli strumenti tradizionali di rilevazione della temperatura, ossia i classici termometri in vetro[28] ed i termometri digitali, poiché non sono in grado di consentire la misurazione della temperatura di un elevato numero di persone, in tempi celeri e senza la formazione di rischiosi assembramenti. Infatti, come noto, la corretta misurazione attraverso termometri classici richiede almeno 4-5 minuti per paziente. Inoltre, l'eventualità che un termometro di questo tipo - attraverso un contatto diretto con il paziente - divenga, a sua volta, veicolo di contagio, sconsiglia ovviamente il suo riutilizzo, imponendo viceversa il ricorso a termometri "usa e getta".

È stata pertanto esplorata la possibilità di utilizzare una diversa tecnologia ed in particolare la termografia ad infrarossi, la quale - pur avendo normalmente altre prevalenti applicazioni[29] - può essere impiegata anche in ambito medico per consentire (tra l'altro) una misurazione della temperatura più veloce e, soprattutto, senza contatto diretto dello strumento con il paziente.

In una prima fase, si è assistito all'impiego, in stazioni, aeroporti, luoghi pubblici, di termometri ad infrarossi c.d. "a pistola", ossia di termometri manuali «puntati verso la fronte o verso la mano [..] a una distanza massima di 15 centimetri»[30]. L'esigenza di mantenere una distanza ravvicinata e comunque la limitata accuratezza dei termometri a pistola[31] ha, tuttavia, condotto a sostituire questi modelli con le c.d. telecamere termografiche o termocamere.

Senza addentrarci nei profili tecnici, per quanto rilevante ai fini del presente lavoro, le termocamere sono uno strumento in grado di rilevare l'energia termica rilasciata da un oggetto o da un corpo (sotto forma di onde elettromagnetiche), rendendo visibile, su display o monitor, la distribuzione del calore del corpo inquadrato.

Al di là delle caratteristiche dei diversi modelli (che verranno di seguito meglio approfondite) si distinguono in due macro categorie: le termocamere c.d. non radiometriche, le quali si limitano a generare una "fotografia termica" che rappresenta la distribuzione del calore del corpo o dell'oggetto ripreso e le termocamere radiometriche che, oltre a convertire l'energia termica in immagine, misurano la temperatura superficiale di ogni pixel del sensore, offrendo la lettura di un dato in gradi centigradi. Naturalmente sono principalmente le seconde a poter essere impiegate come strumento di controllo dell'epidemia, in quanto appunto esprimono in centigradi il dato relativo alla temperatura del soggetto inquadrato.

---

[28] Termometro in vetro simile in tutto e per tutto a quello a mercurio (vietato da aprile 2009), contiene all'interno una lega di metalli meno inquinante chiamata Galinstan, fluida a temperatura ambiente.

[29] Nella sorveglianza militare, nella prevenzione degli incendi, a tutela dell'ambiente (ad esempio per misurare le temperature degli oceani e, anche in medicina, per analisi non invasive dei tessuti e dei fluidi).

[30] L. Berberi, *Coronavirus, controlli con gli scanner termici negli aeroporti italiani,* in *Corriere della Sera*, 4 febbraio 2020.

[31] Cfr. l'articolo del New York Times di D. Yaffe-Bellany, *'Thermometer Guns' on Coronavirus Front Lines Are 'Notoriously Not Accurate'*, 14 febbraio 2020, sul sito *nytimes.com.*

La precisione delle letture della misurazione della temperatura della pelle dipende da diversi fattori come «la fotocamera utilizzata, la sensibilità del piano focale, le impostazioni della fotocamera e la distanza dagli obiettivi»[32].

4. Le caratteristiche (potenzialmente molto invasive) dei principali modelli di termocamere in commercio

Se ciò che accomuna tutte le termocamere è la possibilità di rilevazione della temperatura corporea senza alcun contatto diretto con l'astante, in commercio esistono modelli con caratteristiche anche molto diverse e che richiedono, di conseguenza, un approccio e riflessioni differenti.
Senza alcuna pretesa di esaustività, al solo fine di analizzare le possibili implicazioni dell'utilizzo di tale tecnologia, è opportuno cercare di sintetizzare le caratteristiche più diffuse[33].
Alcuni modelli sono in grado di effettuare la misurazione ad una distanza di circa un metro/ un metro e mezzo, altri possono consentire la rilevazione con un raggio ben più lungo, oltre i 9-10 metri. Alcuni di questi, studiati per ambienti ampi ed affollati, consentono inoltre di "catturare" il dato relativo alla temperatura corporea di più persone contemporaneamente (anche fino a 20-30 persone). Altri, invece, sono maggiormente indicati per i controlli a "imbuto", cioè nei passaggi obbligati che incanalano il flusso di transito.
Dal punto di vista estetico e della portabilità, le termocamere possono essere fisse o portatili.
Quelle portatili sono pensate per un utilizzo manuale da parte di un operatore e, di conseguenza, hanno un raggio più ridotto; inoltre, sono normalmente dotate di un *display*, ma alcune possono anche essere collegate ad un monitor esterno. In alcuni casi contemplano la memorizzazione dei dati, ma nella maggior parte dei casi non registrano la temperatura rilevata, la quale viene semplicemente mostrata sul display per l'intervento immediato da parte dell'operatore. Il raggio ridotto di ripresa presuppone ovviamente una certa vicinanza dell'operatore come accade anche per i termometri infrarossi a pistola.
Quelle "fisse" possono essere applicate su diversi tipi di supporto: i) fissate a parete o a soffitto, in collegamento con sistemi di videosorveglianza; ii) installate su colonnine mobili (i c.d. *totem*); iii) o ancora posizionate e collocate, tipicamente attraverso bracci meccanici e pedane, su banconi o tornelli nonché a porte automatiche di accesso.
Mentre le termocamere collegate ai sistemi di accesso hanno normalmente uno schermo che riprende il volto del soggetto ed evidenzia il dato relativo alla temperatura, negli altri due casi sono normalmente collegate a sistemi esterni di videosorveglianza.
Infine, esiste un particolare modello integrato direttamente sui caschi (c.d. *helmet*); ide-

[32] C. Dominelli, *Coronavirus: l'Oms punta sulle termocamere per rafforzare la lotta al COVID-19*, in *Il Sole 24 Ore*, 17 aprile 2020.

[33] La panoramica che segue è il risultato del confronto dei siti internet di rivenditori e produttori di tali prodotti.

ato per essere impiegato nell'ambito delle operazioni di soccorso, nell'ultimo periodo è stato riconvertito anche per le finalità di contrasto al virus ed è in dotazione alle forze dell'ordine[34].

Naturalmente a seconda della tipologia di strumento adoperato, è possibile che sia necessario il supporto di uno (o più) operatori dedicati, i quali possono essere collocati presso appositi "varchi" di ingresso, oppure essere chiamati a gestire il dispositivo da remoto, attraverso videoterminali.

Alcuni di questi dispositivi, infine, oltre al mero rilevamento della temperatura corporea, possiedono ulteriori funzionalità potenzialmente molto invasive, alle volte predefinite (di fabbrica o di *default*) oppure opzionali. Alcuni modelli sono, ad esempio, in grado di verificare se il soggetto ripreso indossa o meno i dispositivi di protezione (nella fattispecie la mascherina); altri presentano un sistema di riconoscimento facciale integrato o possono essere associati a sistemi elettronici di rilevazione degli accessi e di apertura automatica di porte e cancelli attraverso l'identificazione del soggetto che viene ripreso (ad es. al badge in dotazione ai dipendenti). Infine, dal momento che si tratta di strumenti che sono stati pensati per la rilevazione della temperatura in ambienti caratterizzati da un'alta pedonabilità e flussi di folla, come appunto gli aeroporti, alcuni di questi sistemi consentono la creazione di *white e black list* per individuare le persone segnalate anche dopo il loro passaggio.

Da ultimo, circa il profilo della memorizzazione o esportazione dei dati, come anticipato alcune termocamere dispongono di *memory card* interne che registrano in modo indiscriminato tutte le rilevazioni. Altri dispositivi prevedono, invece, l'esportazione automatica ed in tempo reale delle misurazioni.

Questa panoramica mette in evidenza che, se sfruttate in tutte le loro potenzialità, le termocamere possono rivelarsi strumenti potenzialmente anche molto invasivi, a maggior ragione in ambiente lavorativo.

5. Le questioni giuridiche emergenti

In tal contesto, molte aziende hanno cominciato ad interrogarsi se fosse opportuno e possibile installare termocamere ad infrarossi all'ingresso dei locali aziendali[35].

Inoltre, prima dell'avvio della c.d. "fase 2", il Governo aveva preso in considerazione l'idea di rendere addirittura obbligatoria l'installazione di termocamere, oltre che nei luoghi di accesso al pubblico, anche all'ingresso delle aziende[36].

---

[34] Dall'inizio di maggio 2020 sono utilizzati dal personale dell'aeroporto internazionale di Fiumicino a Roma. Si tratta di «una soluzione che combina termoscanner, realtà aumentata ed ha una struttura modulare che permette di espanderne le funzionalità con l'aggiunta di ulteriori sensori, come quello per la lettura dei codici QR e a barre; in futuro potrebbe essere quindi usato anche per controllare la validità dei biglietti aerei» (cfr. l'articolo *Caschi smart all'aeroporto di Fiumicino per rilevare la temperatura corporea* dell'8 maggio scorso, pubblicato sul blog online *HDblog.it*).

[35] Come già avvenuto in Cina sin dalla fine di gennaio. Cfr. il servizio *Wuhan virus: More companies looking to buy thermal scanners,* realizzato dalla CNA il 24 febbraio 2020 e disponibile sul canale ufficiale Youtube.

[36] Secondo quanto riferito nell'articolo "*Coronavirus Fase 2 Termoscanner all'ingresso di negozi ed uffici*", pubblicato sul sito Web del Corriere della Sera il 15 aprile 2020, che riporta gli stralci delle dichiarazioni del Ministro della Salute, Pierpaolo Sileri, secondo il quale il termoscanner «Dovrà [ndr. avrebbe dovuto]

Tali proposte non si sono poi concretizzate. Tuttavia, numerose imprese, specie quelle di grandi dimensioni, hanno ugualmente deciso di dotarsi di tali strumenti[37].
È, quindi, importante esplorare le implicazioni giuridiche dell'utilizzo di tale tecnologia.
Anzitutto, ci si domanda ovviamente se l'uso di termometri o di termocamere ad infrarossi all'ingresso dei locali aziendali sia compatibile con la normativa, di matrice europea, a tutela della privacy e in particolare con le limitazioni alla raccolta ed al trattamento di dati "particolari", come quelli relativi alla salute.
Al contempo, l'esigenza di impiegare tali strumenti solleva alcuni interrogativi con riferimento alle rigorose disposizioni normative previste in Italia che vietano il compimento di accertamenti ed indagini sullo stato di salute dei lavoratori e che regolano, a particolari condizioni, l'installazione di impianti di videosorveglianza nei luoghi di lavoro.
In estrema sintesi, dunque, la questione deve essere esaminata sotto due differenti profili:
da un lato, sotto il profilo della liceità della raccolta e del trattamento di tali dati nel rispetto della normativa vigente in materia di privacy (regolamento UE 679/2016, nonché d.lgs. 196/2003, come modificato, da ultimo, dal d.lgs. 110/2018);
dall'altro lato, sotto il profilo dei limiti al potere di controllo da parte del datore di lavoro stabiliti dallo Statuto dei lavoratori e, in particolare, dagli artt. 4 e 5 dello statuto; il primo limita l'installazione di impianti audiovisivi o altri strumenti dai quali derivi potenzialmente *"anche la possibilità di un controllo a distanza*" sull'attività dei dipendenti, il secondo vieta l'effettuazione di accertamenti sanitari da parte del datore di lavoro.

6. Il quadro normativo: il diritto alla tutela dei dati personali nella normativa europea e nazionale ed il necessario coordinamento con la speciale normativa giuslavoristica

La rilevazione della temperatura corporea costituisce un vero e proprio trattamento dei dati personali[38] che, pertanto, deve avvenire ai sensi della disciplina vigente in materia.
La normativa cui fare riferimento è il regolamento (UE) 2016/679 (c.d. GDPR) che ha introdotto una regolamentazione uniforme a livello dell'Unione europea (da qui in avanti, per brevità, UE).
La disciplina europea è però completata, a livello nazionale, dalle disposizioni del c.d.

essere sistemato all'ingresso di tutti i luoghi dove ci sono persone che lavorano, esattamente come i guanti, le mascherine e gli erogatori per il disinfettante». «Si tratta di un accorgimento indispensabile, la temperatura alta è uno dei sintomi caratteristici di questa malattia e dunque bisogna prevederlo ovunque».

[37] La notizia è stata riportata da diversi quotidiani. Cfr. C. Dominelli, *Coronavirus: le grandi aziende si attrezzano con le termocamere in vista della ripartenza*, in *Il Sole 24 ore*, 8 aprile 2020, che menziona (tra le altre) Ferrero, Generali, ArcelorMittal.

[38] Come riconosciuto anche dal Protocollo condiviso del 14 marzo 2020, alla nota n. 1 a pagina 5.

Codice per la protezione dei dati personali (D.lgs. 196/2003[39] e da qui in prosieguo "Codice privacy"), come modificato dal D.lgs. 101/2018[40] che, in attuazione della legge delega 25 ottobre 2017 n. 163[41,] ha provveduto ad adeguare le disposizioni previgenti alla regolamentazione europea.

Benché, infatti, il GDPR sia un atto di diritto dell'UE dotato di diretta applicabilità, che - come tale – non avrebbe richiesto alcun atto interno di recepimento, agli Stati membri è lasciato un margine di apprezzamento per implementare a livello nazionale alcune materie[42], tra le quali rientra anche la materia del diritto del lavoro[43].

Nello specifico – in virtù del margine di discrezionalità previsto dal regolamento all'art. 88[44] - gli Stati membri sono autorizzati a «prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di

[39] Pubblicato in *G.U.R.I.* n. 174 del 29 luglio 2003 - Suppl. Ordinario n. 123.

[40] Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), pubblicato in *G.U.R.I.* Serie Generale n. 205 del 4 settembre 2018.

[41] Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017, pubblicata in *G.U.R.I.* 6 novembre 2017, n. 259. In particolare, il Parlamento Italiano ha delegato il governo ad: a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, [..] incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679; b) modificare il codice [..] limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento [..]; c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento [..]; d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento [..]; e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento [..] con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

[42] Cfr. considerando 10 GDPR «[….] Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE, gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito».

[43] Cfr. A. Miani - A. Foschi (a cura di) *La tutela della privacy del lavoratore controllato a distanza*, Documento del 31 ottobre 2019, elaborato dal Consiglio Nazionale dei Dottori Commercialisti e degli esperti contabili, 30 ss.

[44] Cfr. anche V. Turco*, Il trattamento dei dati personali nell'ambito del rapporto di lavoro*, in V. Cuffaro - R. D'Orazio - V. Ricchiuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 517.

lavoro, [..]»[45] a condizione che queste non contraddicano i principi del GDPR[46].
Si rende, dunque, necessario un coordinamento tra le norme di diritto dell'UE e la specialità della normativa nazionale in ambito giuslavoristico. L'Italia, in particolare, si è avvalsa della facoltà prevista dall'art. 88 GDPR, facendo salve le specifiche previsioni nazionali[47] disposte in *primis* dallo Statuto dei Lavoratori (Legge 20 maggio 1970, n. 300)[48] dal quale, come noto, discendono importanti limiti al potere di controllo esercitabile da parte del datore di lavoro nei confronti dei propri dipendenti[49]. Un espresso richiamo a tali previsioni è, pertanto, contenuto nel sopraccitato Codice Privacy, all'interno della Parte II, titolo VIII, rubricata "Trattamenti nell'ambito del rapporto di lavoro". L'art. 113 - ribadendo che «resta fermo quanto disposto dall'art. 8 della legge 20 maggio 1970, n. 300[50], nonché dall'art. 10 del decreto legislativo 10 settembre 2003, n. 276[51]» - non fa altro che richiamare il generale divieto per il datore di lavoro di effettuare indagini su dati e informazioni che non hanno una attinenza con l'attitudine

[45] Ai sensi del par. 2 dell'art. 88 GDPR: «Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro».

[46] In dottrina cfr. M. Brkan, *Introduction: Employee's Privacy at the Forefront of Privacy Debates,* in *EDPL,* 2017, 543.

[47] Cfr. art. 9, d.lgs. 101/2018. Ancora V. Turco*, Il trattamento dei dati personali nell'ambito del rapporto di lavoro*, cit., 518.

[48] Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento (in *G.U.R.I.* Serie Generale n. 131 del 27 maggio 1970). Il riferimento è, in particolare agli artt. 1, 2, 3, 4, 5, 6 e 8.

[49] Da tempo gli studiosi hanno, invero, osservato che tali limiti – «legati a una particolare concezione dell'impresa e del modo di organizzare l'attività produttiva che riflette le esigenze e le problematiche proprie del periodo storico e culturale in cui lo Statuto fu emanato» – non sono più adeguati alle nuove forme di organizzazione dell'impresa ed alle esigenze contraddistinte dall'impiego di tecnologie informatiche che rendono non solo più facile, ma a volte inevitabile l'acquisizione di informazioni. Da qui, «la necessità di ridefinire i limiti al potere di indagine del datore di lavoro e ricercare nuovi equilibri di conciliazione tra i valori fondamentali del lavoratore e le mutate esigenze di organizzazione dell'impresa» (I. Bresciani, *Le forme di controllo nello Statuto dei lavoratori: orientamenti giurisprudenziali e questioni di attualità*, in *Variazioni su Temi di Diritto del Lavoro*, 4, 2016, 731 ss.) che sulla scorta di alcune aperture giurisprudenziali ha condotto negli ultimi anni ad alcune riforme, particolarmente in tema di videosorveglianza.

[50] «È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore».

[51] «1. È fatto divieto alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonché ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento della attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa. È altresì fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo. 2. Le disposizioni di cui al comma 1 non possono in ogni caso impedire ai soggetti di cui al medesimo comma 1 di fornire specifici servizi o azioni mirate per assistere le categorie di lavoratori svantaggiati nella ricerca di una occupazione».

allo svolgimento della prestazione di lavoro. Il successivo art. 114 contiene un analogo richiamo alle garanzie previste dall'art. 4 St. Lav. a proposito dell'utilizzo di impianti audiovisivi ed altri strumenti di lavoro dai quali possa derivare, potenzialmente, anche un controllo a distanza sull'attività dei lavoratori. A sua volta, il nuovo art. 4 St. Lav., come si vedrà in prosieguo, contiene un rinvio al rispetto della normativa a tutela dei dati personali. Tale richiamo ha, evidentemente, la funzione di subordinare il trattamento e la raccolta dei dati da parte del datore di lavoro al rispetto delle regole imposte in materia di privacy a livello europeo[52]. Costituisce, da ultimo, un ulteriore limite al trattamento dei dati personali dei lavoratori - sebbene manchi un espresso richiamo nel Codice Privacy - anche il divieto di compimento di accertamenti sanitari previsto dall'art. 5 dello Statuto dei Lavoratori.

La normativa privacy e quella di diritto del lavoro sono dunque strettamente collegate e risulta opportuno esaminarle congiuntamente, affrontando in modo trasversale le questioni che derivano dalla particolare tipologia dei dati trattati (la febbre, ossia un dato relativo alla salute) e dalla tipologia di strumento prescelto per la misurazione e, specialmente, dall'utilizzo di telecamere termografiche.

In breve, si proverà a rispondere ai seguenti interrogativi: a) a quali condizioni il trattamento di tali dati da parte del datore di lavoro sia consentito e quale sia la base giuridica; b) se la rilevazione possa essere effettuata direttamente ed autonomamente dal datore di lavoro o si tratti di un accertamento sanitario riservato al medico competente; c) se ed in quali casi l'installazione di termocamere sia soggetta ai limiti previsti a livello europeo e a livello nazionale circa i sistemi di videosorveglianza e di controllo a distanza sull'attività dei lavoratori; d) infine, quali ulteriori limitazioni discendano dall'applicazione dei principi di trasparenza, minimizzazione e sicurezza nel trattamento dei dati.

6.1. La febbre come un dato relativo alla salute: la base giuridica per il trattamento

Rappresentando a tutti gli effetti un trattamento di dati, il rilevamento da parte del datore di lavoro della temperatura dei visitatori e dei dipendenti all'ingresso dei locali aziendali, deve essere reso in conformità ai principi enunciati agli artt. 5 e seguenti del citato GDPR, ossia di legittimità, trasparenza, correttezza, nonché di limitazione della finalità del trattamento e minimizzazione. Inoltre, i dati devono essere trattati in modo sicuro e da non subire alterazioni o accessi non autorizzati.

Occorre, quindi, innanzitutto identificare la base giuridica che legittima il trattamento, che si rinviene nel GDPR agli artt. 6 e 9, relativi rispettivamente alla disciplina generale dei dati personali e a quella dei dati c.d. "particolari".

Nel contesto in esame, come anticipato, i dati personali raccolti dal datore di lavoro rientrano nei-dati definiti dal GDPR "categorie particolari di dati personali". La temperatura corporea rappresenta, infatti, uno di quei dati "relativi alla salute", definiti

[52] A. Ingrao, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, in *Diritto delle Relazioni Industriali*, 3, 2019, 895.

all'art. 4, par. 1, n. 15 come «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute». La definizione contenuta nell'art. 4 deve essere, inoltre, letta in combinato disposto col considerando 35, secondo cui «Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono «[….] le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato [….]».

Trattandosi di dati considerati appunto "particolari", in ragione delle gravi ripercussioni che una loro violazione può comportare sui i diritti degli interessati, vige un generale divieto di trattamento, salvo i casi espressamente elencati nelle lett. da *a)* a *j)* del par. 2 dell'art. 9.

Ciò premesso, tornando all'ipotesi considerata di rilevazione effettuata da parte del latore di lavoro, la misurazione della temperatura corporea si giustifica in base all'art. 9, par. 2, lett. *b)* GDPR[53], che consente il trattamento dei dati particolari quando è reso necessario dall'obbligo imposto in capo al titolare del trattamento[54] di assolvere gli obblighi in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, a condizione che sia: i) «autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri», ii) «vengano fornite adeguate garanzie per i diritti fondamentali e gli interessi dell'interessato».

Invero, in una prima fase dell'emergenza – precedente alla firma del Protocollo condiviso del 14 marzo 2020 – la rilevazione della temperatura corporea negli ambienti di lavoro non rientrava tra le misure previste normativamente o raccomandate dalle parti sociali e, dunque, non poteva dirsi autorizzata dal diritto degli Stati membri o da un contratto collettivo.

Anche il Garante Italiano per la Protezione dei dati personali[55] aveva richiamato i datori di lavoro al rigoroso rispetto della normativa in materia di privacy, invitandoli ad astenersi dall'assumere iniziative autonome che prevedessero la raccolta di dati anche sulla salute di utenti e lavoratori (sia relativi alla presenza di sintomi che relativamente ai loro contatti sociali)[56], di fatto confermando che l'art. 2087 c.c. di per sé non costituisce una base giuridica sufficiente per effettuare il trattamento di tale tipologia di dati in ambito lavorativo, a meno di ulteriori specifiche normative o di apposite previsioni da parte

[53] Cfr. sul punto P. Ricchiuto, *Termoscanner in azienda e privacy: c'è una soluzione*, in *Interlex*,20 marzo 2020.

[54] Definito all'art. 4, par. 1, n. 7 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

[55] Comunicato del Garante del 2 marzo 2020, in *garanteprivacy.it.*

[56] Per un commento Cfr. S. Catelano, *Emergenza "coronavirus" e privacy, Trattamento dei dati personali da parte dei datori di lavoro*, in*Filodiritto.com*, 2 aprile 2020.

della contrattazione collettiva[57].

Attualmente la base giuridica per il trattamento può rinvenirsi nel Protocollo condiviso del 14 marzo 2020[58], nei successivi provvedimenti che ne richiamano l'applicazione, oltre che - in alcuni casi - nei più stringenti provvedimenti regionali, prevedenti l'obbligo e non già solo la facoltà di rilevazione della temperatura del personale[59].

Si tratta, evidentemente, di misure di carattere transitorio, destinate ad applicarsi fino al termine del periodo emergenziale o comunque fino a diversa previsione normativa, con la conseguenza che, una volta terminato lo stato di emergenza[60], tale trattamento non potrà più dirsi lecito.

Altre basi giuridiche per il trattamento dei dati sanitari sono state rinvenute, in base al parere reso dallo European Data Protection Board (d'ora in avanti EDPB)[61] il 19 marzo 2020[62]- che ha dato, quindi, un'interpretazione meno restrittiva di quella offerta dal Garante italiano - nell'art. 9, par. 2, lett. *i*), ossia per necessità di interesse pubblico rilevante nel settore della sanità pubblica, o «[….] per tutelare un interesse vitale dell'interessato o di un'altra persona fisica […]» (art. 9, par. 2, lett. *c*). Quest'ultima ipotesi, sempre in base a quanto sostenuto dallo EDPB, sarebbe ulteriormente supportata dal considerando 46, ove viene esplicitamente prevista la possibilità di trattare i dati personali «[…] per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie [….]».

Per completezza espositiva si sottolinea, infine, che il consenso non sembra un'ipotesi concretamente invocabile nel caso di specie, nonostante rappresenti una delle condizioni legittimanti il trattamento dei dati sanitari ai sensi dell'art. 9, par. 1, lett. *a)*. Come noto, la stessa stipulazione del contratto di lavoro determina «inevitabilmente ed intrinsecamente una rinuncia parziale e consensuale del lavoratore alla tutela assoluta della propria riservatezza ai fini della esecuzione del rapporto di lavoro»[63], dal momento che il dipendente si trova in una posizione contrattuale sbilanciata che difficilmente gli permetterebbe di prestare in maniera davvero libera e incondizionata il consenso[64].

---

[57] «Il richiamo del Garante ad evitare "soluzioni fai da te" è stato interpretato dagli operatori del settore come una sorta di "cartellino rosso" alla rilevazione della temperatura dei dipendenti (con termoscanner o con altri apparecchi) in assenza di una necessaria base giuridica» (ancora P. Ricchiuto, *Termoscanner in azienda e privacy: c'è una soluzione,* cit.).

[58] Il Protocollo condiviso indica, invero, come base giuridica del trattamento l'art. 1, n. 7, lett. *d*) del DPCM 11 marzo 2020.

[59] Ordinanze Reg. Lombardia n. 546 del 13 maggio 2020 e n. 547 del 17 maggio 2020, nonché da ultimo Ordinanza n. 604 del 10 settembre 2020.

[60] 31 gennaio 2021.

[61] L'EDPB è un organismo europeo che si occupa di garantire l'uniforme applicazione delle norme a tutela dei dati personali. Le sue funzioni e poteri sono disciplinati agli artt. 68 ss. del GDPR.

[62] EDPB, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*, 19 marzo 2020.

[63] Cfr. l'intervento di L. Failla, *Il controllo dell'attività dei lavoratori e la tutela della privacy. Internet, posta elettronica e social network*, al convegno AIDP tenutosi a Milano il 9 novembre 2018, in *aidp.it*.

[64] Gruppo di lavoro Articolo 29, Parere n. 2/2017, *Trattamento dei dati sul posto di lavoro*, 3. In tal senso si è espressa recentemente, anche la Suprema Corte italiana: Cass. pen., sez. III, 17 gennaio 2020, n. 1733.

6.2. Il divieto di accertamenti sanitari da parte del datore di lavoro nell'art. 5 St. Lav.

Come anticipato, la speciale natura del dato oggetto del trattamento (la febbre) impone anche alcune riflessioni con riguardo al soggetto che può legittimamente effettuare tale controllo.

In particolare, è necessario domandarsi se la misurazione della temperatura corporea - in quanto in grado di rivelare un dato relativo alla salute del lavoratore, costituisca un "accertamento sanitario" e, cioè un esame che non può essere effettuato direttamente ed autonomamente dal datore di lavoro ai sensi dell'art. 5, c. 1, dello Statuto dei Lavoratori.

Per rispondere alla domanda, occorre approfondire la *ratio* della norma e cosa si intenda per accertamento sanitario.

Da un punto di vista sistematico, come noto, l'art. 5 St. Lav. risulta animato dal medesimo scopo che ha ispirato anche la previsione più ampia contenuta nell'art. 8 St. Lav. che vieta il compimento da parte del datore di lavoro di indagini sulle opinioni politiche, religiose o sindacali del lavoratore (in virtù di una sorta di presunzione di irrilevanza di tali informazioni in ambito lavorativo[65]), nonché su ogni altro fatto non attinente alla valutazione dell'attitudine professionale.

Entrambe le norme mirano, in generale, a limitare forme di controllo da parte del datore di lavoro che non abbiano una stretta attinenza con l'esecuzione della prestazione lavorativa. Ciò che cambia è l'ambito di applicazione del divieto: nel contesto dell'art 5 St. Lav. rientrano le indagini di natura "sanitaria" sulla «idoneità e sulla infermità per malattia o infortunio»; nell'ambito dell'art. 8 St. Lav. ogni altro tipo di accertamento, appunto non "sanitario".

Le considerazioni che precedono ci suggeriscono che il controllo vietato dall'art. 5 è esclusivamente un accertamento di carattere medico, intendendosi per tale quell'insieme di esami, operazioni e in generale attività di carattere diagnostico, effettuato da personale sanitario, volto a verificare lo stato di salute del lavoratore e l'esistenza di una patologia o stato di infermità.

È evidente, tuttavia, che lo stato di salute del lavoratore non possa dirsi totalmente estraneo ad una valutazione circa la sua attitudine professionale, poiché attiene «alla stessa capacità del prestatore di assumere e mantenere la qualità di debitore della prestazione»[66], anche nella misura in cui è suscettibile di incidere sull'idoneità allo svolgimento della specifica mansione lavorativa alla quale lo stesso è adibito. Si è pertanto reputato necessario assicurare tale valutazione, ma sottraendo tale potere di verifica al datore di lavoro, rimettendola rispettivamente ai servizi ispettivi INPS ed INAIL[67]

---

[65] I. Bresciani, *Le forme di controllo nello Statuto dei lavoratori,* cit.

[66] P. Chieco, *Privacy e Lavoro*, *La disciplina del trattamento di dati personali del lavoratore*, Bari, 2000, 96.

[67] Il controllo può essere effettuato solo attraverso i servizi ispettivi degli istituti previdenziali, i quali sono tenuti a disporlo quando il datore lo richieda, per il tramite dei medici dei servizi sanitari indicati dalle regioni (art. 2, d.l. 30 dicembre 1979, n. 663, convertito in l. 29 febbraio 1980, n. 33) o ricorrendo al personale medico iscritto nelle liste speciali tenute dall'INPS (art. 5, d.l. 12 settembre 1983, n. 463, convertito in l. 11 novembre 1983, n. 638).

per ciò che attiene allo stato di infermità o di infortunio, nonché alla figura del medico competente, per l'attività di sorveglianza sanitaria volta a verificare la specifica idoneità alla mansione[68]. Da qui l'importanza di questa disposizione in grado di: i) evitare che il datore di lavoro possa venire a conoscenza di dati relativi alla sfera più "intima" del lavoratore e che quest'ultimo ha interesse che rimangano riservati (almeno nella misura in cui non incidono sull'idoneità allo svolgimento della prestazione lavorativa); ii) scongiurare che gli esiti di tali accertamenti (appunto laddove evidenzino una particolare patologia o, ad esempio, uno stato di gravidanza) sfocino in un atteggiamento discriminatorio da parte del datore di lavoro; iii) infine, sottrarre al datore di lavoro (creditore della prestazione) tale potere di controllo in modo da preservare «l'obiettività dell'accertamento medico»[69].

Alla luce di quanto precede, è chiaro che il controllo vietato dall'art. 5 St. Lav. è solo quello svolto direttamente dal datore di lavoro, autonomamente o per il tramite di proprio personale[70].

Premessi lo scopo della disposizione e la nozione di accertamento sanitario, si ritiene di poter escludere che l'operazione della mera rilevazione della temperatura corporea dei dipendenti rientri nel divieto in parola. Infatti, tale rilevazione non consente di valutare l'effettivo stato di salute del lavoratore, né tanto meno di accertare la presenza o meno di una specifica patologia. Ciò che l'operazione è in grado di rilevare è esclusivamente la presenza di un sintomo, non immediatamente riconducibile ad un particolare stato di infermità.

Non trattandosi strettamente di indagini "mediche", sembra quindi che si possa escludere che sia indispensabile che la rilevazione della temperatura sia effettuata dal medico competente dell'impresa, ben potendo essere individuato un addetto o un operatore deputato a tale controllo.

Al contempo, per le medesime ragioni, non risulta strettamente necessario che il lavoratore vi adibisca personale medico o infermieristico, non essendo necessarie particolari specializzazioni o competenze tecniche. Al contrario, si rischierebbe di trasformare tale procedura in un accertamento "medico/sanitario", effettivamente vietato, ove tale rilevazione "sconfinasse" in un controllo più invasivo.

Le considerazioni sopra esposte offrono, infine, un ulteriore spunto di riflessione, relativamente alla questione – anch'essa particolarmente dibattuta – circa la legittimità della richiesta del datore ai propri dipendenti di sottoporsi ai test sierologici per individuare nel sangue la presenza di anticorpi al virus. In tal caso, trattandosi a tutti gli effetti di un'attività diagnostica, non si può che pervenire ad una soluzione diametralmente opposta. Al riguardo, anche il Garante italiano privacy71 ha chiarito che il datore di lavoro può richiedere l'effettuazione di test sierologici ai propri dipendenti solo qualora questa sia disposta dal medico competente e, in ogni caso, nel rispetto delle indicazioni

---

[68] Art. 41, d.lgs. 81/2008.

[69] Cfr. I, Bresciani, *Le forme di controllo nello Statuto dei lavoratori,* cit.

[70] Sono estranei a tale limitazione appunto solo gli accertamenti svolti dal medico competente (anche quando dipendente) nell'ambito dell'attività di "sorveglianza sanitaria" *ex* art. 41, d.lgs. 81/2008.

[71] V. comunicato del 14 maggio 2020. Sul punto cfr. anche le Faq del Garante, *Trattamento dei dati nel contesto lavorativo pubblico e privato nell'ambito dell'emergenza sanitaria*, in *garanteprivacy.it*.

fornite dalle autorità sanitarie, anche in merito all'affidabilità e all'appropriatezza di tali test. Solo il medico competente, infatti, può stabilire la necessità di particolari esami clinici e biologici e suggerire l'adozione di mezzi diagnostici, qualora ritenuti utili al fine del contenimento della diffusione del virus e della salute dei lavoratori[72].

6.3. (*segue*) La videosorveglianza nei luoghi di lavoro nel contesto europeo

A questo punto, risulta necessario soffermarsi sulle implicazioni giuridiche che discendono dal ricorso alla termografia ad infrarossi. Come visto nel par. 4, nella maggior parte dei casi le termocamere sono a tutti gli effetti integrate in veri e propri sistemi di videosorveglianza, prevedendo la possibilità di un controllo da remoto. Come noto, la pervasività di tale forme di sorveglianza ha comportato la previsione di limiti a livello europeo e nazionale.

Pertanto occorre verificare quali condizioni devono essere assicurate in caso di installazione di impianti di questo tipo poiché, se non adottati con le adeguate garanzie, violano il diritto alla privacy dei dipendenti e possono condurre ad un'ingiustificata e non proporzionata sorveglianza dei movimenti e delle attività sul luogo di lavoro.

A livello europeo, il controllo a distanza dei lavoratori è, da tempo, un tema "caldo", dal momento che – anche al di fuori dello specifico caso trattato – le nuove tecnologie facilitano la possibilità per i datori di lavoro di fare ricorso a misure di sorveglianza dei propri dipendenti, sia attraverso l'utilizzo di telecamere sempre più piccole e sofisticate che permettono di captare immagini con una risoluzione più alta e sono facilmente occultabili sul luogo di lavoro, sia attraverso l'installazione di sistemi di localizzazione (attraverso il tracciamento Wi-fi o Bluetooth), o l'intercettazione delle comunicazioni.

In risposta alle crescenti preoccupazioni circa i rischi connessi all'utilizzo di videocamere sui soggetti interessati, il Gruppo di lavoro Articolo 29[73] si è espresso con un documento che analizza le diverse questioni giuridiche sul tema e fornisce strumenti pratici per guidare le attività dei diversi titolari del trattamento[74]. In particolare, la consapevolezza di essere sorvegliati, ricorda l'organismo consultivo europeo in materia di privacy, potrebbe influenzare il modo in cui i lavoratori svolgono le proprie mansioni e di fatto congelare alcuni dei loro diritti - come ad esempio quello di organizzare riunioni, comunicare in maniera confidenziale - cosi come d'altronde avviene già su scala più ampia nel caso di sorveglianza dei cittadini da parte dei governi. Il monitoraggio costante, posto in essere tramite la captazione di immagini o di conversazioni, può

[72] Cfr. par. 12 del Protocollo condiviso tra il Governo e le Parti sociali aggiornato il 24 aprile 2020.

[73] Il cosiddetto Gruppo di lavoro Articolo 29 è un organismo consultivo e indipendente, istituito dall'art. 29 della direttiva 95/46 del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il Gruppo è composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.

[74] Gruppo di lavoro Articolo 29, Parere n. 2/2017 *Trattamento dei dati sul posto di lavoro,* cit.

inoltre condurre ad una vera profilazione dei dipendenti[75].
Il Gruppo di lavoro Articolo 29 ha infine esortato i datori di lavoro ad evitare, per quanto possibile, il ricorso a tecnologie che permettono il riconoscimento facciale[76].
Sempre nel contesto europeo, l'EDPB, l'organismo europeo, già richiamato nei paragrafi precedenti, che ha ora sostituito il Gruppo di lavoro Articolo 29, ha adottato lo scorso gennaio le linee guida relative, invece, al trattamento generale dei dati attraverso videosorveglianza[77]. In particolare, nel documento vengono invitati i titolari del trattamento a ricorrere con particolare cautela alle telecamere di sorveglianza, potendo queste rappresentare strumenti molti invasivi della vita privata delle persone, e potendone addirittura condizionare comportamenti e abitudini. Il ricorso alla videosorveglianza deve pertanto avvenire sempre nel rigoroso rispetto dei principi di legittimità, necessità, proporzionalità, trasparenza e minimizzazione. Invero, il titolare del trattamento, prima di installare le telecamere, deve verificare che la misura sia adeguata e necessaria alle finalità perseguite[78]. Il principio di necessità riguarda anche le modalità e la durata di conservazione dei dati.
In base al principio di trasparenza, poi, è necessario informare i soggetti interessati, attraverso l'affissione di informative privacy ben visibili, della presenza di videocamere. Queste devono essere posizionate in zone ben precise e funzionali alle finalità perseguite. Il titolare del trattamento, inoltre, deve predisporre le misure di sicurezza idonee a prevenire l'accesso non autorizzato ai dati dei soggetti interessati, soprattutto da parte di soggetti estranei all'organizzazione aziendale.
Per quanto riguarda nello specifico l'installazione di misure di sorveglianza sul luogo di lavoro, il trattamento dei dati può essere giustificato da un interesse legittimo del titolare del trattamento ai sensi dell'art. 6, par. 1, lett. *f)*, rappresentato, ad esempio, dalla necessità di per prevenire furti o danneggiamenti.
A livello giurisprudenziale, sul tema delle misure di sorveglianza occulte adottate dai datori di lavoro nei confronti dei lavoratori, si è pronunciata recentemente anche la Corte europea dei diritti umani (da qui in prosieguo, per brevità, EDU) nel caso *Lopez Ribalda e altri c. Spagna.*[79] In particolare, i ricorrenti denunciavano la violazione dell'art. 8 CEDU - che tutela nella Convenzione la vita privata e familiare - essendo stati ripresi, a loro insaputa, da telecamere nascoste installate dal datore di lavoro. Le registrazioni, che mostravano i dipendenti nell'atto di compiere dei furti, avevano poi condotto al loro licenziamento. Orbene, la Corte EDU in Grande Camera ha stabilito che l'adozione di telecamere occulte deve ritenersi del tutto eccezionale e soggetta a determinati requisiti[80] e che, in ogni caso, le misure di limitazione al diritto alla privacy devono

[75] Ivi, 10. Cfr. sul tema F. Domenici, *Profilazione illecita dei dipendenti, lo scandalo H&M: quali insegnamenti per tutte le aziende*, in *cybersecurity360.it,* 2 ottobre 2020.

[76] Ivi, 19.

[77] EDPB, *Linee guida n. 3/2019 sulla videosorveglianza*, versione adottata dopo la consultazione pubblica, 29 gennaio 2020.

[78] Ivi, 10.

[79] CEDU (GC), *Bărbulescu c. Romania*, ric. 61496/08 (2017); CEDU (GC), *López Ribalda e altri c. Spagna*, ricc. 1874/12 e 8567/13 (2019).

[80] La Corte europea dei diritti umani ha stabilito infatti che nel caso di specie il datore di lavoro fosse legittimato ad installare telecamere nascoste per controllare i dipendenti a) solo nel caso di fondati e

avvenire nel rispetto del principio di proporzionalità. Nel caso di specie, l'interesse legittimo del datore di lavoro che giustificava il ricorso a telecamere occulte poteva rinvenirsi nella tutela della proprietà societaria, nella sicurezza e la salute dei lavoratori o nella prevenzione di condotte illecite[81].

In conclusione, sulla base delle opinioni espresse dai diversi organi competenti in materia di privacy a livello europeo, cosi come esposte nel presente paragrafo, il datore di lavoro può ritenersi legittimato ad installare misure di videosorveglianza, a condizione che le suddette misure siano sempre di natura eccezionale e siano giustificate da validi interessi legittimi, nonché dai principi sanciti dal GDPR e della CEDU.

6.4. (*Segue*): la videosorveglianza nei luoghi di lavoro nell'art. 4 St. Lav.

Come anticipato, i principi stabiliti dal GDPR e le "linee guida" europee devono essere lette congiuntamente con la normativa nazionale che disciplina, all'art. 4 St. Lav., l'utilizzo in ambito lavorativo degli impianti audiovisivi o strumenti dai quali derivi «anche la possibilità di controllo a distanza sull'attività dei lavoratori».

Occorre premettere che il testo dell'articolo in parola è stato in parte riscritto dall'art. 23 d.lgs. 151/2015[82] e dall'art. 5, c. 2, d. lgs. 185/2016[83]. Le modifiche sono state dichiaratamente ispirate dall'esigenza di adeguare la previgente disciplina dei controlli a distanza all'evoluzione tecnologica, preservando comunque le garanzie della dignità e riservatezza del lavoratore[84].

Come noto, rispetto alla formulazione previgente è, anzitutto, venuto meno il divieto testuale contenuto al vecchio primo comma, di utilizzare impianti audiovisivi ed altri strumenti di lavoro per finalità di controlli a distanza dell'attività dei lavoratori. Viene, tuttavia, ribadito che il datore di lavoro non può installare impianti audiovisivi o altri strumenti che abbiano precipuamente la finalità di sorvegliare l'esecuzione della prestazione lavorativa o il compimento di illeciti disciplinari[85]. Infatti, possono essere installati solo quando il controllo a distanza risulti un "effetto collaterale" ed "acci-

ragionevoli sospetti di furti commessi ai danni del patrimonio aziendale; b) l'area oggetto di ripresa era circoscritta; c) le videocamere funzionavano per un periodo temporale limitato, e, il loro uso era limitato a provare i furti commessi e, infine, d) non era possibile ricorrere a mezzi alternativi. Cfr. a riguardo A. Ciriello - F. Ariante, *Videosorveglianza "occulta" sul luogo di lavoro: il caso López Ribalda e altri c. Spagna e la giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *Lavoro Diritti Europa*, 3, 2019.

81 Cfr. F. Toffoletto, *La Cedu apre alle telecamere nascoste sul luogo di lavoro*, in *Guida al Lavoro*, 43, 1 novembre 2019, 23-25.

82 Pubblicato in *G.U.R.I.* n. 221 del 23 settembre 2015 - Suppl. Ordinario n. 53.

83 Pubblicato in *G.U.R.I.* n. 235 del 7 ottobre 2016.

84 V. legge delega (l. 10 dicembre 2014, n. 183, in *G.U.R.I.* n. 290 del 15 dicembre 2014), all'art. 1, c. 7, lett. *f*). Per un commento alla riforma V.G. Vidiri, *I controlli difensivi: ovvero il bilanciamento degli interessi nel "nuovo" art. 4 statuto dei lavoratori*, in *Massimario della giurisprudenza del lavoro*, 11, 2017, 731 ss.; L. Foglia, *Il controllo a distanza sull'attività del lavoratore: dallo Statuto dei lavoratori al Jobs act e ritorno*, in *Massimario della giurisprudenza del lavoro*, 10, 2016, 651 ss.; M.T. Goffredo - V. Meleca, *Jobs Act e nuovi controlli a distanza*, in *Diritto & Pratica del Lavoro*, 31, 2016, 1894 ss.

85 Cfr., *ex multis*, L. Foglia, *Il controllo a distanza sull'attività del lavoratore,* cit.

dentale" della finalità "lecite" elencate dalla norma. In altre parole, la possibilità di un controllo a distanza è ammessa solo sotto forma di controllo «preterintenzionale»[86], conseguente, cioè , ad una funzione accessoria ed ineliminabile dell'apparecchiatura.
Tra le finalità per cui l'installazione di apparecchi audiovisivi e altri strumenti potenzialmente invasivi è consentita, il nuovo primo comma contempla – come già la precedente versione – la sicurezza sul lavoro[87]. La liceità dell'installazione discende comunque dalla stipula da parte del datore di lavoro di un apposito accordo sindacale con le rappresentanze sindacali aziendali o unitarie, con lo scopo di regolamentarne le modalità di utilizzo. O, nel caso in cui tale accordo non possa essere raggiunto, il datore di lavoro deve ottenere la previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro. In altre parole, anche laddove tali strumenti siano installati al fine di garantire la sicurezza sul lavoro, tale finalità è solo «uno dei fattori che, in linea astratta, rendono possibile l'attivazione di tale tipo di impianti, salva, tuttavia, la realizzazione anche delle successive forme di garanzia a tutela dei lavoratori previste dalle norme precettive dianzi ricordate»[88].
Fanno eccezione alle limitazioni ed alle procedure sopra descritte – anche laddove possa derivare potenzialmente un controllo a distanza del dipendente – gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa (individuati tipicamente nei seguenti dispositivi: computer, telefoni, *tablet*, eventualmente anche ove assegnati a più lavoratori ma con accesso personalizzato per ciascuno, ma anche carte di credito, telepass) e gli strumenti di registrazione degli accessi e delle presenze (essenzialmente i c.d. lettori *badge*)[89].
Infine, come accennato *supra*, l'art. 4 per la prima volta ha richiamato espressamente al rispetto della normativa in materia di protezione dei dati personali[90].

---

[86] Espressione di U. Romagnoli, *sub art. 4*, in G. Ghezzi - F. Mancini - L. Montuschi - U. Romagnoli, *Statuto dei diritti dei lavoratori*, Bologna, 1979, 28 ss.

[87] Rispetto alla precedente versione, invece, il testo è stato novellato includendo tra le finalità per cui l'istallazione risulta consentita le esigenze di tutela del patrimonio aziendale. Sul punto la riforma ha, da un lato, recuperato la categoria di elaborazione giurisprudenziale dei c.d. "controlli difensivi", ossia i «controlli diretti ad accertare condotte illecite del lavoratore» (cui ha dato il "via" la storica sentenza della Cass. Civ., sez. lav., 3 aprile 2002, n. 4746) legittimando espressamente l'utilizzo dei sistemi audiovisivi anche per la «tutela del patrimonio aziendale», dall'altro, l'ha però ricondotta, appunto, entro lo schema dell'art. 4 St. Lav. Di fatto, «producendo il risultato paradossale che in talune circostanze la possibilità di un datore di lavoro di agire a tutela del proprio patrimonio aziendale avrebbe potuto essere più ampio prima della novella (ancorché il diritto non fosse espressamente riconosciuto)» (L. Saglione, *Il controllo a distanza dei lavoratori alla prova della Corte Europea dei Diritti Umani*, in *Guida al Lavoro*, 50, 2018, 27 ss.).

[88] Cfr. Cass. pen., sez. III, 17 dicembre 2019, n. 50919. Per completezza è importante tenere presente che l'accordo sindacale o l'autorizzazione amministrativa devono precedere l'installazione dell'impianto, non solo la messa in funzione (Cass. pen., sez. III, 30 gennaio 2014, n. 4331), per cui se l'impianto è installato prima dell'accordo si è in violazione delle norme (art. 38, l. 300/1970), anche nel caso in cui i dipendenti siano stati correttamente informati. In tal senso anche la più recente Cass. pen., sez. III, 17 gennaio 2020, n. 1733.

[89] Tale semplificazione si giustifica in quanto si tratta di strumenti che sono destinati a «svolgere una essenziale funzione di ammodernamento ed efficientamento dell'organizzazione e dell'attività produttiva» (L. Foglia *Il controllo a distanza sull'attività del lavoratore,* cit.).

[90] Ossia, tra l'altro, la condizione che i lavoratori siano informati adeguatamente circa le modalità con le quali devono essere utilizzati gli strumenti concessi in dotazione (ad esempio, se destinati ad un uso privato o lavorativo oppure promiscuo, se il loro utilizzo è tollerato o vietato all'interno dell'impresa), le modalità con le quali verrà esercitato il controllo (indicazione dei nominativi dei soggetti preposti

In base a quanto esposto, dunque, si deve ritenere che l'obiettivo perseguito attraverso l'installazione di termocamere in questa fase di emergenza rientri tra le finalità consentite dall'art. 4 St. Lav.; l'impiego risulta infatti giustificato a fronte di esigenze (peraltro straordinarie) di tutela della salute e della sicurezza dei dipendenti. Al contempo – nei casi in cui appunto il dispositivo sia inserito in sistemi di videosorveglianza o collegato a monitor esterni – esattamente come i tradizionali strumenti audiovisivi non può escludersi a priori che le riprese possano accidentalmente trasformarsi in una forma di controllo a distanza.
Si deve ritenere pertanto che, in tali casi, l'art. 4 St. lav. obblighi il datore di lavoro, prima di munirsi e di utilizzare tali dispositivi, a concludere un apposito accordo sindacale con le rappresentanze in azienda (se presenti e se collaborative) o viceversa ad ottenere l'autorizzazione dell'ITL, oltre che ovviamente a rispettare i principi sanciti dalla regolamentazione europea a protezione dei dati, come richiamata anche dal c. 3° della disposizione.

6.5. I principi di trasparenza, proporzionalità, necessità, minimizzazione e sicurezza nel trattamento dei dati

Fermo quanto precede, il datore di lavoro, nell'adozione di misure che interferiscono con il diritto alla privacy dei lavoratori - rappresentate in questo caso dall'installazione di termocamere – deve sempre agire nel rispetto dei principi di trasparenza, proporzionalità, necessità, minimizzazione e sicurezza nel trattamento dei dati.
In primo luogo, in ossequio al principio di trasparenza del trattamento, i soggetti interessati (in questo caso i lavoratori dipendenti) devono ricevere adeguate informazioni circa le modalità del trattamento dei loro dati, compreso il periodo di conservazione e le finalità del trattamento. L'informativa sul trattamento dei dati personali deve essere facilmente accessibile e fornita in un linguaggio chiaro e preciso[91] . Affinché l'informazione sia trasparente, occorre che sia individuata e, ovviamente, comunicata a tutti gli interessati, anche in forma orale[92], la specifica finalità per la quale i dati vengono raccolti e trattati. È noto che, ai sensi dell'art. 5, par. 1, lett. *b*), i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità [...]. In questo caso la finalità è esclusivamente il contrasto al contagio da COVID-19. Al riguardo, il Garante italiano suggerisce, infatti, una volta fornita idonea informativa, di raccogliere solo i dati necessari (principio di necessità), adeguati e pertinenti rispetto alla prevenzione del contagio da COVID-19. Per la stessa ragione, «i datori di lavoro devono invece astenersi dal raccogliere, a priori e in modo sistematico e generalizzato, anche attraverso specifiche richieste al singolo

ai controlli; la periodicità o occasionalità; il tipo di programmi informatici utilizzati), specificando le informazioni che sono oggetto di temporanea memorizzazione, la durata della conservazione dei dati etc.).

[91] EDPB, *Linee guida n. 3/2019 sulla videosorveglianza*, cit., 26-27.

[92] Al riguardo, vale la pena sottolineare che alla nota n. 1, p. 6, del Protocollo condiviso è espressamente ammesso che l'informativa possa essere data anche oralmente.

lavoratore o indagini non consentite, informazioni sulla presenza di eventuali sintomi influenzali del lavoratore e dei suoi contatti più stretti o comunque rientranti nella sfera extra lavorativa»[93].

Il trattamento deve avvenire, inoltre, nel rispetto dei principi di proporzionalità e di minimizzazione. Questo comporta, da un lato, l'obbligo in capo al titolare del trattamento di raccogliere solo il dato relativo alla temperatura corporea (principio di minimizzazione) e dall'altro lato di favorire le misure meno intrusive per il raggiungimento delle suddette finalità (principio di proporzionalità), effettuando un giudizio di bilanciamento tra l'obiettivo di prevenzione dalla diffusione del COVID-19 e i rischi per i diritti dei soggetti interessati.

In quest'ottica, quindi, dovranno essere prescelti modelli che rilevino esclusivamente il dato relativo alla temperatura e identifichino l'interessato solo per il tempo necessario a garantirne l'accesso agli stabilimenti aziendali o comunque che limitino ogni altra possibilità di intrusione nella sfera personale del lavoratore.

In generale, è consentita la registrazione dei dati relativi alla temperatura corporea solo nel caso di superamento della soglia stabilita dalla legge e quando si rende, quindi, necessario documentare le ragioni che hanno impedito l'accesso al luogo di lavoro[94]. In quest'ultimo caso, però, per stabilire la durata di conservazione dei dati, occorre fare riferimento al termine dello stato d'emergenza[95].

È, infine, importante adottare misure di sicurezza adeguate, che consentano di assicurare la confidenzialità dei dati, soprattutto al fine di impedire che essi vengano rivelati e trasmessi a parti terze non autorizzate[96] (art. 5, par. 1, lett. *f*), GDPR; art. 32 GDPR). In particolare, sotto il profilo organizzativo, è necessario individuare i soggetti preposti al trattamento dei dati e fornire loro le istruzioni necessarie.

6.6. (*segue*) La valutazione d'impatto sulla protezione dei dati e il registro delle attività di trattamento

Come già precedentemente esposto, non tutte le termocamere presentano lo stesso livello di intrusività.

Pertanto, il datore di lavoro dovrà verificare la compatibilità tra le specifiche caratteristiche dello strumento che intende adoperare con i principi di minimizzazione, proporzionalità e sicurezza sopra richiamati, orientando la propria scelta verso un certo tipo di modello, a discapito di un altro, sulla base della c.d. valutazione di impatto sulla tutela dei dati prevista all'art. 35 GDPR.

Infatti, come tra l'altro evidenziato dal Gruppo di lavoro Articolo 29, la valutazione

[93] *Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati*, comunicato del 2 marzo 2020, in *garanteprivacy.it*.

[94] Garante della privacy, *Trattamento dei dati nel contesto lavorativo pubblico e privato nell'ambito dell'emergenza sanitaria*, cit. Cfr. anche il Protocollo condiviso, nota 1, 5.

[95] *Ibidem*. Cfr. sempre Protocollo condiviso, nota 1, 5.

[96] EDPB, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*, adottata il 19 marzo 2020, 2. In base al Protocollo condiviso la trasmissione dei dati può avvenire solo su richiesta delle autorità sanitarie competenti, per fini connessi alla gestione del rischio sanitario.

d'impatto è uno strumento volto a valutare la necessità e la proporzionalità del trattamento e costituisce un elemento importante per la c.d. *accountability*. La mancata effettuazione della Valutazione d'impatto sulla protezione dei dati, nelle ipotesi in cui questa è necessaria, può condurre ad amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente[97].
Ai sensi dall'art. 35, il titolare del trattamento deve procedere alla valutazione d'impatto ogni qualvolta si avvalga, per la raccolta e il trattamento dei dati, di nuove tecnologie che possono comportare un rischio elevato per i diritti e le libertà delle persone fisiche[98]. Inoltre, l'art. 35 GDPR elenca diverse ipotesi in cui la valutazione d'impatto è sempre richiesta, tra cui vi rientra «b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, [….]»[99] - che include, appunto, i dati sanitari oggetto della presente analisi.
Orbene, sulla base dell'analisi precedentemente svolta, è pacifico ritenere che i diversi modelli termocamere rientrino nella categoria di nuove tecnologie che comportano di fatto un rischio elevato per i soggetti interessati.
In questa valutazione, il titolare del trattamento deve tenere in considerazione, tra le altre cose, i rischi concreti in capo ai soggetti interessati e le modalità di trattamento meno lesive per raggiungere le finalità di contrasto alla diffusione del COVID-19 sul luogo di lavoro[100]. Il datore di lavoro, infatti, in virtù del principio di proporzionalità, deve adottare, qualora possibile, le misure considerate meno invasive, al fine di ridurre al minimo i rischi per i diritti dei soggetti interessati e dimostrare, allo stesso, di agire in conformità al regolamento (art. 35, par. 7).
La valutazione pertanto deve contenere, nello specifico, a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento[101].

---

[97] Art. 83 GDPR. Il GDPR non prevede un obbligo di pubblicare la valutazione d'impatto, ma il Gruppo di lavoro Articolo 29 consiglia, quanto meno, di pubblicarne alcune parti. Questo aiuterebbe infatti a rinforzare la fiducia nei confronti del titolare del trattamento e a dimostrare di operare in conformità ai principi di *accountability* e traparenza il titolare del trattamento deve inoltre indicare i ruoli e le responsabilità dei soggetti coinvolti nel trattamento (Gruppo di lavoro Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati,* 4 aprile 2017, WP248, 18).

[98] Art. 35, par. 1, GDPR.

[99] Art. 35, par. 3, lett. *b)*, GDPR.

[100] Previsto anche dal considerando 90: «In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento».

[101] Inoltre, ai sensi del par. 4 dell'art. 35, le autorità di sorveglianza devono redigere e pubblicare una lista delle attività che necessitano la valutazione d'impatto e comunicarla all'EDPB. Per quanto riguarda la disciplina italiana, il Garante italiano privacy ha pubblicato l'elenco nel 2018, ove risultano, tra le attività elencate necessitanti di una valutazione d'impatto, quelle relative alla raccolta di categorie particolari di dati ai sensi dell'art. 9 e le attività di sistematiche di raccolta di dati biometrici.

Alla luce di quanto esposto, si deve ritenere che la scelta del titolare del trattamento deve orientarsi, pertanto, verso l'adozione di modelli di termocamere che, a parità di efficacia nel raggiungimento della finalità di garantire la sicurezza sul luogo di lavoro attraverso il preventivo controllo della temperatura corporea, sono ritenute, in seguito alla valutazione d'impatto sulla protezione dei dati, il meno intrusive possibili.
A livello temporale, la valutazione d'impatto deve essere effettuata prima che inizi il trattamento dei dati. Questo criterio è, d'altronde, in coerenza con i principi *privacy by design* e *privacy by default* enunciati all'art. 25 e al considerando 78 GDPR[102].
Infine, vige in capo al titolare del trattamento un obbligo di predisporre anche il cosiddetto Registro delle attività di trattamento previsto all'art. 30 GDPR. In base alla suddetta norma, il titolare del trattamento deve conservare il registro – contenente tutte le informazioni indicate all'art. 30 (nome del titolare del trattamento, finalità del trattamento, categorie di dati raccolti ecc.) – nel caso in cui il trattamento riguardi appunto «categorie particolari di dati di cui all'art. 9, paragrafo 1 […]».

7. Conclusioni

In base alle considerazioni svolte nei paragrafi precedenti, risulta che il datore di lavoro sia autorizzato (in taluni casi persino obbligato) ad effettuare la rilevazione della temperatura corporea dei dipendenti all'ingresso dei locali aziendali.
La base giuridica del trattamento può rinvenirsi, come illustrato, nell'art. 9 par. 2, lett. *b*), GDPR, oltre che nelle lett. *c*) e *i*) della medesima disposizione. Ai sensi della citata lett. *b*), a livello nazionale vengono in rilievo, più precisamente, il Protocollo condiviso del 14 marzo 2020 come successivamente modificato in data 24 aprile 2020[103], nonché i più stringenti provvedimenti assunti su base regionale[104].
Tale facoltà (o obbligo) sarà comunque limitata(o) alla sola fase di emergenza.
Come chiarito, non trattandosi di un accertamento "sanitario" ai sensi dell'art. 5 St. Lav., la rilevazione può e potrà essere effettuata autonomamente dal datore di lavoro, senza l'intervento del medico competente della società.
L'art. 2087 c.c. suggerisce di procedere a tale rilevazione con strumenti che evitino il contatto diretto con la "pelle", consentano una celere misurazione e prevengano la formazione di assembramenti. In questa prospettiva, è evidente che il ricorso alla termografia risulti più sicuro dell'utilizzo dei classici termometri a contatto (anche digitali).
Al contempo, se da un lato non sembrano porre particolari problemi i termometri ad infrarossi – dotati solo di un display, pensati per l'utilizzo manuale da parte di un operatore e in generale privi della possibilità di registrazione del dato – viceversa l'impiego di termocamere impone particolari riflessioni. Infatti, data l'estrema variabilità dei modelli in commercio (anche molto invasivi) non è indifferente il tipo di strumento

[102] Gruppo di lavoro Articolo 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati*, cit., 14.

[103] Il Protocollo condiviso indica, invero, come base giuridica del trattamento l'art. 1 n. 7, lett. *d*) del DPCM 11 marzo 2020.

[104] Ordinanze Reg. Lombardia n. 546 del 13 maggio 2020 e n. 547 del 17 maggio 2020.

adoperato. In tutti i casi, per il principio di minimizzazione già richiamato, il modello prescelto può rilevare esclusivamente il dato relativo alla temperatura corporea. Non dovrebbero dunque essere previste funzioni accessorie, di identificazione o riconoscimento facciale, né di collegamento con il badge o altri strumenti di apertura automatica di porte e cancelli, poiché consentono di rilevare ulteriori dati.

Inoltre, per il principio di proporzionalità, ove possibile è certamente consigliabile prediligere telecamere prive di collegamenti a distanza, fermo restando che, ove viceversa siano ravvisabili specifiche esigenze organizzative che impongano il ricorso ad un modello di termocamera collegato ad un monitor esterno ed inserito in un sistema di videosorveglianza, sia imprescindibile il preventivo accordo sindacale ovvero l'autorizzazione da parte dell'Istituto territoriale del lavoro.

Per il principio di trasparenza, deve essere fornita ai dipendenti apposita informativa (come si è visto, senza particolari requisiti di forma), recante le finalità, la durata del trattamento, le misure di sicurezza all'uopo predisposte.

Per quanto riguarda la durata di conservazione, conformemente a quanto previsto dal protocollo condiviso del 14 marzo 2020, è consentita la registrazione del dato esclusivamente quando necessaria per documentare l'impossibilità di consentire l'accesso ai locali aziendali e solo limitatamente al periodo dell'emergenza. L'installazione di tali strumenti deve essere, inoltre, preceduta da un'accurata valutazione d'impatto sui dati personali, tenendo conto delle implicazioni giuridiche e dei rischi per i lavoratori interessati.

In conclusione, si può ritenere che il ricorso a termocamere rappresenti ad oggi una valida misura per contenere la diffusione del COVID-19 sui luoghi di lavoro, a condizione però che siano rispettati tutti i precetti enunciati sia a livello nazionale che europeo in materia di privacy e controllo sull'attività lavorativa.

Il tema trattato offre, infatti, anche lo spunto per un'ultima considerazione di carattere generale: nel caso di impiego di mezzi tecnologici, l'applicazione dalla normativa non può prescindere da una valutazione delle specificità tecniche. Si impone, cioè, al giurista di approfondire le peculiarità dello strumento in concreto prescelto ed adoperato dal datore di lavoro al fine di regolamentarne adeguatamente l'utilizzo.

Note a sentenza

Sezione Europa

Discriminazione razziale e propaganda, obblighi di valutazione del contesto e critica politica tra diritto interno e diritto internazionale

Marina Castellaneta

Corte di Cassazione, sez. I penale, 16 gennaio 2020, n. 1602
Corte di Cassazione, sez. V penale, 30 luglio 2019, n. 34815

Nel decidere la condanna in base alla legge n. 654/1975 per propaganda di idee discriminatorie e per istigazione all'odio razziale nei confronti di migranti, i giudici nazionali devono fornire una motivazione volta a ricostruire il contesto nel quale le dichiarazioni sono rese. In questo modo, è infatti assicurato un giusto bilanciamento tra libertà di espressione e divieto di discriminazione.
Un uomo politico, condannato per diffamazione aggravata dalla finalità di discriminazione etnica e razziale, che divulga attraverso una radio nazionale frasi contro un ministro per ragioni legate al colore della pelle o alla razza non può godere della scriminante del diritto di critica politica.

Sommario

Keywords

discriminazione razziale – propaganda - libertà di espressione Convenzione ONU sull'eliminazione di ogni forma di discriminazione razziale - corte europea dei diritti dell'uomo.

1. L'applicazione della Convenzione sull'eliminazione di ogni forma di discriminazione razziale in due pronunce della Corte di Cassazione

La proliferazione, in ogni parte del mondo, di manifestazioni di odio razziale e di discriminazioni nei confronti di determinati gruppi etnici o in generale di migranti, ha condotto, da un lato, al maggiore impegno nell'individuazione di strumenti, anche legislativi, per fronteggiare questi fenomeni e, dall'altro lato, a interventi dei giudici nazionali che sempre più di frequente si rivolgono al diritto internazionale per la corretta interpretazione delle norme interne che spesso sono adottate per assicurare l'attuazione effettiva di obblighi assunti sul piano internazionale.

In questa direzione appare interessante considerare due pronunce della Corte di Cassazione che permettono di svolgere alcune considerazioni sulla normativa italiana sui reati d'odio, con particolare riferimento al caso della propaganda discriminatoria e sull'attuazione del diritto internazionale sul piano interno con riguardo agli elementi necessari per accertare la commissione di un reato legato alla propaganda della discriminazione razziale. Si tratta, in particolare, della sentenza della I sezione penale, n. 1602/20, depositata il 16 gennaio 2020, relativa a un caso di propaganda di idee fondate sull'odio e della pronuncia n. 34815 resa dalla V sezione penale il 30 luglio 2019 che ha al centro un caso di diffamazione aggravata dalla finalità di discriminazione etnica e razziale che – come precisato dalla Suprema Corte – ha la stessa offensività del reato di propaganda razziale, permettendo, così, talune valutazioni d'insieme partendo da entrambe le pronunce.

Con la prima delle indicate sentenze, la Suprema Corte ha stabilito che le espressioni violente che invocano in modo cruento e plateale l'applicazione della pena capitale, riportate in alcuni manifesti, non sono *ex se* attività discriminatoria e il giudice di merito è tenuto a motivare la condanna degli autori di dette espressioni non limitandosi a indicare il manifesto, ma piuttosto procedendo a una ricostruzione del contesto, passaggio necessario per provare il contenuto discriminatorio di un messaggio e giustificare la condanna penale. Ed invero, per la Cassazione, la pronuncia della Corte di appello di Milano, che aveva condannato gli imputati per istigazione all'odio razziale in base alla legge 13 ottobre 1975, n. 654 (di ratifica della Convenzione sull'eliminazione di ogni forma di discriminazione razziale, sulla quale ci soffermeremo nel secondo paragrafo), come modificata in varie occasioni, doveva essere annullata, con rinvio per un nuovo giudizio ad altra sezione, perché i giudici di secondo grado sono tenuti a procedere a un'adeguata ricostruzione della vicenda e a indicare come la manifestazione di odio in discussione provochi un concreto pericolo di comportamenti discriminatori in un determinato contesto. I giudici di merito avevano condannato due cittadini italiani che avevano esposto su un camion pubblicitario un manifesto con il messaggio "clandestino uccide tre italiani a picconate – pena di morte subito". Il testo era accompagnato da un'immagine ancora più forte costituita da una ghigliottina con una lama grondante di sangue, l'immagine della testa di un uomo di colore decapitato e, in primo piano, la scritta pubblicitaria del negozio. Il Tribunale di Busto Arsizio, con sentenza del 15 novembre 2017, aveva condannato i responsabili per aver propagandato idee fondate

sull'odio razziale a 6 mesi di reclusione, con la concessione di alcuni benefici. La Corte di appello di Milano, con la pronuncia del 14 febbraio 2019, aveva confermato il verdetto e, quindi, i due autori avevano presentato ricorso in Cassazione sostenendo di essere stati condannati per il reato di cui all'art. 6 del d.l. 122/1993 ("Misure urgenti in materia di discriminazione razziale, etnica e religiosa")[1], ma non per quello previsto dalla l. 654/1975 che era stato loro contestato, con violazione del contraddittorio ed errore nel trattamento sanzionatorio. Tra gli altri motivi, i ricorrenti sostenevano che fosse stato violato l'art. 21 della Costituzione che assicura la libera manifestazione del pensiero.

La Corte di Cassazione, come detto, ha accolto il ricorso nella parte in cui i giudici di merito non hanno adeguatamente motivato l'accertamento dell'esistenza di una propaganda discriminatoria per l'esposizione dei manifesti pubblicitari, aspetto sul quale intendiamo soffermarci nel prosieguo.

La propaganda discriminatoria per motivi legati alla razza è venuta in rilievo anche con la sentenza n. 34815 depositata il 30 luglio 2019 dalla V sezione penale. In questo caso, la Cassazione ha confermato la condanna disposta dalla Corte di appello di Milano per diffamazione aggravata dalla finalità di discriminazione etnica e razziale perpetrata dall'allora parlamentare europeo Mario Borghezio che, nel corso di una trasmissione radiofonica, aveva commentato la nomina di Cecile Kyenge a Ministro dell'integrazione definendola "del bonga bonga" e aggiungendo espressioni "noi non siamo congolesi". In questo caso, la Suprema Corte ha ritenuto il ricorso dell'ex parlamentare infondato rilevando che la diffamazione aggravata ai sensi dell'art. 3, c. 1, della l. 205/1993[2] è una "*species*" del più ampio *genus* dei discorsi di propaganda razziale *ex* art. 3, c. 1, lett. *a*) della l. 654/1975 chiarendo, inoltre, che la propaganda di idee finalizzata all'odio razziale o etnico deve essere integrata non da «qualsiasi sentimento di generica antipatia, insofferenza o rifiuto riconducibile a motivazioni attinenti alla razza, alla nazionalità o alla religione ma solo da un sentimento idoneo a determinare il concreto pericolo di comportamenti discriminatori», specificando che «la 'discriminazione per motivi razziali' è quella fondata sulla qualità personale del soggetto e non – invece - sui suoi comportamenti». L'aggravante, quindi, opera solo nei casi in cui si manifesti un'azione che ha in sé un esplicito pregiudizio di inferiorità di una razza che si concretizza «nell'intenzionale esternazione del medesimo sentimento ed alla volontaria provocazione in altri di analogo sentimento di odio fino a dar luogo, in futuro o nell'immediato, al concreto pericolo di comportamenti discriminatori», mentre non ha rilievo il fine specifico di incitamento all'odio razziale. La Cassazione, inoltre, ha ritenuto che i giudici di merito avessero valutato correttamente il contenuto integrale dell'intervista considerando il complessivo contesto comunicativo. È stata altresì respinta l'applicazione della scriminante del diritto di critica politica, sulla quale torneremo successivamente[3], anche per l'assenza della necessaria continenza espressiva.

[1] In *GU* n. 97 del 27 aprile 1993, convertito con modificazioni con legge 25 giugno 1993 n. 205, in *GU* del 26 giugno 1993 n. 148.

[2] *Supra,* n. 2.

[3] Si rinvia al par. 5.

Le due sentenze permettono, così, di svolgere alcune osservazioni sul reato di propaganda di idee finalizzata alla discriminazione razziale in relazione ai limiti e agli obblighi posti dal diritto internazionale. Pertanto, prima di alcune considerazioni sulle pronunce, è necessario precisare il quadro internazionale esistente, seppure nei limiti legati alle sentenze in esame.

2. Il quadro internazionale sul divieto di propaganda finalizzata alla discriminazione

Un ruolo di primo piano in quest'ambito è svolto, infatti, da atti internazionali come, per limitarci a quelli di portata universale e a quelli più significativi in relazione ai casi qui esaminati, la Dichiarazione universale dei diritti dell'uomo adottata dall'Assemblea generale delle Nazioni Unite, a New York, il 9 dicembre 1948, la quale prevede, oltre all'uguaglianza di ogni essere umano (art. 1), che ogni individuo ha diritto a una eguale tutela contro la discriminazione nonché contro qualsiasi incitamento a tale discriminazione (art. 7)[4] e che i diritti inclusi in tale atto non possono essere esercitati in modo contrario ai fini e ai principi delle Nazioni Unite (art. 29, c. 3), che incoraggiano il rispetto dei diritti dell'uomo e delle libertà fondamentali per tutti senza distinzione di razza, di sesso, di lingua o di religione. Centrale, come visto nelle due sentenze della Cassazione, è stata ed è la Convenzione internazionale sull'eliminazione di ogni forma di discriminazione razziale, adottata a New York il 21 dicembre 1965, in vigore sul piano internazionale dal 4 gennaio 1969 e ratificata dall'Italia con la l. 654/1975, che contiene anche l'ordine di esecuzione (in vigore per l'Italia dal 4 febbraio 1976)[5]. Tale atto dispone che è vietata «ogni propaganda ed ogni organizzazione che s'ispiri a concetti ed a teorie basate sulla superiorità di una razza o di un gruppo di individui di un certo colore o di una certa origine etnica, o che pretendano di giustificare o di incoraggiare ogni forma di odio e discriminazione razziale» (art. 4). Inoltre, secondo la Convenzione, gli Stati sono tenuti ad adottare anche misure positive per realizzare gli obblighi convenzionali[6].

Grazie all'art. 8 è stato istituito un Comitato per l'eliminazione della discriminazione razziale con il compito di monitorare l'attuazione della Convenzione da parte degli

[4] Si veda, tra la sterminata bibliografia, R. Pisillo Mazzeschi, *Diritto internazionale dei diritti umani. Teoria e prassi,* Torino, 2020, spec. 294, il quale sottolinea che «il divieto generale di discriminazione…deriva, più che da una norma, da un vero e proprio *principio generale* che sovrintende all'intero settore dei diritti umani, perché alla base di tale sistema vi sono sia l'idea dell'universalismo (come riconoscimento globale) dei diritti fondamentali sia quella, strettamente collegata, per cui gli Stati devono garantire tali diritti *a tutti gli esseri umani* senza discriminazioni».

[5] Cfr. I. Dore, *United Nations Measures to Combat Racial Discrimination: Progress and Problems in Retrospect*, in *Denver Journ. Int. Law*, 2020, 299 ss.; L. Manca, *Sul contrasto al* racial Hate Speech *nella prassi del Comitato delle Nazioni Unite per l'eliminazione della discriminazione razziale*, in *OIDU,* 2018, 457 ss.; M. Goldmann - M. Sonnen, *Soft Authority Against Hard Cases of Racially Discriminating Speech: Why the CERD Committee Needs a Margin of Appreciation Doctrine,* in *ssrn.com*, 2015.

[6] Le traduzioni in italiano degli atti internazionali citati nel presente lavoro sono reperibili in R. Luzzatto - F. Pocar, *Codice di diritto internazionale pubblico*, Torino, 2016.

Stati e, previa dichiarazione di accettazione di competenza sempre ad opera degli Stati parti, con il compito di ricevere ed esaminare comunicazioni di persone o gruppi di persone che si lamentino di essere vittime di una violazione di uno dei diritti stabiliti nella Convenzione[7]. A tale Trattato è seguito il Patto sui diritti civili e politici del 16 dicembre 1966[8]: l'art. 26 impone agli Stati di punire «ogni discriminazione fondata sulla razza, il colore, il sesso, la lingua, la religione, l'opinione politica o qualsiasi altra opinione, l'origine nazionale o sociale, la condizione economica, la nascita o qualsiasi altra condizione» e, inoltre, in modo innovativo per quei tempi, l'art. 20 sancisce il divieto per coloro che esercitano la libertà di espressione di «ogni appello all'odio nazionale, razziale o religioso che costituisca incitamento alla discriminazione, all'ostilità o alla violenza»[9], così come ogni propaganda a favore della guerra. A sottolineare l'importanza di impedire forme di discriminazione che portano a compromettere ogni diritto umano, vale la pena ricordare l'art. 4 che ammette la possibilità per gli Stati di prendere talune misure, in caso di pericolo pubblico eccezionale, per derogare agli obblighi imposti dal Patto, ma a condizione che dette misure non comportino una discriminazione fondata sulla razza, sul colore, sul sesso, sulla lingua, sulla religione o sull'origine sociale.

Sul piano regionale, limitando l'analisi al contesto europeo, giova ricordare la Convenzione europea dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950, citata nella sentenza Borghezio, il cui art. 14 dispone che il godimento dei diritti e delle libertà riconosciute nella Convenzione deve essere assicurato senza distinzione di religione, di opinione politica o di altro genere, di origine nazionale etc., norma che opera solo in collegamento con la violazione di altri diritti sostanziali riconosciuti nella Convenzione. Tuttavia, con il Protocollo n. 12, adottato il 4 novembre 2000 (in vigore sul piano internazionale dal 1° aprile 2005) – che non è stato ratificato da tutti gli Stati del Consiglio d'Europa, inclusa l'Italia -, il divieto generale di discriminazione ha assunto una portata autonoma, prevedendo, altresì, che «nessuno può essere oggetto da parte di un'autorità pubblica di una qualunque discriminazione fondata in particolare sui motivi elencati al paragrafo 1», il quale dispone il divieto di discriminazione fondato «sul sesso, la razza, il colore, la lingua, la religione, le opinioni politiche o sociali, l'appartenenza ad una minoranza nazionale, la ricchezza, la nascita od ogni altra situazione».

Rispetto al Patto sui diritti civili e politici, la Convenzione europea non esplicita, nel riconoscimento del diritto alla libertà di espressione di cui all'art. 10[10], il divieto di *hate*

---

[7] Si veda anche il *Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence*, 11 gennaio 2013, A/HRC/22/17/Add.4, in *ohchr.org*, nonché *The UN Strategy and Plan of Action on Hate Speech*, 2019, in *un.org*.

[8] I testi e la documentazione sono reperibili nel sito *ohchr.org/english/bodies/hrc/index.htm*. Per quanto riguarda i ricorsi individuali al Comitato si veda *ohchr.org/english/bodies/hrc/procedure.htm*.

[9] Cfr. M. Castellaneta, *L'*hate speech*: da limite alla libertà di espressione a crimine contro l'umanità*, in G. Venturini - S. Bariatti (a cura di), *Diritti individuali e giustizia internazionale, Liber Fausto Pocar,* Milano, 2009, 157 ss.; P. Lambert, *Racisme et liberté d'expression dans la Convention européenne des droits de l'homme,* in P. Mahoney (ed.), *Protection des droits de l'homme: la perspective européenne, Mélanges à la mémoire de Rolv Ryssdal*, Köln – Berlin – Bonn -München, 2000, 735 ss.

[10] Cfr. T. McGonagle, *Freedom of Expression and Defamation,* Strasbourg, 2016; M. Oetheimer - A. Cardone, *Art. 10*, in S. Bartole - P. De Sena - V. Zagrebelsky (a cura di), *Commentario breve alla Convenzione*

speech, prevedendo, però, che tale libertà, «*comportando doveri e responsabilità*», possa essere sottoposta «*a determinate formalità, condizioni, restrizioni o sanzioni previste dalla legge costituenti misure necessarie in una società democratica, per la sicurezza nazionale, l'integrità territoriale o l'ordine pubblico, la prevenzione dei disordini e dei reati, la protezione della salute e della morale, la protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni confidenziali o per garantire l'autorità e l'imparzialità del potere giudiziario*». Tuttavia, grazie alla giurisprudenza della Corte europea, sin dalla sentenza del 23 settembre 1994, *Jersild c. Danimarca*[11], è stato stabilito che l'incitamento all'odio è in contrasto con i principi e i valori affermati dalla Convenzione e non rientra nell'ambito del diritto alla libertà di espressione. Tra l'altro, la Corte europea ha fornito indicazioni agli Stati precisando che un discorso o un articolo costituiscono un incitamento all'odio in presenza di due requisiti che devono essere cumulativamente presenti: l'utilizzo di espressioni che minano la dignità umana, con un carattere discriminatorio e il particolare contesto nel quale i discorsi sono pronunciati, anche se tale ultimo elemento non è stato considerato in presenza di un evidente incitamento all'odio in grado di fare apparire subito il contrasto delle dichiarazioni rese con i valori fondamentali come la tolleranza, la pace sociale e la non discriminazione[12]. Così, ad esempio, nella sentenza del 4 dicembre 2003, *Gündüz c. Turchia*, ric. 35071/97, la Corte ha osservato che un discorso va inquadrato tra i casi di incitamento all'odio in presenza di espressioni che minano la dignità umana, con un carattere discriminatorio e del particolare contesto nel quale i discorsi sono pronunciati. In quell'occasione, la Corte ha ritenuto che la condanna del ricorrente pronunciata dai tribunali turchi fosse in contrasto con la Convenzione perché, pur essendo presente il primo requisito indicato, valutando il contesto, non si poteva ritenere che vi fosse stato un caso di *hate speech*. Nella decisione sulla ricevibilità del 20 febbraio 2007, *Ivanov c. Russia*, ric. 35222/04, la Corte, invece, ha dichiarato irricevibile il ricorso perché la pubblicazione degli articoli che incitavano all'odio contro gli ebrei non poteva usufruire della protezione di cui all'art. 10 in quanto in contrasto con valori fondamentali come la tolleranza, la pace sociale e la non discriminazione, rilevando, però, che non era necessario valutare il contesto a causa del carattere marcatamente antisemita delle dichiarazioni.

I principi affermati dalla Corte sono stati enunciati dal Comitato dei Ministri nella raccomandazione R(97)20 del 30 ottobre 1997 con la quale il Comitato ha chiesto agli Stati di combattere l'*hate speech* che riguarda «*all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance...*».

Per quanto riguarda l'Unione europea è da ricordare l'art. 21 della Carta dei diritti fondamentali in base al quale «*È vietata qualsiasi forma di discriminazione fondata, in particolare,*

europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, Padova, 2012, 397 ss.

[11] La Corte ha rilevato che l'*hate speech* non è protetto dal diritto alla libertà di espressione, anche se la condanna al giornalista, inflitta dai tribunali nazionali perché il codice penale danese vieta i discorsi di incitamento all'odio, era in contrasto con l'art. 10 perché le interviste a un gruppo di giovani neonazisti erano state condotte durante una trasmissione televisiva destinata a un pubblico "ben informato" e perché il giornalista aveva controbilanciato le affermazioni, non incitando all'odio.

[12] Va ricordato che anche la Carta sociale europea nella sua versione riveduta nel 1996, in vigore dal 1999, ha introdotto, rispetto alla versione del 1961, all'articolo E, il divieto di discriminazione.

sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale»[13]. Tra gli atti di diritto comunitario derivato si può ricordare, tra i tanti, la direttiva 2000/43/CE del 29 giugno 2000 che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica[14] e la decisione quadro 2008/913/Gai del 28 novembre 2008 sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale[15].

3. L'attuazione in Italia degli atti internazionali sul divieto di diffusione di idee discriminatorie

Il quadro normativo nazionale, come detto, è in gran parte fondato sulla Convenzione sull'eliminazione di ogni forma di discriminazione razziale e, quindi, sulla citata l. 654/1975 il cui originario art. 3 ha introdotto il reato di diffusione di idee fondate sulla superiorità o sull'odio razziale, nonché l'incitamento a commettere atti di violenza o di provocazione alla violenza «nei confronti di persone perché appartenenti ad un gruppo nazionale, etnico o razziale». La pena prevista era la reclusione da uno a quattro anni. Successivamente, con la legge 25 giugno 1993, n. 205 (nota come "legge Mancino") di conversione, con modificazioni, del d.l. 122/1993 «recante misure urgenti in materia di discriminazione razziale, etnica e religiosa»[16], la sanzione è passata alla reclusione sino a 3 anni. Inoltre, ai casi di incitamento alla violenza per motivi razziali, etnici, nazionali, è stato aggiunto quello per motivi religiosi[17]. Ulteriori modifiche nel segno dell'alleggerimento della pena sono state apportate con l'art. 13, c. 1, della legge 24 febbraio 2006, n. 85 (con la reclusione fino ad un anno e sei mesi o con la multa fino a 6.000 euro per la propaganda, che ha sostituito la diffusione di idee ed istigazione, termine che ha sostituito l'incitamento). Successivamente, con la modifica

[13] Il par. 2 dell'art. 21 stabilisce, inoltre, che «Nell'ambito d'applicazione dei trattati e fatte salve disposizioni specifiche in essi contenute, è vietata qualsiasi discriminazione in base alla nazionalità». L'art. 20 assicura il diritto di uguaglianza di tutte le persone dinanzi alla legge.

[14] In *GUCE* L 180, 18 luglio 2000, 22 ss. Si veda anche la direttiva 2000/78 del 27 novembre 2000 che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro, in *GUCE* L 303 del 2 dicembre 2000, 16 ss., recepite, la prima con il decreto legislativo n. 215 del 9 luglio 2003 (in *GU* n. 186 del 12 agosto 2003) e, la seconda, con il decreto legislativo n. 216 del 9 luglio 2003 (in *GU* n. 187 del 13 agosto 2003). Con la legge n. 167/2017 è stato inserito nel decreto legislativo n. 231/2001 il reato di istigazione e incitamento al razzismo e alla xenofobia con la previsione della responsabilità delle società punite con una sanzione pecuniaria.

[15] In *GUUE* L 328, 6 dicembre 2008, 55 ss. Nella direttiva 2012/29/UE del 25 ottobre 2012, che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato e che sostituisce la decisione quadro 2001/220/GAI (in *GUUE* L 315, 14 novembre 2012, 57 ss., recepita in Italia con decreto legislativo 15 dicembre 2015, n. 212) le vittime di messaggi di incitamento all'odio sono incluse tra quelle particolarmente vulnerabili.

[16] Cfr., tra gli altri, E. Fronza, *Il negazionismo come reato,* Milano, 2012; M. Manetti, *Libertà di pensiero e negazionismo,* in M. Ainis (a cura di), *Informazione, potere, libertà,* Torino, 2008, 41 ss.

[17] È altresì punita la partecipazione ad organizzazioni o associazioni che propugnano detta discriminazione.

apportata con la legge 16 giugno 2016, n. 115, l'art. 3 è stato inserito all'interno del codice penale con il decreto legislativo 1° marzo 2018, n. 21 e, in particolare, negli artt. 604-*bis* e 604-*ter* dedicati al divieto di propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa[18]. Inoltre, a completare il quadro, è intervenuta la legge 25 ottobre 2017 n. 163 "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea – Legge di delegazione europea 2016-2017", con la quale, per assicurare la completa attuazione della citata decisione quadro 2008/913/GAI, è stata modificata l'aggravante del negazionismo aggiungendo i casi di minimizzazione grave o l'apologia della Shoah o dei crimini di genocidio, dei crimini contro l'umanità, dei crimini di guerra come stabiliti nello Statuto della Corte penale internazionale. L'indicata decisione quadro impone agli Stati di punire in sede penale, tra gli altri, i reati di «istigazione pubblica alla violenza o all'odio nei confronti di un gruppo di persone o di un suo membro, definito in riferimento alla razza, al colore, alla religione, all'ascendenza o all'origine nazionale o etnica» (art. 1, lett. a)[19].

4. La propaganda con finalità di discriminazione e l'obbligo di valutazione del contesto

Ricostruito il quadro esistente, seppure sommariamente e per i soli fini di analisi delle sentenze in oggetto, passiamo ad analizzare le questioni problematiche in relazione all'applicazione delle regole internazionali indicate, sollevate dalle due citate pronunce tenendo conto che in entrambe le sentenze si è posta la questione di individuare gli elementi costitutivi del reato di propaganda di idee fondate sull'odio razziale e di fissare il punto di equilibrio tra diritto alla libertà di espressione e divieto di discriminazione. Precisato che "diffusione di idee" e "propaganda" vanno interpretate nel senso di una continuità della fattispecie[20], nella sentenza n. 1602/20, la Cassazione ha considerato errato il percorso logico giuridico seguito dai giudici di merito secondo i quali il richiamo "in modo cruento e plateale" all'applicazione della pena di morte è di per sé un'attività discriminatoria in quanto collegata al colore della pelle dell'uomo accusato di omicidio. La mancata ricostruzione del contesto da parte dei giudici di primo e di secondo grado impedisce – osserva la Cassazione – la comprensione del carattere "discriminatorio della pubblicità esposta sul camion" che sembra legata ai comportamenti degli individui oggetto del manifesto, accusati di triplice omicidio, piuttosto che

[18] Riguardo alla sostituzione dei termini indicati, la Corte di Cassazione, sez. III penale, con la sentenza n. 37581 del 7 maggio 2008 ha evidenziato una continuità tra le fattispecie incriminatrici con la conseguenza che il cambiamento dei termini non incide in alcun modo sulla fattispecie punita in sede penale. Cfr. G. Pavich - A. Bonomi, *Reati in tema di discriminazione: il punto sull'evoluzione normativa recente, sui principi e valori in gioco, sulle prospettive legislative e sulla possibilità di interpretare in senso conforme a Costituzione la normativa vigente,* in *Dir. Pen. Cont.,* 2014, 10 ss.

[19] Cfr. la Comunicazione sul recepimento della decisione quadro presentata dalla Commissione europea il 27 gennaio 2014 (COM(2014)27), nonché il parere dell'Agenzia europea dei diritti fondamentali dell'Unione europea n. 2/2013 del 15 ottobre 2013, reperibile nel sito http://www.fra.europa.eu.

[20] Si veda *supra,* nota 18.

alla qualità personale del soggetto destinatario dei messaggi discriminatori e, quindi, in sostanza, all'individuo in quanto appartenente ad un gruppo. Ci sembra, inoltre, in aggiunta a quanto sostenuto dalla Cassazione, che solo un'adeguata motivazione permette di cogliere la matrice discriminatoria e razzista del fatto e di procedere a una corretta imputazione e condanna che poi regga anche al vaglio della Corte europea dei diritti dell'uomo, la quale, in diverse occasioni, ha sottolineato che nei casi di ricorsi per violazione dell'art. 10 della Convenzione in caso di condanne per diffamazione o incitamento alla discriminazione va tenuto conto del contesto nel quale le manifestazioni sono rese proprio per raggiungere un giusto bilanciamento tra i diritti in gioco.
Per quanto riguarda la necessità di fare riferimento alla qualità personale del soggetto che viene colpito per ciò che rappresenta e non per i suoi comportamenti, la Cassazione ha evidenziato il rilievo di tale aspetto anche nella pronuncia Borghezio nella quale è stato rilevato che non è necessario il fine specifico di un incitamento all'odio, ma è sufficiente l'esternazione di una condizione di inferiorità «attribuita a soggetti determinati e fatta derivare dall'appartenenza ad una determinata razza».
In sostanza, per accertare l'effettiva commissione del reato o dell'aggravante nel caso di diffamazione, è necessario individuare un preciso collegamento tra qualità del soggetto che viene colpito in base a una sua specifica caratteristica, come l'appartenenza a un gruppo, e il messaggio, mentre non rilevano i suoi comportamenti. Nel caso Borghezio, le dichiarazioni dell'ex parlamentare europeo avevano al centro proprio l'etnia e la razza, mentre nel caso del manifesto pubblicitario, a causa della mancata analisi del contesto, non è stato chiarito se il manifesto pubblicitario fosse legato al dato fattuale del reato presumibilmente commesso dai tre migranti o alla sola razza dei tre individui.
È poi rilevante, come detto, il contesto in cui si colloca la singola condotta che serve, altresì, ad «assicurare il contemperamento dei principi di pari dignità e di non discriminazione con quello di libertà di espressione» (sentenza n. 1602, § 3.1). La Cassazione, proprio nel caso del manifesto pubblicitario, ritiene necessario che i giudici di merito non si limitino a stabilire che le espressioni riportate siano "*ex se* attività discriminatoria" in ragione della contrapposizione tra "clandestino", di pelle nera, e gli italiani, anche in connessione all'esibizione di una ghigliottina con la testa decapitata di un uomo, perché nel giudizio di merito è necessario dimostrare che l'odio razziale o etnico sia integrato «da un sentimento idoneo a determinare il concreto pericolo di comportamenti discriminatori, idoneità che nel caso di specie non è stata in alcun modo indagata dai giudici di merito e che viene, anzi, di fatto presunta in base alla circostanza dell'esposizione al pubblico del manifesto pubblicitario». Sembra evidente, quindi, che si debba dimostrare la concreta pericolosità del fatto non delimitata, però, al momento in cui la comunicazione controversa viene effettuata, consentendo così una più ampia applicazione, con un accertamento, però, del contesto.
Resta da vedere se la richiesta degli indicati elementi ai fini della punibilità sia conforme alla Convenzione del 1965 il cui art. 4 chiede agli Stati parti di procedere alla condanna di ogni propaganda basata sulla superiorità della razza o di un gruppo di individui «di un certo colore o di una certa origine etnica», precisando, alla lett. *a*), che va considerata punibile la diffusione di idee basate sulla superiorità o sull'odio razziale nonché ogni incitamento alla discriminazione, non legando la previsione del reato e

l'esigenza punitiva necessaria anche come deterrente alla perpetrazione di comportamenti discriminatori, a una valutazione del contesto[21].

Tuttavia, taluni chiarimenti sulla norma in esame sono arrivati dal Comitato per l'eliminazione della discriminazione razziale (CERD) che, nelle Osservazioni generali n. 35 presentate il 26 settembre 2013, relative all'art. 4[22] e intitolate "*Combating racist hate speech*"[23], precisato che malgrado la Convenzione non parli espressamente di *hate speech* è a questo che si intende fare riferimento[24], ha sottolineato che bisogna tener conto della natura del discorso e del suo contenuto, del contesto, dello *status* di chi compie il messaggio e della portata. L'art. 4 non fornisce un elenco o elementi per la qualificazione di un fatto come propaganda da proibire; tuttavia, il Comitato ha chiarito che discorsi che in determinato contesto sono neutri, in altri possono risultare pericolosi, provocando una progressione di eventi di matrice discriminatoria.

Proprio la valutazione del contesto, a nostro avviso, è poi essenziale per contemperare l'esigenza di punire la propaganda di idee e la discriminazione per motivi razziali con la libertà di espressione. Ci sembra, quindi, che la richiesta di motivare, sulla base del contesto, le ragioni che portano a una condanna per propaganda con fine discriminatorio prospettata dalla Cassazione, come elemento per individuare anche la pericolosità del fatto, sia conforme alla Convenzione. D'altra parte, proprio perché è in gioco un bilanciamento tra diritti, poggiare una condanna sul solo dato formale ossia l'espressione riprodotta nel manifesto porterebbe a un ridimensionamento troppo forte del diritto alla libertà di espressione che in determinati Stati potrebbe dare vita ad abusi. In questo senso, si può richiamare quanto sostenuto da un componente del Comitato, Carlos Manuel Vazquez, nell'opinione dissenziente allegata alla Comunicazione *TBB-Tukish in Berlin contro Germania*[25] - con la quale il Comitato ha accolto il ricorso - il quale ha osservato che «*States parties should take account of the context and the genre of the discussion in which the statememts were made*».

Nella stessa direzione è orientata la Corte europea dei diritti dell'uomo che, con la citata sentenza *Gündüz c. Turchia*, ha chiarito che un discorso o un articolo costituiscono un incitamento all'odio in presenza di due requisiti che devono essere cumulativamente presenti: l'utilizzo di espressioni che minano la dignità umana, con un carattere discriminatorio, e il particolare contesto nel quale i discorsi sono pronunciati[26]. Tale orientamento è stato confermato in altre occasioni come ad esempio nella sentenza dell'11 gennaio 2000, *News Verlags GmbH & CoKG c. Austria,* ric. 31457/96 e nella sentenza del 10 luglio 2008, *Soulas e altri c. Francia,* ric. 15948/03, nella quale la Corte

[21] Si veda il rapporto sull'Italia del 6 marzo 2019, CERD/C/ITA/21, reperibile nel sito https://www.ohchr.int. Nell'allegato al rapporto sono riportate le sentenze più significative sull'applicazione della Convenzione.

[22] Sulla stessa disposizione si vedano le Osservazioni generali n. 7 sull'attuazione dell'art. 4 (INT_CERD_Gec_7479).

[23] CERD/C/GC/35.

[24] Si veda T. McGonagle, *General Recommendation 35 on Combating Racist Hate Speech*, in D. Keane - A. Waughray (eds.), *Fifty Years of the International Convention on the Elimination of All Forms of Racial Discrimination. A living Instrument*, Manchester, 2017, 246 ss.

[25] Documento CERD/C/82/D/48/2010, 10 maggio 2013, § 14 dell'opinione.

[26] La Corte ha sottolineato l'importanza della lotta contro la discriminazione razziale e ha ritenuto

ha sottolineato che «*L'ouvrage litigieux a été publié dans un contexte qui, en France, est particulier*» (§ 52), giustificando così la condanna. Ancora più di recente, poi, la Corte, con la sentenza del 7 luglio 2020, *Rashkin c. Russia,* ric. 69575/10, ha osservato che i giudici nazionali non avevano preso in considerazione il contesto nel quale il politico aveva reso le sue dichiarazioni e, così, la Corte ha accolto il ricorso del politico condannato per diffamazione con finalità discriminatorie a causa di alcune espressioni utilizzate durante un comizio elettorale[27], proprio a causa della mancata valutazione del contesto. Quest'ultima serve anche per graduare gli interventi punitivi, considerando che non in ogni occasione è necessario, per fronteggiare la diffusione di idee discriminatorie, procedere sul piano penale in quanto gli Stati, proprio perché tenuti ad adottare misure positive, devono individuare gli strumenti ritenuti migliori per raggiungere gli obiettivi della Dichiarazione universale dei diritti dell'uomo e della stessa Convenzione. È stato lo stesso CERD, in varie occasioni, a rilevare che gli Stati devono accertare se la misura di natura penale sia necessaria e proporzionale e, nell'effettuare tale accertamento, devono tenere conto di numerosi fattori tra i quali la forma con la quale la dichiarazione è diffusa, le persone che possono essere raggiunte dalla comunicazione e se la dichiarazione offensiva è rivolta direttamente a un gruppo. Il test sulla proporzionalità e la necessarietà in una società democratica di una misura che incide sulla libertà di espressione, giustificata da un bisogno sociale imperativo costituito, in questi casi, dalla tutela della dignità umana, è centrale anche nella giurisprudenza della Corte europea.
Pertanto, la richiesta di una motivazione in ordine al contesto imposta dalla Cassazione ai giudici di merito è anche funzionale ad evitare condanne da Strasburgo tenendo conto che la stessa Corte europea procede a verificare che tale attività, come avvenuto con la sentenza del 23 luglio 2019 *Gürbüz c. Turchia* (ric. 8860/13), sia stata svolta dai giudici nazionali tenuti a «*porter attention aux termes employés et au contexte dans lequel leur publication s'inscrit*» (§ 35). Nella stessa direzione, con la sentenza dell'11 febbraio 2020, *Atamanchuk c. Russia* (ric. 4493/11), la Corte europea ha respinto il ricorso di un uomo d'affari condannato per incitamento all'odio e alla discriminazione sulla base dell'etnia perché i tribunali nazionali hanno attentamente valutato il contesto nel quale il limite alla libertà di espressione era stato applicato.
Alla luce di quanto detto, quindi, possiamo ritenere che le sentenze della Cassazione rispettino gli standard internazionali.
Un'unica affermazione della Corte di Cassazione, nella sentenza Borghezio, non ci sembra del tutto condivisibile ossia che, ad avviso della Suprema Corte, l'orientamento di Strasburgo sia cambiato nel senso che in passato i ricorsi per violazione dell'art. 10 in materia di istigazione all'odio razziale erano respinti e considerati inammissibili per contrasto con l'art. 17[28] che vieta l'abuso del diritto stabilendo che nessuna disposi-

conforme alla Convenzione la condanna dei tribunali francesi nei confronti dei ricorrenti autori di un libro e di articoli contro gli immigrati musulmani perché i giudici nazionali avevano fondato la condanna degli autori e dell'editore sulla valutazione che detto testo fosse, nel contesto in cui le idee erano diffuse, un incitamento alla discriminazione, all'odio e alla violenza nei confronti di un gruppo in ragione della loro origine.

[27] Si veda il § 14 e le sentenze lì richiamate. Cfr. anche la sentenza del 13 marzo 2018, *Stern Tarlats e Roura Capellera c. Spagna*, ricc. 51168/15 e 51186/15, § 41.

[28] Sull'art. 17 si veda, tra gli altri, F. Falconi, *Alcune considerazioni sull'abuso della libertà di espressione nella*

zione della Convenzione può essere interpretata come implicante il diritto per uno Stato o gruppo o individuo di esercitare un'attività «mirante alla distruzione dei diritti o delle libertà riconosciti nella presente Convenzione…», mentre oggi «un più recente approccio suggerisce…che tutti i casi di libertà di espressione siano trattati alla luce dell'art. 10, par. 1, e che ogni ingerenza con il diritto sia vagliata alla luce del test di necessità dell'art. 10, par. 2». In realtà, a ben vedere, in quest'ambito è indispensabile un'analisi caso per caso ed è così difficile desumere un preciso orientamento, anche se la Corte ricorre all'art. 17 nei casi in cui è "del tutto chiaro" che quanto dichiarato a titolo di libertà di espressione è manifestamente contrario ai valori convenzionali e viene utilizzato per colpire proprio il fine specifico dell'art. 10 della Convenzione e per comprometterne i valori (si veda la sentenza del 17 dicembre 2013, *Perincek c. Svizzera*, ric. 27510/08, § 114, confermata dalla Grande Camera con sentenza del 15 ottobre 2015). Ed invero, nella decisione *M'Bala M'Bala* (noto come *Dieudonnê*) *c. Francia* (ric. 25239/13) del 20 ottobre 2015, la Corte ha addirittura applicato l'art. 17 non solo con riguardo a manifestazioni esplicite e dirette per le quali non è necessaria alcuna interpretazione, ma anche con riferimento alle espressioni antisemite "*travestie sous l'apparence d'une production artistique*", ritenendo tali espressioni "*dangereuse qu'une attaque frontale et abrupte*" (§ 40)[29].

In ogni caso, l'applicazione dell'art. 10, par. 2, non ha conseguenze negative rispetto al divieto di propaganda di idee incentrate sulla discriminazione razziale perché richiede unicamente una maggiore attenzione nell'accertare che il bilanciamento sia stato corretto e che la misura limitativa della libertà di espressione sia stata necessaria in una società democratica e proporzionale, oltre a garantire una valutazione del contesto che, come visto poc'anzi, è alla base anche dell'applicazione dell'art. 4 della Convenzione sull'eliminazione di ogni forma di discriminazione razziale.

*giurisprudenza di Strasburg*o, in *Studi sull'integrazione europea*, 2020, 359 ss.; C. Frances Moran, *Responsibility and freedom of speech under article 10*, in *Eur. Hum. Rights Law Rev.*, 1, 2020, 67 ss.; P. Tanzarella, *Discriminare parlando. Il pluralismo democratico messo alla prova dai discorsi d'odio razziale*, Torino, 2020; Id., *Il caso Taormina e la Corte di giustizia. Dalla libera espressione alla discriminazione*, in *questa Rivista*, 2, 2020, 289 ss.; M. Castellaneta, *Il negazionismo tra abuso del diritto e limite alla libertà di espressione in una decisione della Corte europea dei diritti dell'uomo*, in *questa Rivista*, 2, 2019, 311 ss.; Id., *L'*hate speech*: da limite alla libertà di espressione a crimine contro l'umanità*, cit., 157 ss.; C. Caruso, *L'*hate speech *a Strasburgo: il pluralismo militante del sistema convenzionale*, in *Quad. costituzionali*, 2017, 963 ss.; M.E. Villiger, *Article 17 ECHR and freedom of speech in Strasbourg practice*, in J. Casadevall - E. Myjer - M. O'Boyle - A. Austin (a cura di), *Freedom of Expression, Essays in honour of Nicolas Bratza*, Oisterwijk, 2012, 321 ss.; I. Hare, *Extreme Speech Under International and Regional Human Rights Standards,* in I. Hare - J. Weinstein (a cura di), *Extreme Speech and Democracy*, Oxford, 2009, 62 ss.; A. Weber, *Manual on hate speech,* Strasburgo, 2009; O. Pollicino, *La repressione del negazionismo e la giurisprudenza della Corte europea dei diritti umani,* in *DUDI*, 2011, 85 ss.

[29] Così nella decisione di irricevibilità *Belkacem c. Belgio* (ric. 34367/14) depositata dalla Corte europea dei diritti dell'uomo il 20 luglio 2017: nei casi di incitamento all'odio non è necessario accertare la proporzionalità della sanzione disposta dalle autorità nazionali competenti, a differenza di quanto accade nelle fattispecie di compressione dell'art. 10 per motivi quali la tutela della reputazione altrui, permettendo così agli Stati una maggiore potestà punitiva.

5. L'impossibilità di applicare la scriminante della critica politica

Nella sentenza n. 34815 relativa alla vicenda dell'*ex* europarlamentare Mario Borghezio è stata affrontata anche la questione dell'applicabilità della scriminante del diritto di critica politica. La Cassazione, a nostro avviso, ha correttamente respinto il ricorso dell'*ex* parlamentare europeo anche su questo punto sia per il tenore delle espressioni adoperate che contenevano "un'esplicita forma di disprezzo", indice dell'assenza della continenza espressiva che è necessaria anche quando si esercita il diritto di critica, sia in forza delle sentenze della Corte europea dei diritti dell'uomo. Proprio la Corte di Strasburgo, che ha ormai consolidato un orientamento volto a rafforzare e privilegiare il diritto alla libertà di espressione – anche in quanto diritto doppio che si sostanzia in un diritto attivo a informare e in un diritto passivo a ricevere comunicazioni – ha sottolineato che anche nei giudizi di valore, non suscettibili di dimostrazione, nei quali è ammissibile un grado di esagerazione e di provocazione, è necessario che ci sia un nucleo fattuale sufficiente altrimenti il «giudizio è gratuito e pertanto ingiustificato e diffamatorio». Inoltre, la stessa Corte europea ha negato protezione ad attacchi personali gratuiti e giustificato la misura detentiva nei confronti di chi commette atti di incitamento alla violenza.

Ci sembra, d'altra parte, che se è vero che la protezione della libertà di espressione all'interno di dibattiti politici debba godere di una protezione ampia, anche quando si tratti di idee controverse, è anche vero che l'esercizio dell'indicata libertà non deve compromettere il diritto all'uguaglianza e il divieto di discriminazione[30]. A ciò si aggiunga un ulteriore elemento: le dichiarazioni di un politico hanno, in via generale, una diffusione più ampia rispetto a quelle del singolo individuo perché non solo il politico si avvale di strumenti a larga diffusione come, nel caso di specie, di una radio nazionale, ma anche perché le dichiarazioni rese sono riprese dalle agenzie di stampa, dai social network e da altri organi d'informazione, con la conseguenza che le indicate dichiarazioni discriminatorie hanno più possibilità di produrre effetti negativi. Sin dalla sentenza del 16 luglio 2009, *Féret c. Belgio*, ric. 15615/07, la Corte ha ritenuto conforme alla Convenzione la condanna decisa dai tribunali nazionali di un parlamentare belga che, con volantini, utilizzava slogan contro gli immigrati, sostenendo che la «*liberté de discussion politique ne revêt assurément pas un caractère absolu*»: in particolare, per prevenire o sanzionare lesioni alla dignità degli esseri umani, le autorità nazionali hanno il diritto/dovere di intervenire proprio perché «*Les discours politiques qui incitent à la haine fondée sur les préjugés religieux, ethniques ou culturels représentent un danger pour la paix sociale et la stabilité politique dans les Etats démocratiques*» (§ 73)[31]. Così, con la decisione del 20 aprile 2010

[30] In questa direzione si veda anche il § 26 delle Osservazioni generali n. 35.

[31] Nella sentenza «*La Cour rappelle qu'il importe au plus haut point de lutter contre la discrimination raciale sous toutes ses formes et manifestations (Jersild c. Danemark, 23 septembre 1994, § 30, série A no 298) et renvoie au texte des différentes résolutions du Comité des Ministres du Conseil de l'Europe relatives à l'action de l'ECRI, ainsi qu'aux travaux et aux rapports de celle-ci, qui démontrent la nécessité de mener à l'échelle européenne en général, et à celle de la Belgique en particulier, une action ferme et soutenue pour lutter contre les phénomènes de racisme, de xénophobie, d'antisémitisme et d'intolérance*» (§ 72). Si veda P. De Sena, M. Castellaneta, La libertà di espressione e le norme internazionali ed europee, prese sul serio: sempre su CasaPound c. Facebook, in *sidiblog.org*, 20 gennaio 2020.

relativa al caso *Le Pen c. Francia*, la Corte di Strasburgo ha affermato l'importanza della lotta contro le discriminazioni razziali sotto tutte le sue forme e manifestazioni e, nel respingere il ricorso del politico dell'estrema destra Le Pen, condannato per i suoi discorsi contro gli immigrati, ha rilevato che il comportamento delle autorità francesi era stato corretto perché il proposito del politico era quello di dare un'immagine negativa di un'intera collettività e di suscitare un sentimento di ostilità verso un determinato gruppo di persone. Pertanto, la misura restrittiva della libertà di espressione era necessaria in una società democratica anche se - a dire del ricorrente - incideva negativamente sul dibattito politico[32].

Nulla poi, nelle dichiarazioni al centro della pronuncia n. 34815/19 permette di individuare una critica politica ma, anzi, come evidenziato dalla Cassazione, le dichiarazioni si concentrano «sul Ministro Kyenge, sia quale persona, nella specifica connotazione di genere e razziale, che quale responsabile del Dicastero assegnatole, alla quale viene riservato un vero e proprio attacco *ad hominem*, ingiustificato per la gratuità delle offese, portate ben oltre la lecita manifestazione di un'opinione dissenziente rispetto alla composizione ed al mandato politico di un Esecutivo tecnico» (§ 3.1 della sentenza). Che proprio un politico, poi, tenuto, a nostro avviso, "a dare un esempio", invece di articolare una critica politica «esprima disprezzo… rimarcandone il genere femminile e l'origine etnica…squalificandone la figura professionale e marcandone l'inferiorità razziale», impone un'applicazione rigorosa del divieto di propaganda di idee discriminatorie. Con la conseguenza che non solo è necessario punire chi divulga e fa propaganda discriminatoria, ma è anche indispensabile non accordare protezione a espressioni che non devono godere di alcuna tutela nell'ambito dell'esercizio del diritto alla libertà di espressione. Pertanto, a nostro avviso, accanto all'insussistenza «della invocata scriminante dell'esercizio del diritto di critica politica, in difetto della necessaria continenza espressiva» va considerato che gli insulti non rientrano nell'esercizio della libertà di espressione, anche nel dibattito politico, se incitano alla discriminazione. Le espressioni «gravemente infamanti e inutilmente umilianti», sicuramente offensive, non possono così godere della scriminante della critica politica e anzi, proprio nel caso di politici - che devono essere particolarmente attenti alla democrazia e all'impatto potenziale sulla società che può avere una dichiarazione d'odio – non può essere invocata la libertà di espressione o la critica politica. Anche il Parlamento europeo, d'altra parte, con decisione del 25 ottobre 2016, aveva respinto la richiesta in difesa dell'immunità invocata da Borghezio tanto più che le dichiarazioni rese nell'intervista radiofonica non avevano alcun collegamento diretto ed evidente con le sue attività di parlamentare[33].

La necessità di assicurare la punizione di coloro che fomentano discriminazione razziale e di genere è quindi maggiore nel caso di interventi di politici, diffusi quasi sempre su larga scala. A tal proposito, va ricordato che il CERD, già da tempo, ha raccomandato all'Italia di assicurare che ogni individuo «*including politicians at all levels, are held accountable*

[32] Cfr. G.E. Vigevani, *La libertà di manifestazione del pensiero*, in G.E. Vigevani - O. Pollicino - C. Melzi d'Eril - M. Cuniberti - M. Bassini, *Diritto dell'informazione e dei media*, Torino, 2019, 3 ss.; Id., *Libertà di espressione e discorso politico tra Corte europea dei diritti e Corte costituzionale*, in N. Zanon (a cura di), in *Le corti dell'integrazione europea e la corte costituzionale italiana*, Napoli, 2006, 459 ss.

[33] Si veda il documento P8_TA-PROV(2016)0397, reperibile nel sito *europarl.eu.int*.

and sanctioned for the dissemination of ideas based in racial superiority or hatred»[34]. Appare così evidente che l'immunità non può certo essere estesa a dichiarazioni discriminatorie rese da politici che non solo dovrebbero rappresentare un modello per la collettività, ma i cui discorsi sono largamente amplificati e diffusi. Ed invero, l'indicato Comitato, *«[it] also expressed deep concerns about racist discourse in politics…and the immunity that has shielded parliamentarians who have made racist remarks»*[35].

Pertanto, la pronuncia della Cassazione nel caso Borghezio, anche sotto questo profilo, è in perfetta sintonia con i principi e gli obblighi internazionali[36].

[34] CERD/C/ITA/CO/19-20, § 15.

[35] Doc. A/HRC/33/61/Add.1, §§ 38-39.

[36] Così, il § 4.1 della sent. 34815/19 e le sentenze lì richiamate.

Catch me if you can: CJEU safeguards the privacy of online copyright infringers in landmark decision *Constantin Film Verleih v YouTube*

Giulia Priora

Court of Justice of the European Union, 9 July 2020, Case C-263/19, Constantin Film Verleih GmbH v YouTube LLC and Google Inc

In Case C-264/19, the CJEU provides clarification on the interpretation of Art. 8 Directive 2004/48/EC, thus on the right of the copyright holder's right to acquire information about the origin and distribution networks of acts infringing his/her exclusive rights. By introducing the EU autonomous concept of "address", the Court excludes the possibility of disclosing phone numbers, email and IP addresses of infringing users, unless explicitly allowed by national law.

Summary

Keywords

EU copyright law - copyright enforcement - online platforms - right of information - name and address

1. Introduction

Copyright law in the EU is undergoing a particularly lively season, characterized by the adoption of the most recent Directive on Copyright in the Digital Single Market[1] as well as by landmark CJEU and national case law grappling with the need to balance copyright with other fundamental rights.[2] Against these developments, the discipline

[1] Directive EU 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

[2] Among the most recent decisions of the Court of Justice of the European Union, Case C-516/17, *Spiegel Online GmbH v Volker Beck* (2019) (*Spiegel Online*); Case C-469/17, *Funke Medien NRW GmbH v Federal Republic of Germany* (2019) (*Funke Medien*); Case C-476/17, *Pelham GmbH and others v Ralf Hütter and Florian Schneider-Esleben* (2019) (*Pelham*) and respective judgements rendered by the German Supreme Court. See, inter alia, T. Snijders – S. van Deursen, *The Road Not Taken. The CJEU Sheds Light*

has been shaken not only by thorough criticisms from the scholarship, but also by an increasingly heated public debate.[3]

Despite the great attention EU copyright law has attracted, some aspects of its evolution tend to be overlooked. This is mainly due to the complex nature of this branch of intellectual property law and the impervious road of its harmonization. The case here under analysis offers an interesting opportunity to shed light on problematic aspects related to the enforcement of copyright entitlements and, more specifically, on the interrelation between copyright and data protection, a point that in most recent debates has faded into the background.

2. Facts

The facts of the case are rather typical of the online environment. The dispute arose from the unauthorized upload on the well-known online platform YouTube of the full-length versions of two films distributed by the German company Constantin Film Verleih GmbH. The uploads occurred between 2013 and 2014. The visualizations of the uploaded videos, before the content was blocked by the platform, amounted to several thousands.

Following the manifest infringement of its exclusive rights, Constantin Film Verleih GmbH demanded US-based companies YouTube and Google to disclose information about the users involved in the upload of the films. After having received fictitious usernames and postal addresses, the German company further asked for IP addresses used for the upload of the infringing video, IP addresses used for the last access of the related accounts, email addresses and phone numbers of the account holders. YouTube and Google refused to disclose this additional information.

3. Legal context

Art. 8 Directive 2004/48/EC on the enforcement of intellectual property rights (En-

on the Role of Fundamental Rights in the European Copyright Framework. A Case Note on the Pelham, Speigel Online and Funke Medien Decisions, in *IIC*, 50, 2019, 1176 ss.; C. Sganga, *A Decade of Fair Balance Doctrine, and How to Fix it: Copyright Versus Fundamental Rights Before the CJEU from Promusicae to Funke Medien, Pelham and Spiegel Online,* in *EIPR,* 41(11), 2019, 672 ss.; G. Priora – B.J. Jütte, *No copyright infringement for publication by the press of politician's controversial essay*, forthcoming in *JIPLP,* 2020; B.J. Jütte – G. Priora, *Leaking of secret military reports qualifies as reporting of current events*, forthcoming in *JIPLP*, 2020.

[3] Among the countless scholarly contributions offering valuable insights on the subject, some make an effective and critical synthesis of the main developments, see S. Dusollier, *The 2019 Directive on Copyright in the Digital Single Market: Some Progress, a Few Bad Choices, and an Overall Failed Ambitions,* in *CMLR,* 57, 2020, 979 ss.; J.P. Quintais, *The New Copyright in the Digital Single Market Directive: A Critical Look*, in *EIPR,* 42(1), 2019, 28 ss.; B. Farrand, *"Towards a modern, more European copyright framework" or how to rebrand the same old approach?*, in *EIPR,* 41(2), 2019, 65 ss. Evidence of the significant public involvement in the copyright discourse can be found scattered in the reporting of the long negotiation process of the 2019 Directive, related protest outbreaks and stakeholders' reactions. See e.g. Deutsche Welle, *EU copyright bill: Protests across Europe highlight rifts over reform plans*, 23 March 2019; The Local, *Wikipedia Italy goes dark to protest EU copyright reform*, 3 July 2018.

forcement Directive) ensures the possibility for national judicial authorities to order the disclosure of information related to the origin and distribution channels of acts in violation of intellectual property rights, including "name and address" of the individual infringer.[4] The provision explicitly includes providers of commercial services used to perpetuate the infringement among the possible addressees of such an order.[5] Section 101 of the German Copyright Act (*Urheberrechtsgesetz*, UrhG) implements verbatim Art. 8 Enforcement Directive, thus enabling right holders who are victims of manifest copyright violations online to claim their right to information against the Internet service providers (ISPs)[6] and obtain names and addresses of producers, suppliers and previous holders of infringing copies, users of the services, intended wholesalers and retailers.[7]

The competent German Courts of all instances found the conditions for the exercise of the claimant's right to information to be satisfied. Nevertheless, controversial aspects arose in regarding which information had to be disclosed. The first instance Court (*Landgericht* Frankfurt am Main) rejected Constantin Film Verleih GmbH's request for IP addresses, email addresses and phone numbers of YouTube's users, while the Appeal Court (*Oberlandesgericht* Frankfurt am Main) approved the disclosure of email addresses, but not of the remainder. The case landed before the German Federal Supreme Court (*Bundesgerichtshof*), which referred it to the CJEU seeking clarification on whether the notion of "address" set in Art. 8 (2)(a) Enforcement Directive encompasses IP addresses, email addresses and phone numbers of copyright infringers. The CJEU rendered its judgement on 9 July 2020, rejecting all three types of information from the scope of the Enforcement Directive.

4. Analysis

The fact that some users relied on the services provided by YouTube and Google for the purpose of perpetuating manifest copyright infringements by way of unauthorized upload of protected audiovisual content is neither contested nor relevant to the question referred to the CJEU. In this sense, the ISP's obligation to provide information about the perpetuators upon request by a competent national judicial authority remains undisputed.[8] As highlighted above, the controversy and the related request for a preliminary ruling pivot on the question as to *which* information can be disclosed to

[4] Directive 2004/48/EC on the enforcement of intellectual property rights (Enforcement Directive), Art. 8(2)(a).

[5] Ivi, Art. 8(1)(c).

[6] German Copyright and Related Rights Act of 9 September 1965 as last amended in 2018 (UrhG), section 101(2), sentence 1, point 3.

[7] UrhG, section 101(3)(1).

[8] CGUE, Case C-264/19, *Constantin Film Verleih GmbH v YouTube LLC and Google Inc* (2020) (*Constantin Film Verleih*) § 27 («[P]ursuant to Article 8 of Directive 2004/48, the Member States must ensure that the competent courts may, in a situation such as that at issue in the main proceedings, order the operator of an online platform to provide the names and addresses of any person referred to in paragraph 2(a) of that article who has uploaded a film onto that platform without the copyright holder's consent»).

the copyright holder.

The notion of address

The CJEU's decision retraces to a large extent the arguments posited by Advocate General (AG) Øe.[9] Following his Opinion, the Court asserts that the notion of "address" set in Art. 8 Enforcement Directive is to be interpreted as an autonomous concept of EU law[10] and understood as referring to postal address.[11] The reasoning is structured as follows. The lack of references to the law of the Member States to determine the meaning and scope of the term "address" in Art. 8(2)(a) Enforcement Directive as well as its missing definition in the same Directive lead the CJEU to attribute an independent and uniform interpretation based on (i) the common everyday understanding of the notion, (ii) the context and (iii) purposes of the rules that include it.[12]

The usual understanding of the term "address" is found to be "the place of a given person's permanent address or habitual residence", thus not covering email address, phone number and IP address.[13] The historical analysis of the Enforcement Directive supports this argument, as nothing in its *travaux préparatoires* and explanatory documents suggests a meaning of "address" that would include the additional data requested by Constantin Film Verleih.[14]

The CJEU further looks at the context in which the term is used, scrutinizing other relevant sources of EU law[15] and highlighting how the EU legislator consistently refers to email addresses and IP addresses using the respective specific terms, instead of the generic notion of address.[16] The restrictive interpretation of this term is found to be in line also with the general objective of the Enforcement Directive, that is to provide an effective remedy to the copyright holder enabling him/her to identify the infringement perpetuators, but, at the same time, to do so by way of a minimum harmonization.[17]

Copyright vs. data protection

In the conclusive part of the decision, the CJEU does not miss the opportunity to

[9] AG Opinion, Case C-264/19, *Constantin Film Verleih GmbH v YouTube LLC and Google Inc* (2020) (AG Opinion in *Constantin Film Verleih*).

[10] *Constantin Film Verleih,* cit., §§ 28-29; AG Opinion in *Constantin Film Verleih,* cit., § 28.

[11] *Constantin Film Verleih,* cit., §§ 30-33; AG Opinion in *Constantin Film Verleih,* cit., §§ 27, 30-39.

[12] The structure of the reasoning is typical to the CJEU's case law on autonomous concepts of EU law. See e.g. *Spiegel Online,* cit., §§ 62-65; Case C-467/08, *Padawan SL v Sociedad General de Autores y Editores de España,* (2010), § 32.

[13] *Constantin Film Verleih,* cit., § 30. See also AG Opinion in *Constantin Film Verleih,* cit., §§ 30-33.

[14] *Constantin Film Verleih,* cit., § 31. See also AG Opinion in *Constantin Film Verleih*, cit., §§ 37-39.

[15] I.e. Regulation (EC) 987/2009 laying down the procedure for implementing Regulation (EC) 883/2004 on the coordination of social security systems, Regulation (EU) 524/2013 on online dispute resolution for consumer disputes, Directive 2014/24/EU on public procurement, Directive (EU) 2015/2366 on payment services in the internal market, Directive 2014/41/EU regarding the European Investigation Order in criminal matters, Regulation (EU) 2017/1128 on cross-border portability of online content services in the internal market, Regulation (EU) 2018/1240 establishing a European Travel Information and Authorisation System.

[16] *Constantin Film Verleih,* cit., § 33. See also AG Opinion in *Constantin Film Verleih,* § 35.

[17] *Constantin Film Verleih,* cit., §§ 34-36.

stress the intention underlying the Enforcement Directive and EU copyright law in general, that is to strike a *fair balance* between, on the one side, the protection of copyright holders and, on the other, of users and the public interest.[18]

While this balancing exercise often sees the juxtaposition of the right to intellectual property *ex* Art. 17(2) Charter of the Fundamental Rights of the EU (CFREU) and the right to expression and information *ex* art. 11 of the same Charter,[19] in the case at stake the clash is between the copyright holder's right to information and the protection of users' personal data as safeguarded by Art. 8 CFREU.[20] The friction between copyright and data protection emerging from Art. 8 Enforcement Directive was already tackled by the CJEU in a 2015 decision in Case *Coty Germany*.[21] In both judgements, the Court emphasizes the need to reconcile these opposing fundamental rights and achieve a fair balance.[22]

A margin of uncertainty remains as to who shall ensure this balance and on the basis of which criteria. The AG in his delivered Opinion advances the idea that «the EU legislature alone has the competence to strike that balance»[23] Yet, according to settled case law of the CJEU, national Courts shall interpret national laws in a manner consistent with the protection of EU fundamental rights and general principles of EU law.[24] Lastly, the Enforcement Directive itself makes national Parliaments bound to achieve this balance by allowing Member States to grant a more extensive right to information to copyright holders[25], provided that a reasonable balance between fundamental rights is struck and the principle of proportionality respected.[26]

5. Conclusive remarks and practical significance

It is common ground that, upon a claimant's justified and proportionate request, a judicial authority can order an ISP to provide information about users who upload copyright infringing content on its platform. The CJEU was asked to intervene to

[18] Ivi, § 37. See also AG Opinion in *Constantin Film Verleih,* cit., § 51 («[I]t must be borne in mind that Directive 2004/48, like all legislation on intellectual property, strikes a balance between, on the one hand, the interest of holders in protecting their intellectual property right, enshrined in Article 17(2) of the Charter and, on the other, the protection of the interests and fundamental rights of users of protected subject matter, and the public interest»).

[19] See e.g. *Spiegel Online, Funke Medien, Pelham*, cit., and CJEU Case C-145/10, *Eva-Maria Painer v Standard VerlagsGmbH and Others* (2013).

[20] See in this regard Enforcement Directive, recital 2, asserting that the protection of intellectual property «should not hamper […] the protection of personal data, including on the Internet».

[21] CJEU Case C-580/13, *Coty Germany GmbH v Stadtsparkasse Magdeburg* (2015) (*Coty Germany*). See also *Constantin Film Verleih,* cit., § 38.

[22] *Coty Germany,* cit., §§ 28, 34-35; *Constantin Film Verleih,* cit., § 38. See also AG Opinion in *Constantin Film Verleih*, cit., § 54.

[23] AG Opinion in *Constantin Film Verleih,* cit., § 58.

[24] See e.g. *Coty Germany*, cit., § 34; CJEU Case C-275/06, *Productores de Música de España v Telefónica de España SAU* (2008) *(Promusicae),* § 70.

[25] Enforcement Directive, Art. 8(3)(a).

[26] *Constantin Film Verleih,* cit., § 39.

clarify how a fair balance between copyright and data protection can be achieved in such a disclosure.

By declaring that email addresses, telephone numbers and IP addresses fall beyond the scope of Art. 8 Enforcement Directive, the CJEU attributes a romantic nuance to the notion of address, favoring the postal address as appropriate understanding of the term and safeguarding the privacy of online users when it comes to other personal data. This argument could be criticized as overly formalistic and outdated, especially with regards to email addresses, which have joined and, to a large extent, replaced the physical address in the everyday language.[27] Moreover, considering the fact that legal norms regularly require dynamic interpretations to fit in with ongoing changes in circumstances and technology,[28] it is worth to point out that all sources of EU law scrutinized by the CJEU in order to contextualize the use of the term "address" were adopted after 2009. As the Enforcement Directive is an older piece of legislation, the need for an up-to-date reading of its provisions seems more than legitimate.

Besides the questionable interpretation of the notion of address, the CJEU's reasoning offers valuable insights on the way the opposing fundamental rights at stake are to reconcile. The significance of the judgement in this regard is twofold.

On the one hand, the firm rejection of the teleological interpretation[29] gives food for thoughts regarding the inconsistent deployment of this tool in CJEU's judicial reasoning on copyright matters. In fact, the literal interpretation provided not only leaves room for ambiguity, as seen above, but also leads to wonder how come the often evoked objective of high level of protection is pushed into the background.[30] This is particularly evident in the line of argument building the EU autonomous concept of address, whereby the specific purpose pursued by Art. 8 Enforcement Directive, i.e. to provide an effective remedy by enabling right holders to identify infringers, is significantly underemphasized.[31] In this light, the reasoning might have benefited from a further elaborated and more explicit engaging with the objectives underlying the protection of personal data as defined in Art. 4(a) Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR). This would not have been an unprecedented restrictive interpretation of the purpose of high level of protection[32] and might have

[27] See also E. Rosati, *An address by any other name? AG Øe advises CJEU to rule that 'address' does not include email and IP addresses*, in *The IPKat*, 15 April 2020.

[28] See, inter alia, AG Opinion, Case C-174/15, *Vereniging Openbare Bibliotheken v Stichting Leenrecht* (2016) (*Vereniging Openbare Bibliotheken*), §§ 25-32.

[29] Suggested by the complainant, see AG Opinion in *Constantin Film Verleih,* cit., §§ 41-47.

[30] See Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society (InfoSoc Directive), recitals 2 and 4. Inter alia, CJEU, Case C-5/08,, *Infopaq International A/S v Danske Dagblades Forening* (2009), § 40; Joined Cases C-403/08, *Football Association Premier League Ltd and Others v QC Leisure and Others* and C-429/08, *Karen Murphy v Media Protection Services Ltd* (2011), § 186; Case C-419/13, *Art & Allposters International BV v Stichting Pictoright* (2015), § 47; *Funke Medien,* cit., § 50; *Pelham,* cit., § 30; *Spiegel Online,* cit., § 35; AG Opinion in *Vereniging Openbare Bibliotheken,* cit., § 33.

[31] *Constantin Film Verleih,* cit., §§ 35-36.

[32] See, for instance, the restrictive interpretation of the exclusive right to distribution, in which the objective of high level of protection was found not to be relevant under the circumstances at stake. CJEU Case C-456/06, *Peek & Cloppenburg KG v Cassina SpA* (2008), §§ 37-38.

helped bringing systematic consistency to the copyright case law at EU level.
On the other hand, the judgement displays an interesting sensitivity towards the protection of rights and interests of online users. Whereas it may be trite to remind that copyright protection is neither absolute nor inviolable[33] and the fundamental rights implications are proving the thorny barrier to its interpretation, it is worth stressing how in the decision here analyzed the case for a stronger protection of users' personal data successfully made its way through the impervious fair balance exercise by way of a straightforward literal and contextual interpretation of EU law.

[33] See e.g. *Promusicae,* cit., §§ 62-70; *Funke Medien,* cit., § 72; *CJEU,* Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA v Netlog NV* (2012), § 41; Case C-461/10, *Bonnier Audio AB and Others v Perfect Communication Sweden AB* (2012), § 56; Case C-201/13, *Johan Deckmyn and Vrijheidsfonds VZW v Helena Vandersteen and Others* (2014), § 26; AG Opinion in *Constantin Film Verleih*, cit., § 52.

Airbnb and Uber: two sides of the same coin

Erion Murati

Court of Justice of the European Union, 19 December 2019, C-390/18, *Ahtop v. Airbnb Ireland*

Art. 2(a) of Directive 2000/31/EC, which refers to Art. 1(1)(b) of Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, must be interpreted as meaning that an intermediation service which, by means of an electronic platform, is intended to connect, for remuneration, potential guests with professional or non-professional hosts offering short-term accommodation, while also providing a certain number of services ancillary to that intermediation service, must be classified as an "information society service" under Directive 2000/31.

Summary

Keywords

Online Platforms – Uber – Airbnb - Internal Market – E-Commerce

1. Introduction

Has Airbnb, in the context of its activity, created an offer with the meaning of the judgments in *Uber Spain* and *Uber France*?[1]

Online platforms, mainly due to sectors digitalization[2], are transforming marketplaces as they create new multi-sided markets connecting service providers and users, in a way that generates new network effects and distributes them among the participants in the ecosystem[3]. By dramatically reducing transaction costs and enabling coordinated transaction globally, platforms are disrupting the existing balance between customers

[1] Opinion AG Szpunuar, Case C-390/18, *Airbnb Ireland vs. Association pour un Hébergement et un Tourisme Professionnel (AHTOP)* (2019), § 55 hereinafter only "Opinion".

[2] Digitalization takes the form of the creation of a data layer on top of the physical world. Sensors extract data from the physical world (from computers, from smartphones, from Internet of Things sensors, etc.) and a parallel virtual map of the world is constructed. Artificial intelligence (AI) makes it possible to automate the management of the large amount of data extracted from reality.

[3] J. Montero, *Regulating Transport Platforms: The Case of Carpooling in Europe*, in M. Finger – M. Audoin (eds.), *The Governance of Smart Transportation Systems*, Dordrecht - Heidelberg - London - New York, 2019, 13 ss.

and suppliers. Existing regulatory framework fail to coherently address this paradigm shift that blurs established lines between traditional legal categories, such as business and consumer, personal and professional, and worker and contractor. Traditional EU regulation, which focus mainly on balancing the interest of two contracting parties, is now confronted with a triangular relationship between a platform, a supplier and a user. Legislators, judges and lawyers across the globe are struggling to determine the legal status of online intermediaries[4]. Therefore, one of the first regulatory challenge around online platforms is to define their legal status[5]: mere facilitator, broker or supplier of integrated service? If platforms do not provide a merely intermediation service, instead, they provide material services (i.e. transportation, accommodation etc) then, often is required a license and full liability for their provisions towards users. In general, online platforms are not designed to provide their own accommodation or transport services, but to facilitate the contracting of services provided by third parties. However, the intermediation service provided by platforms is particularly powerful. Indeed, even the notion of internet intermediaries, defined by the OECD[6] as entities that «bring together or facilitate transactions between third parties on the Internet», is increasingly replaced in common parlance by the more palatable term of "platform", which evokes a role that goes beyond one of mere messenger or connector, and extends to the provision of a shared space defined by the applications within which users can carry out their activities and generate value[7].

Acting as an intermediary has several advantages for the platform[8] and it is usually expressed in the platform operator's terms of service. Nevertheless, it's doubtful whether such a declaration is sufficient for reducing the role of the platform to an intermediary. The EU Commission had underlined that whether an online platform also provides the underlying service has to be established on a case by case basis[9]. Among protesters, traditional transport operators, in particular, have challenged before Courts all around Europe the legality of transport platforms, accusing them for unfair competition. This has certainly been the case of Uber, but also of BlaBlaCar in a specific market: Spain.

---

[4] See preface, B. Deveolder (ed.), *The Platform economy unravelling the legal status of online intermediaries,* New York, 2018.

[5] See G. Resta, *Digital platforms under Italian law*, in U. Blaurock – M. Schmidt-Kessel - K. Erler (eds.), *Plattfomen*, Baden-Baden, 2018, 97 ss.

[6] See OECD, *The economic and social role of Internet intermediaries*, at *oecd.org,* 9.

[7] L. Belli – N. Zingales, *Online Platforms' Roles and Responsibilities: a Call for Action*, in L. Belli – N. Zingales (eds.), *Platform regulations: how platforms are regulated and how they regulate us,* FGV Direito Rio, 2017, 25 ss.

[8] a) The electronic intermediary service will benefit from the principle of freedom to provide services as guaranteed in EU legislation — Article 56 TFEU and Directives [2006/123] and [2000/31]; b) they cannot be held responsible for any ill-execution of the underlying contract (service) or for damage accruing therefrom under Art. 3 E-Commerce directive; and c) they can claim to be fully absolved from any liability, including for misrepresentation, offensive or illegal content, under Articles 13,14. 15 of the E-Commerce Directive.

[9] The key criteria to be considered are: a) the circumstance that the collaborative platform sets the final price to be paid by the user; b) the fact that the platform sets other key contractual terms; and c) the fact that the platform owns the key assets used to provide the underlying service. See European Commission, *A European agenda for the collaborative economy*, COM(2016) 356, 6.

BlablaCar, a ridesharing company[10] has been held by the Madrid Commercial Tribunal to be a mere intermediary, not in competition with traditional coach and train service[11]. The European Commission guidelines on platform economy, found a concretisation in the CJEU *Uber Spain* judgement of 20 December 2017, where the Court declared that an intermediation service such as UberPOP must be classified as "a service in the field of transport" within the meaning of EU law[12]. Uber Spain was memorable for introducing a new test for determining whether an online platform provides an information society service caught by the *lex specialis* of the E-Commerce Directive or whether it provides a composite service governed by general EU law on the freedom to provide services (or not, if the service relates to transport)[13]. Almost two years after Uber decision, the focus of the regulatory battle shifted towards short term rental platforms[14]. Similar to Elite Taxi, in Airbnb Ireland, an association of real estate brokers based in Paris challenged the fact that Airbnb advertises rental opportunities online without having been duly authorized to do so through a professional card. Its delivery is subject to the fact that an applicant has a demonstrable professional qualification, provide financial guarantees and have professional liability insurance. Of course, Airbnb and, above all, its hosts have none. Airbnb contests that these restrictions are not applicable to the extent that its activities fall within the scope of the E-Commerce Directive. Thus, following - or departing - from the Uber judgement, the CJEU was required to rule on whether Airbnb is a market maker not limited to matching demand and supply, but engaged in offering the underlying service as well. By its judgment of 19 December 2019, the Grand Chamber of the Court[15] held that Airbnb's intermediation service is an information society service regulated under Directive 2000/31 on electronic commerce[16]. Unlike UberPop, in Airbnb ECJ took a different view which will have some important implications on the debate of how to regulate platform economy in general. Recently, another request for a preliminary ruling has reached ECJ from the highest Italian administrative Court *Consiglio di Stato*[17]. Luxemburg judges are called this time to assess the compatibility with EU law of the so called "Airbnb law"[18].

---

[10] Which matches individuals driving to some long-distance destination with other individuals wishing to go to that same destination.

[11] The Commercial Court in Madrid decided that BlaBlaCar was only mediating in the provision of the carpooling service, and furthermore, that the underlying carpooling services mediated by BlaBlaCar are private services that can be provided with no license as the price is below EUR 0.19/km, the legal reference to reimburse expenses to civil servants when traveling with their own car; that is, the service is being provided with no profit. See *Confesbus v Blablacar* SJM M 6/2017 (2 February 2017) ES:JMM: 2017:364.

[12] CJEU Case C-434/15, *Elite Taxi vs. Uber* (2017).

[13] See M. Finck, *Distinguishing internet platforms from transport services*, in *CMLR*, 55, 2018, 1619 ss.

[14] See C. Busch, *The Sharing Economy at the CJEU: Does Airbnb pass the 'Uber test'? Some observation on the pending case C-390/18 - Airbnb Ireland*, in *EuCML*, 7, 2018, 172 ss.

[15] CJEU Case C-390/18, *Airbnb Ireland vs. AHTOP* (2019).

[16] 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 (hereafter "E-Commerce Directive").

[17] Council of State (Consiglio di Stato), sez. IV, order (*ordinanza)* 11 July – 18 September 2019, no. 6219.

[18] See Art. 4, paras. 4, 5 and 5-bis, Law Decree 24 April 2017, no. 50 ("*Disposizioni urgenti in materia*

2. The Airbnb Ireland

Like other platform services, Airbnb has become a favourite of digitally savvy consumers who know that some of the greatest benefits of our globalizing society can be found online. Offering a platform through which hosts can advertise their apartments to potential guests worldwide, Airbnb provides a real, and in many ways attractive, alternative to visitors who are looking for something else than a hotel room[19]. Hosts as well as guests can only make use of Airbnb's website for bookings once they have registered as users. Guests can contact hosts through their listings to make a reservation. The site makes it possible to send messages to hosts to request further information and, if desired, to negotiate further terms about the rental. Once host and guest agree on a booking, the guest can confirm the booking and pay for it through the Airbnb website. Airbnb holds the payment in escrow until the guest has arrived at the accommodation and releases it to the host 24 hours after the guest checks in. For its services, Airbnb charges hosts and guests a commission fee which constitute the main income that Airbnb itself makes from the website and enable the company to make a profit. The emergence of Airbnb comes with some clear benefits, but it also entails undeniable economic, social and environmental drawbacks which have given authorities in different countries[20] the need to come up with balanced legislation that considers the various interests at play (lessors, tourists, neighbours, residents).

2.1. Factual and legal background

On 24 January 2017, Association *pour un hébergement et un tourisme professionnel* (Ahtop) lodged a complaint with the *Tribunal de grande instance* of Paris about the commercial practices of Airbnb. Ahtop claimed that Airbnb violates Arts. 3 and 5 of the Hoguet law, which regulates the activities of real estate brokers. Under Art. 3(1) of the Hoguet law real estate brokers are required to have a professional card issued by the local chamber of industry and commerce. The card is only issued to applicants who demonstrate their professional qualification, provide a satisfactory financial guarantee and have a professional liability insurance[21]. Moreover, Art. 5 of the Hoguet law requires real estate brokers to keep a register which contains a documentation of payments received by their clients. A violation of the above requirements constitutes a criminal act under the Hoguet law and can result in imprisonment and fines[22]. In response to the

finanziaria, iniziative a favore degli enti territoriali, ulteriori interventi per le zone colpite da eventi sismici e misure per lo sviluppo").

19 V. Mak, *Private Law Perspectives on Platform Services': Airbnb: Home Rentals between AYOR and NIMBY*, in *EuCML*, 5, 2016, 19 ss.

20 See A.I. Nadal, *Regulating Airbnb in Spain*, in *EuCML*, 8, 2019, 42 ss.; C. Busch, *Regulating Airbnb in Germany – status quo and future trends*, in *EuCML*, 8, 2019, 39 ss.; E. Terryn, *The sharing economy in Belgium – a case for regulation?*, in *EuCML*, 5, 2016, 45 ss.; M. Bartoloni, *Stop ai «furbetti» degli affitti brevi: Airbnb dovrà riscuotere la cedolare*, in *Il Sole 24 Ore*,18 February 2019.

21 Opinion, § 9.

22 Ivi, § 9.

complaint by Ahtop, the Public Prosecutor's Office brought a criminal action against Airbnb Ireland for violating the Hoguet law. In its defence[23], Airbnb argued, that its commercial activities do not qualify as real estate brokerage and that the Hoguet law does not apply because it is incompatible with the E-Commerce Directive[24]. Ahtop, which joined the criminal proceedings as "parte civile", in turn, argued that the commercial activities of Airbnb do not fall under E-Commerce Directive because they are not limited to connecting two parties via a platform, but include additional services which are characteristic of the real estate business[25]. Against this background, the Tribunal de grande instance de Paris on 7 June 2018 sent a request for a preliminary ruling to the CJEU and asked the following two questions: 1) Do the services provided in France by Airbnb Ireland via its electronic platform, which is operated from Ireland, fall under the freedom of services guaranteed by Art. 3(2) of Directive 2000/31/EC? 2) Can the restrictive provisions concerning the profession of the real estate brokers under Act No. 70-9 of 2 January 1970 (the Hoguet law) be invoked against Airbnb Ireland?

2.2. Opinion of Advocate General Szpunar

Advocate General Szpunar delivered his opinion on 30 April 2019. In order to answer the first question, he first made a few general observations about Airbnb Ireland's activities[26] and if those activities fall within the concept of "information society service"[27]. He noted that the Airbnb's service is an electronic service provided at a distance (the intermediation function and payment) while the accommodation itself is not[28]. Therefore, in order to clarify the division line he turned to UberPop, where CJEU had already been requested to rule on the classification of mixed services (online vs. material), establishing the criterion of new market creation and the exercise of decisive influence over it[29]. According to AG Szpunar, as to the first criteria, of whether Airbnb has created an offer within the meaning of the Uber judgments, the question must be answered negatively for the following reasons[30]. First, unlike UberPop's platform, Airbnb Ireland's platform is open to professional hosts and non-professional

[23] The Czech and Luxembourg Governments and the Commission share the same view; Opinion, § 22.

[24] Ivi, § 15.

[25] On the other hand, French and Spanish Governments supported this different position; Opinion, § 23.

[26] Ivi, §§ 25 to 33.

[27] An information society service is defined by art. 1(2) of Technical Standards Directive «as a service (i) provided for remuneration, at a distance, by electronic means (ii) and at the individual request of a recipient of services (iii)». As he already observed in UberPop, the first and the third leg of the test did not appear problematic and focused in the second leg as far as here «the line between the component of the services that is provided by electronic means and that which is not so provided is sometimes blurred». See Opinion, § 37.

[28] Ivi, § 41.

[29] Ivi, § 44.

[30] Ivi, § 56.

hosts. Second, the accommodation services are not inseparably linked to the service provided by Airbnb Ireland by electronic means, in the sense that they can be provided independently of that service and they retain their economic interest[31].

Having answered negatively to the first criterion, the next step was to determine whether Airbnb Ireland exercises control over the conditions governing the provision of the short-term accommodation services. AG Szpunar stressed that the criterion relating to the creation of a supply is merely an indication of whether a service provided by electronic means forms an inseparable whole with a service having a material content, instead, «it is the decisive influence exercised by the service provider over the conditions of the supply of the services having material content that is capable of rendering those services inseparable from the service that that provider provides by electronic means»[32]. Consequently, it cannot be concluded that Airbnb Ireland's electronic service satisfies the criterion relating to the exercise of control over the accommodation services for the following reasons. First, Airbnb Ireland does not exercise «control over all the economically significant aspects of the short-term accommodation service, such as price, the location and standards of the accommodations»[33]. Second, the fact that Airbnb also offers other services, namely a photography service, civil liability insurance and a guarantee for damage, does not prevent Airbnb from being classified as an "information society service", «provided that those other services are not inseparable from the service provided by electronic means, in the sense that the latter service does not lose its economic interest and remains independent of the services having a material content»[34]. Therefore, as a matter of EU law, a service consisting in connecting, via an electronic platform, potential guests with hosts offering short-term accommodation, in a situation where the provider of that service does not exercise control over the essential procedures of the provision of those services, constitutes an information society service within the meaning of Art. 2(a) of E-Commerce Directive.

As regards to the second question, namely, whether the Hoguet Law is enforceable against Airbnb Ireland, the Advocate General observed that Airbnb activity falls *prima facie* within the scope E-Commerce Directive and in order for a requirement, laid down by a Member State other than that in which the provider of the information society services is established, to be enforceable against that service provider and to result in the restriction of the free movement of those services, that requirement must be a measure that satisfies the substantive and procedural conditions laid down by that directive (Art. 3(4)(a)(b)[35]. In other terms, Art. 3(1) of Directive 2000/31 imposes on the Member States of origin the obligation to ensure that the information society services provided by a service provider established in their territories comply with the national provisions applicable in those Member States that fall within the coordinated

[31] And, as the Luxembourg Government observed, professional and non-professional hosts can offer their assets via more traditional channels or they may create a website devoted solely to their accommodation that can be found with the help of search engines. Ivi, §§ 58-59.

[32] Ivi, § 67.

[33] Ivi, § 71.

[34] Ivi, § 85.

[35] Ivi, §§ 123 to 146.

field[36]. In contrast with that general obligation, in order not to "dilute" the principle of freedom to provide information society services (Art. 3(1) of Directive 2000/31), Art. 3(4) of that directive might be understood as authorising Member States other than the Member State of origin to derogate from the free movement of services only in an indirect manner. Accordingly, in the light of the substantive requirements[37] laid down by E-Commerce Directive in Art. 3(4)(a) the AG Szpunar took the view that a Member State other than the Member State of origin «may derogate from the free movement of information society services only by measures taken on a "case-by-case" basis»[38] and the measures adopted shall not concern the information society services *per se* but a *given* service. He avoided to enter into the merit of whether if the Hoguet law satisfies these substantive conditions required by E-commerce Directive in Art. 3(4)(a) for three reasons. First, France itself did not provided any evidence that the substantive conditions are fulfilled by the concerned national law[39]. Second, in any case «the requirements laid down by the Hoguet law raise doubts as to their proportionality»[40]. Finally, it is for the national court to determine whether, having regard to all the factors brought to its attention, the measures at issue are necessary in order to ensure the protection of consumers and are also proportionate to those objectives[41].

On the other hand, procedural conditions (Art. 3(4)(b) of E-Commerce) require that a Member State which proposes to adopt measures restricting the free movement of information society services originating in another Member State must first notify the Commission of its intention and ask the Member State of origin to take measures in respect of information society services[42]. According to Advocate General these two procedural conditions were not fulfilled by France[43] and, consequently, that failure to notify entails the sanction of unenforceability of a measure against the provider of those services[44] – Airbnb Ireland.

---

[36] In the words of Art. 2(h) of Directive 2000/31: «"coordinated field": requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them. The coordinated field concerns requirements with which the service provider has to comply in respect of: a) the taking up of the activity of an information society service, such as requirements concerning qualifications, authorisation or notification; b) the pursuit of the activity of an information society service, such as requirements concerning the behaviour of the service provider, requirements regarding the quality or content of the service including those applicable to advertising and contracts, or requirements concerning the liability of the service provider».

[37] It follows from Art. 3(4)(a)(i) of Directive 2000/31 that derogations from the free movement of information society services are permitted, in particular, when they are *necessary* for reasons relating to public policy, the protection of public health, public security or the protection of consumers.; it must be taken against an information society service which actually undermines those objectives or constitutes a serious and grave risk to those objectives and it must be *proportionate* to those objectives.

[38] Opinion § 135.

[39] Ivi §§ 127-129.

[40] Ivi, § 136.

[41] Ivi, § 137.

[42] Ivi, § 138.

[43] Ivi, §§ 139-140.

[44] Ivi, §§ 150-151.

2.3. Judgement of the Court

The Grand Chamber of the Court[45] concurred with Advocate General Szpunar, classifying Airbnb's intermediation service as an information society service regulated under E-Commerce Directive. The Court considered a number of elements to determine that the main component of the service provided by Airbnb Ireland is intermediation service. First, the Court underlined that, in principle, Airbnb's service intermediation satisfies all the conditions, laid down in Art. 1(1)(b) of Directive 2015/1535, to which Art. 2(a) of E-Commerce Directive refers, as an "information society service", distinct from the subsequent service to which it relates[46]. However, this will not be the case «if it appears that that intermediation service forms an integral part of an overall service whose main component is a service coming under another legal classification» (i.e. UbePop)[47]. Second, to underline the separate nature of such intermediation service in relation to the accommodation services to which it relates, the Court noted, that Airbnb services consists essentially of providing a tool for presenting and finding accommodation for rent, - facilitating the conclusion of future rental agreements - and that constitutes the essential feature of the electronic platform managed by Airbnb Ireland. Consequently, Airbnb services «constitutes a service which cannot be regarded as merely ancillary to an overall accommodation service»[48] and «it is in no way indispensable to the provision of accommodation services, since the guests and hosts have a number of other channels in that respect, some of which are long-standing»[49]. Third, the Court stated that there was nothing in the file to indicate that Airbnb sets or caps the amount of the rents charged by the hosts using that platform. At most, «it provides them with an optional tool for estimating their rental price having regard to the market averages taken from that platform, leaving responsibility for setting the rent to the host alone»[50]. In addition, the other services offered by Airbnb Ireland are «merely ancillary to the intermediation service provided by that company»[51]. Therefore, «unlike the intermediation services at issue in the Uber Spain judgments, neither that intermediation service nor the ancillary services offered by Airbnb Ireland make it possible to establish the existence of a decisive influence exercised by that company over the accommodation services to which its activity relates, with regard both to determining the rental price charged and selecting the hosts or accommodation for rent on its platform»[52]. In a nutshell, for the Court, Airbnb is solely a virtual market place, matching demand and supply, thus having no control whatsoever over hosts and guests.

By its second question, the referring court asks the Court of Justice whether the

[45] CJEU Case C-390/18, *Airbnb Ireland*, cit (hereinafter the "Judgment").

[46] Ivi, § 49.

[47] Ivi, § 50.

[48] Ivi, § 54.

[49] The Court referred to estate agents, classified advertisements, whether in paper or electronic format, or even property lettings websites, see § 53 and § 55.

[50] Ivi, § 56.

[51] Ivi, §§ 57 to 64.

[52] Ivi, § 68.

Hoguet legislation is enforceable against Airbnb Ireland. In other terms, whether Art. 3(4) of Directive 2000/31 must be interpreted as meaning that, in criminal proceedings with an ancillary civil action, an individual may oppose the application to him or her of measures of a Member State restricting the freedom to provide an information society service which that individual provides from another Member State, where those measures do not satisfy all the conditions laid down by that provision. The Court recognized that Hoguet law is restrictive of the freedom to provide information society services and the fact that that law predates the entry into force of Directive 2000/31 cannot have had the consequence of freeing the French Republic of its notification obligation[53]. The notification obligation is a mechanism for monitoring that the freedom to provide information society services between Member States is limited only according to the given exceptions. Therefore, «a Member State's failure to fulfil its obligation to give notification of such a (restriction) measure may be relied on by an individual, not only in criminal proceedings brought against that individual, but also in a claim for damages brought by another individual who has been joined as civil party[54]». As concerning the second question, the Court, unlike AG Szpunar, did not enter at all into the discussion of whether the Hoguet Law satisfied the substantial conditions required by E-Commerce Directive. To rule for the Court was sufficient to note that France did not met none of the procedural conditions laid down by the E-Commerce Directive.

3. Analyse and comment

In Airbnb Ireland, the ECJ has delivered an important judgement on the law applicable to Airbnb but more in general to online platforms. The Court has answered to a question asked also by academics, namely, what is the platform operator's role: mere facilitator, broker or supplier of integrated services?[55] To put it in EU internal market terms, do online platforms provide an information society service and do they also supply an underlying service in the end?[56] If platforms do not provide a merely intermediation service, instead, they provide material services (i.e. transportation, accommodation etc) then, often is required a license and full liability for their provisions towards users. Unlike UberPop, in the Airbnb the Court confirmed that it provides an intermediation service which must be classified as an "information society service"

[53] Ivi §§ 81 and 87.

[54] Ivi, § 100.

[55] Any discussion of the legal issues raised by digital platforms faces at the outset two main difficulties. The first is the lack of a clear and widely shared definition of what a digital platform is. The second is the stark heterogeneity of the issues involved, which are not limited to a single discipline, but lie at the interface of different branches of the legal system, like consumer law, competition law, administrative law, labour law, data protection, etc. See G. Resta, *Digital platforms under Italian Law*, cit., 100; see K. Sein, *Legal problems of electronic platform economy – Estonian perspective*, in U. Blaurock – M. Schmidt-Kessel - K. Erler (eds.), *Plattformen,* cit., 80; see preface by B. Deveolder (ed.), *The Platform economy unravelling the legal status of online intermediaries,* cit.

[56] See M. Inglese, *Regulating the Collaborative Economy in the European Union Digital Single Market,* Heidelberg - New York - Dordrecht – London, 2019, 20.

regulated under E-Commerce Directive. Accordingly, the law of the state of establishment applies (Ireland) and the recipient states (France and the rest) can only impose restrictions on a limited number of general interest grounds, restrictions have to pass a proportionality test and they have to be notified to the Commission and the state of establishment. Thus, Airbnb benefit from free movement principles and can be required only to obeys the laws of the state where it is established. The significance is considerable. Being subject to the laws of 27 different countries could mean substantial additional administrative and legal costs.

3.1. Airbnb as market maker

The first criteria of the "Uber test" is whether a digital platform is a market maker. According to ECJ[57] and AG Szpunar[58] Airbnb provides merely a digital distribution channel which is open to all categories of hosts and the accommodation services are not inseparably linked to the service provided by Airbnb Ireland by electronic means, in the sense that they can be provided independently of that service and they retain their economic interest. To AG Szpunar, Airbnb does not defer from online intermediaries for the purchase of flights or hotel bookings as «the supply made by the intermediary represents real added value for both the user and the trader concerned, but remains economically independent since the trader pursues his activity separately»[59]. As business ideas, both ridesharing and accommodation letting have been around for some time. But in both models a new digital platform has revolutionised their scale and success. The "economic interest" in both cases actually lies in the efficiency and popularity of the platform – not whether the users of the platform could operate independently of it[60]. Further, platforms like Airbnb extend the market for residential accommodation and create a new supply of short-term rentals that would not exist without those platforms. Indeed, it is an essential element of the business model of sharing economy platforms to overcome the transaction costs, the trust and reputational barriers that, in the past, restricted sharing activities. From this perspective, Airbnb can be considered a market maker[61]. However, as AG Szpunar underlined, «it is not sufficient that a service provider creates a new supply of services that are not provided by electronic means [...] the creation of those services must be followed by the maintenance, under the control of that provider, of the conditions under which they are provided»[62]. In other terms, «it is the decisive influence exercised by the service provider over the conditions of the supply of the services having material content that is capable of rendering those ser-

[57] Judgement, § 55.

[58] See Opinion, § 58.

[59] AG Opinion, Case C-434/15, *Asociación Profesional Elite Taxi v Uber Systems Spain* (2017), § 34.

[60] For an overview see D. Poyton, *What makes Uber and Airbnb different in the eyes of the EU – and why it matters*, in *theconversation.com,* 20 December 2019.

[61] See C. Busch, *The Sharing Economy at the CJEU*, cit., 173.

[62] Opinion § 65.

vices inseparable from the service that that provider provides by electronic means»[63].

3.2. Airbnb does not exercise "decisive influence" over the accommodation service

The second criterion of the "Uber test" is whether the platform operator exercises "decisive influence" over the provision of the underlying services. According to AG Szpunar[64], first, and confirmed by ECJ, later, Airbnb Ireland does not exercises decisive control over all the economically significant aspects of the short-term accommodation service, such as price, the location and standards of the accommodations[65]. In addition, «the provision of other services offered by Airbnb Ireland are optional in nature by comparison with the service provided by electronic means and separable from the service provided by electronic means»[66]. However, although Airbnb does not exercise a decisive influence over accommodation services itself, the accommodation marketing is focused on the platform and not on the supplier. For example, sometimes Airbnb use discounts for guests on the platform, intervening on the prices set by the hosts. The value to suppliers lies in the platform itself – the usability and market reach of Airbnb and Uber. Both enjoy a position of influence over their end-service suppliers because without them, success would diminish considerably. In those terms, Airbnb could be better categorised as a predominant intermediary.

3.3. Future regulatory battles on the horizon

Although ECJ qualified Airbnb as an intermediary, this does not mean that Member States are banned from regulating short-term rental services and correcting identified market failures[67]. E-Commerce Directive does not preclude requirements relating to offline activities that are provided via a digital platform. Indeed, social policy objectives such as ensuring available and affordable housing or the protection of the urban environment is probably best addressed by policy action targeting accommodation providers, not platforms[68]. The E-Commerce and Service Directive[69] have been criticized to belong to another era[70]. On one hand, E-Commerce Directive has the aim to create

63 Opinion, § 67.

64 Ivi, § 71.

65 Judgement, § 68.

66 Opinion, § 82.

67 See B. Edelman - D. Geraldin, *Efficiencies and Regulatory Shortcuts: How Should We Regulate Companies like Airbnb and Uber*, in *Stanford Technology Law Review*, 19, 2016, 293 ss.

68 See C. Busch, *The Sharing Economy at the CJEU*, cit., 174.

69 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market (hereafter "the Service Directive").

70 In these terms, see Corporate Europe Observatory, *UnFairbnb. How online rental platforms use the EU to defeat cities' affordable housing measures*, 2 May 2018.

a legal framework that ensures the free movement of "information society services" between Member States. E-Commerce Directive is a *lex specialis*[71] in relation to the Service Directive, to extent that it applies only to information society services i.e. mere intermediation and does not extend to affecting in the provision of the underlying service[72]. The provision of such service in the EU is, in principle, subject to no prior authorization in the providers home State (Art. 4) and benefit from the "internal market clause (Art. 3(2)), according to which all other (host) member States are precluded from raising any obstacles. Subsequently, "information society services" smart move is to pick a base in a Member State with favourable conditions, in this case Ireland. Moreover, under this Directive, authorities are not allowed to impose a "general obligation" to monitor activity on the website[73]. This could mean that, for instance, Airbnb can be asked to act on a specific suspicion of an illegal listing, but in principle it cannot be asked to check systematically if listings are illegal. Therefore, housing rented conditions through Airbnb is *de facto* unregulated by E-commerce Directive. Indeed, this was also pointed out by AG Szpunar «that the conditions of renting the accommodations, that is to say, of the services provided by the hosts, do not come within the scope of Directive 2000/31 and must be assessed in the light of other provisions of EU law»[74]. On the other hand, the Service Directive is supposed to have "horizontal" application and to cover most services. Several activities, however**,** are excluded, i.e. transportation services**,** financial services, healthcare services etc. Market access for those collaborative platforms which do fall within its scope will be facilitated, both at the level of taking up the activity (at home member state) and that of offering services in other (host) state. Under the Service Directive, the requirement of a prior authorization is not excluded (as in the case of E-Commerce Directive), but it needs to be justified, necessary and proportionate (Art. 9). It is under this Directive where the accommodation sector is included[75]. Therefore, any restrictions imposed by Member States on short-term rentals, in particular authorization or notification requirements, will have to be assessed in the light of that directive.

One of the immediate effects of this decision is that Airbnb can now require to all Member States to review all the obligations imposed on him. For instance, are they included in the closed list of grounds that justify restrictions? Are they proportionate? Have the restrictions been notified? In Germany, municipalities like Hamburg, Berlin and Munich have enacted over the past years local regulations that impose limitations on short -term rentals. In particular, under the new Hamburg's housing law hosts renting out individual rooms or an entire apartment have to notify their rental activity to the city in order to obtain a registration number ("Housing Protection Number")[76].

[71] V. Hatzopoulos*, The collaborative economy under EU law,* London, 2018, 31.

[72] V. Hatzopoulos and S. Roma, *Caring for sharing? The collaborative economy under EU law*, in *CMLR Rev.*, 54, 2017, 82 ss.

[73] Art. 15(1) of E-Commerce Directive.

[74] Opinion, § 90.

[75] See European Commission, *Handbook on the implementation of the Services Directive*, 2007, 10.

[76] Hamburgisches Wohnraumschutzgesetz, zuletzt geändert durch das Dritte Gesetz zur Änderung von Vorschriften im Bereich des Wohnungswesens v. 23.10.2018, HambGVBl. 2018, 349.

Second, the law imposes a maximum limit for short-term rentals of eight weeks per calendar year. For short-term rentals exceeding this limit a special permit is required. Third, hosts have to notify the city's administration about the duration of any guest's stay. Finally, the new law explicitly states that online intermediaries like Airbnb must ensure that no listings are published on their platform without a publicly visible registration number[77]. In Spain as well different measures has been taken by municipalities to regulate the short-term rent conditions. However, currently there is no legal requirement for registering or authorizing platforms that serve to commercialize short-term tourist stays, nor are there any related professional regulations (as there are, for example, for travel agencies and real estate agencies) that are specifically applicable[78]. While Italy has been more active in this aspect through the so called "Airbnb law". The law imposes to Airbnb (and to other similar platforms) the obligation to hold directly 21% on the sums collected by the landlords and then to transfer every amount to the Italian tax authorities[79]. It seems that this provisions hinder the freedom to provide services (protected by Art. 56 TFEU), as far as Airbnb is required to operate as a substitute tax in the first case, or responsible for paying the tourist tax, in the second case, assuming charges and responsibilities completely unrelated to the service provided. Second, the law introduces the obligation to telematic real estate brokerage portals to appoint a tax representative in Italy and to act as tax manager. Airbnb opposed to comply with these measures, arguing that they restrict the freedom to provide information society services granted to intermediaries within the internal market. Therefore, the *Consiglio di Stato* asked if the provisions of Articles 4, 5 ss. of Directive 1535/2015/EU, Art. 8 of Directive 98/34/EC and Art. 56 TFEU preclude national legislation which, without prior notification to the European Commission, imposes on the operator of a telematic real estate brokerage portal the above restrictive measures[80]. As it was already underlined above, if substantial and procedural conditions are not met by Member States who wish to restrict a given "information society service", the legal consequence is the inapplicability to the intermediary of the restrictive measures. Therefore, it is highly possible that the *Consiglio di Stato* will withdraw it request for a preliminary ruling.

4. Conclusion

Although with a different outcome, the Court had another chance to assess the effectiveness of the criteria used in Uber Spain. Since Uber and Airbnb belong to the "sharing economy" category[81] within the huge ecosystem of online intermediaries, it

[77] C. Busch, *Regulating Airbnb in Germany – status quo and future trends*, cit., 39-41.

[78] See A.I. Nadal, *Regulating Airbnb in Spain*, cit., 42-45.

[79] For an overview see, C. Dell'Oste – M. Finizio, *Affitti brevi, il Consiglio di Stato rinvia alla Corte Ue la legge Airbnb*, in *Il Sole 24 Ore,* 18 September 2019.

[80] Council of State (Consiglio di Stato), order no. 6219/2019, cit., § 10.

[81] Platforms cover a wide-ranging set of activities including online advertising platforms, marketplaces, search engines, social media and creative content outlets, application distribution platforms, communications services, payment systems, and platforms for the collaborative economy. For more information on platforms classification see A. Strowel – W. Vergote, *Digital platforms: to regulate or not to*

was "easier" for Court to re-use the same criteria. However, if in the future the Court will be confronted again to unravel the legal status of online intermediaries falling outside this category, then, perhaps, the Court must use additional criterion. For instance, some scholars argue that there is a better way for courts to resolve these platform-or-service-provider quan-daries[82]. Accordingly, they suggest decision-makers to adopt a functionalist approach to these questions. To implement such a functionalist approach, courts should compare platform-enabled transactions to analogous transactions that are not facilitated by any platform or other third party. That comparison will in turn allow courts to assess the extent to which the platform is usurping aspects of what would otherwise be a relationship between service and customer into a triadic relationship in which the platform has its own relationships with the other two parties. In any case, the impression and the ECJ's message is that platforms should limit their influence over the activities of users if they wish to benefit from free movement provisions of E-Commerce Directive. However, this is not what regulators or consumers need. Beyond regulatory and judicial solutions, platforms could play an important role as "regulatory intermediaries". Indeed, Airbnb has undertaken collaborative efforts with public authorities in matters related to short-term tourist rentals in different EU States[83]. For example, Airbnb could enforce applicable thresholds for the maximum number of nights via automated limits as required from some local house law[84]. Similarly, Airbnb could be required to make sure that information is actually exchanged between guests and hosts. The French legislator has already taken this step by introducing the duty of the platform to inform consumer in a loyal, clear and transparent manner about the capacity of the provider and the rights and obligation of the contracting parties, when consumer is put in contact with professional or non-professional[85]. It is an open question, however, whether such a duty would amount to a "general monitoring obligation" prohibited by Art. 15 of E-Commerce Directive. An alternative to monitoring (tracking, red lamps etc) is to oblige the platform to "guide" users to comply with the applicable information obligations or other duties. Summarising, collaboration is probably the most effective and pragmatic way to achieve results within the platform economy, rising controls over the provision of goods and services and favouring transparency and good practices. As a matter of fact, platforms tend evolve towards a more active intervention into the provision of goods or services. It will be not be a surprise if Airbnb owns hotels in the coming years. Therefore, the challenge

regulate?, in B. Deveolder (ed.), *The Platform economy unravelling the legal status of online intermediaries,* cit., 3 ss.; P.J. Dittrich, *Online platforms and how to regulate them: An EU overview*, policy paper no. 227, 14 June 2018, Jacques Dolers Institute Berlin.

[82] See C. Garden – N. Leong, *The Platform Identity Crisis: Responsibility, Discrimination, and a Functionalist Approach to Intermediaries*, in N. Davidson – M. Finck – J. Infranca (eds.), *The Cambridge Handbook of the law of the Sharing Economy*, Cambridge, 2018, 457.

[83] For instance, in 2018 they signed with the regional government of Andalusia to facilitate the online registration of tourism dwellings on the Airbnb platform itself and with the City Council of Barcelona to detect and remove illegal dwellings from the platform, see A.I. Nadal, *Regulating Airbnb in Spain*, cit., 45.

[84] It could be rather easy to verify the legality of listings via an application program interface (API) that connects the platform with a database of registered hosts provided by the city.

[85] See Art. L.111-7, II French Code de la Consummation, available at *Legifrnace.*

awaiting legislators is to determine whether legislative change is required as a consequence of these evolutions.

Note a sentenza

Sezione comparata

L'efficacia extraterritoriale dei diritti fondamentali in una storica sentenza del Tribunale costituzionale federale tedesco

Raffaele Bifulco

Tribunale costituzionale federale della Repubblica federale di Germania (BVerfG), 19 maggio 2020 - 1 BvR 2835/17

La sentenza del Tribunale costituzionale federale tedesco è una sentenza di grande rilievo. Essa colpisce la recente legge tedesca sull'attività informativa svolta sull'estero dai servizi segreti per contrasto con gli artt. 19, c. 3, 5, c. 2, e 10, c. 1, della legge fondamentale. In particolare, il Tribunale arriva a questa conclusione attribuendo ai diritti fondamentali un'efficacia extraterritoriale. È questo profilo della sentenza che il commento vuole mettere in evidenza.

Sommario

Keywords

diritti fondamentali – diritti dell'uomo – sorveglianza elettronica - efficacia extraterritoriale – dimensione difensiva dei diritti fondamentali

1. Diritti fondamentali, territorio statale e sorveglianza elettronica

La funzione originaria e ancora principale dei diritti fondamentali è quella difensiva, di protezione dal potere, dalla inestirpabile tendenza ad aggredire la sfera privata del cittadino. Da sempre è lo Stato, la forma più visibile del potere, a rappresentare il maggior pericolo per la libertà individuale. Ed è per questo motivo che la riflessione sui diritti dell'individuo si è tradizionalmente sviluppata intorno al rapporto tra Stato e individuo. La dimensione verticale e difensiva dei diritti fondamentali è un dato acquisito per la dottrina giuridica moderna, sulla quale non bisogna spendere altre parole.

Maggiore attenzione merita la dimensione spaziale di questo potere aggressivo e debordante. Al netto delle ricerche più recenti sulle grandi imprese multinazionali e sugli effetti delle loro azioni e decisioni sugli Stati e sugli individui[1], neppure gli studi più avvertiti dal punto di vista sociologico hanno dubitato della centralità della dimensione nazionale, comunque legata ad un determinato territorio, del potere[2].

L'apertura al diritto internazionale e al pluralismo delle democrazie costituzionali ha naturalmente favorito, in molti casi, interpretazioni costituzionali sensibili al fattore 'cosmopolitico[3]. Basti pensare, con riguardo all'ordinamento internazionale, alla posizione di apertura della Corte costituzionale che, superando il dato testuale, tende a riconoscere anche in capo agli stranieri i diritti fondamentali non strettamente legati al possesso della cittadinanza. In questo caso specifico vi è stata una sorta di ibridazione tra diritti e libertà fondamentali, classicamente riferiti ai cittadini, e diritti dell'uomo, nati nella sfera del diritto internazionale e perciò a vocazione universale. La dimensione spaziale è tuttavia rimasta quella del territorio statale: è in questo determinato ambito che lo Stato, in quanto detentore del legittimo monopolio della forza, può entrare in conflitto con i diritti e le libertà degli stranieri. E anche l'ulteriore acquisizione teorica della efficacia orizzontale dei diritti fondamentali lascia intatto il perimetro costituito dal territorio dello Stato.

In poche parole, è il territorio che, tradizionalmente, definisce l'ambito di validità e di efficacia dei diritti fondamentali.

La prospettiva cambia allorché i poteri di una democrazia costituzionale, fortemente orientata ai principi del *rule of law*, si confrontano con le situazioni giuridiche di individui stranieri in territorio straniero. È stato ed è ancora, principalmente ma non esclusivamente, il caso degli Stati Uniti d'America (è questa la ragione del riferimento al *rule of law*), nel cui ordinamento la questione dell'efficacia extraterritoriale dei diritti fondamentali si è posta con una certa frequenza; e ciò è avvenuto sia perché, essendo gli Stati Uniti una potenza centrale nello scenario geopolitico, gli apparati militari di quel potere sono spesso venuti a contatto con cittadini stranieri su suolo straniero sia perché, essendo una democrazia costituzionale molto radicata, si presume che tutte le forme di quell'apparato di potere siano vincolate dal diritto.

Non è possibile ricostruire in questa sede un dibattito teorico di lunga durata, costellato da alcune importanti sentenze della Corte Suprema, che si è confrontato con il problema del trattamento degli stranieri, al di fuori del territorio statunitense, dal punto di vista soprattutto della incidenza sulla libertà personale degli stranieri. Vale la pena però ricordare che, anche dopo le rivelazioni di Edward Snowden che hanno rivelato al mondo l'attività di sorveglianza elettronica svolta da agenzie governative statunitensi in collaborazione con i servizi di intelligenze britannici, australiani, neozelandesi e canadesi, l'Amministrazione federale ha tenuto la linea di difesa secondo cui i diritti

[1] Cfr. ora molto fruttuosamente A. Golia jr., *Imprese transnazionali e vincoli costituzionali. Tra pluralismo e responsabilità*, Milano, 2019.

[2] Ma cfr. G. Teubner, *Verfassungsfragmente. Gesellschaftlicher Konstitutionalismus in der Globalisierung* (2012), trad.it. *Nuovi conflitti costituzionali*, Milano, 2012.

[3] Il rapporto di influenza è stato anche inverso. Sul punto sia permesso rinviare a R. Bifulco, *La c.d. costituzionalizzazione del diritto internazionale: un esame del dibattito*, in *Rivista internazionale di filosofia del diritto*, 2014, 239 ss.

fondamentali garantiti dalla Costituzione ai cittadini statunitensi si applicano solo ai cittadini statunitensi e a coloro che presentano legami con la *community* tali da considerarli parte di quest'ultima [4].

Ed è proprio il tema della sorveglianza elettronica a porre in una nuova luce la questione della sfera territoriale di efficacia dei diritti fondamentali. Il coperchio sollevato da Snowden ha mostrato un salto di qualità dell'attività di sorveglianza svolta dai servizi di *intelligence* attraverso l'intercettazione delle comunicazioni elettroniche, caratterizzata dai seguenti elementi: ampliamento della platea degli Stati coinvolti nell'attività di sorveglianza elettronica; uso intenso delle tecnologie informatiche nell'attività di sorveglianza; violazione dei diritti individuali collegati all'uso delle tecnologie informatiche, dalla segretezza delle comunicazioni interpersonali al rispetto della *privacy*, dal segreto professionale alla libertà d'informazione; e soprattutto – per quanto rileva in questa sede – capacità dei servizi di *intelligence* di sottoporre a sorveglianza elettronica non solo i propri cittadini ma anche quelli stranieri residenti in territori stranieri o comunque attivi al di fuori del territorio dello Stato che effettua l'attività di *intelligence*. Appare quest'ultimo il tratto maggiormente caratterizzante l'attività di sorveglianza elettronica, oltre alla dimensione semplicemente gigantesca di dati che questo tipo di controllo riesce a intercettare.

Il nuovo scenario ha provocato e sta tuttora provocando una serie di sentenze che, ai più diversi livelli ordinamentali, si confrontano con la sfida di ricondurre dentro il perimetro dello Stato di diritto le nuove vie del potere statale. Senza alcuna pretesa di completezza possono ricordarsi, come direttamente collegati al tema della sorveglianza elettronica da parte dei servizi segreti, almeno i seguenti importanti arresti giurisprudenziali. Innanzitutto le due sentenze della Corte di giustizia dell'Unione europea, legate al nome della parte M. Schrems [5], nelle quali il sistema di trasferimento dei dati dall'Unione europea verso gli Stati uniti è stato annullato a causa della inadeguatezza del sistema giuridico statunitense nel garantire una tutela del diritto alla tutela dei dati personali e del diritto ad un ricorso effettivo paragonabili a quelli garantiti ai cittadini europei dalle norme dei trattati, in particolare dalla Carta dei diritti fondamentali dell'Unione europea. Di notevole interesse sono anche le sentenze *Big Brother Watch* e *EGMR* e *Centrum för Rättvisa* della Corte europea dei diritti dell'uomo, entrambe in attesa di giudizio da parte della *Grande Chambre*. Infine, anche all'interno degli Stati Uniti, le vicende svelate da Snowden hanno molto recentemente portato il giudice del Nono Distretto a dichiarare che il sistema di sorveglianza di cui era a capo la NSA era illegittimo (United States Court of Appeals for The Ninth Circuit, *United Stated of America v. Basaaly Saeed Moalini*, 13-50572, 2 settembre 2020).

[4] Per una ricostruzione più attenta di questa linea argomentativa, sostenuta dall'Amministrazione federale anche di fronte al Comitato dei diritti dell'uomo presso l'ONU, sia permesso rinviare a R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza costituzionale*, 1, 2016, 289 ss.

[5] CGUE (Grande Sezione), C-362/14, *Maximilian Schrems c. Data Protection Commissioner* (2015) e C-311/18, *Data Protection Commissioner c. Facebook Ireland Lts, Maximilian Schrems* (2020).

2. La sentenza del Tribunale costituzionale federale tedesco del 19 maggio 2020 relativa alla legge sulla sorveglianza estero-estero

È in questo contesto che si inserisce la sentenza del primo Senato del Tribunale costituzionale federale tedesco del 19 maggio 2020 (BvR 2835/17). La sentenza ha il profilo delle grandi decisioni[6]. Non solo perché tenta di ricondurre l'attività di *intelligence* nei canoni dello Stato di diritto[7], dichiarando molte disposizione della legge sull'attività informativa svolta sull'estero dai servizi segreti (Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes) del 23 dicembre 2016 non conformi (*unvereinbar*) alla Legge fondamentale tedesca, e dando termine al Parlamento per introdurre una nuova disciplina fino al 31 dicembre 2021[8].

Lo è soprattutto perché prende una posizione molto innovativa sulla questione dell'efficacia extraterritoriale dei diritti fondamentali. Ed è proprio questo specifico profilo della sentenza – peraltro estremamente articolata (141 pagine, 332 punti) - che le presenti note vogliono analizzare [9]. Tuttavia, anche per poter apprezzare i profili relativi all'efficacia dei diritti fondamentali, appare indispensabile un sintetico ragguaglio riguardante i motivi dell'illegittimità e i principi che il Tribunale ha elaborato come direttive per il legislatore.

La sorveglianza estero-estero è autorizzata dalla legge tedesca nei casi enumerati dall'art. 1, tutti rivolti alla necessità di conoscere in anticipo situazioni di pericolo per la sicurezza interna ed esterna per la Repubblica federale e alla tutela della capacità di azione della Repubblica federale e in particolare del Governo federale.

Le violazioni costituzionali ravvisate dal Tribunale riguardano in particolare, dal punto di vista sostanziale, gli artt. 10, c. 1, (segreto delle telecomunicazioni), 5, c. 2, al n. 2, (libertà d'informazione) e, dal punto di vista formale, l'art. 19, c. 1, della Legge fondamentale tedesca (da ora anche "GG", Grundgesetz,).

All'origine della legge vi sono, ancora una volta, le rivelazioni di Snowden che hanno portato, nel corso della XVIII legislatura, all'istituzione di una commissione parlamentare d'inchiesta (NSA-Untersuchungsausschuss), nel cui rapporto finale sono state denunciate le carenze del precedente sistema di informazione strategica estero-estero

---

[6] Varie le valutazioni della sentenza, ma tutte di segno positivo: "*ein Grundlagenurteil*", secondo H.P. Aust, *Auslandsaufklärung durch den Bundesnachrichtendienst*, in *Die öffentliche Verwaltung*, 2020, 715; "*ein Meilenstein*", secondo J.H. Dietrich, *Ausland-Fernmeldeaufklärung nach §§ 6 ff BNDG (Anmerkung)*, in *Zeitschrif für das Gesamte Sicherheitsrecht*, 4, 2020, 182 e B. Huber, *Das BverG und die Ausland-Ausland-Fernmeldeaufklärung des BND*, in *Neue Verwaltungszeitschrif-Beilage*, 2020, 9; una sentenza dotata dello "*charme der Einfachheit*", nella più critica lettura di M. Löffelmann, *Anmerkung*, in *Juristiche Rundschau*, 9, 2020, 515.

[7] In tal senso S. Muckel, *Fernmeldeaufklärung im Ausland im BND-Gesetz verfassungswidrig geregelt*, in *Juristiche Arbeit*, 2020, 635, che sottolinea lo sforzo del Tribunale di ripensare l'attività dei servizi segreti all'interno dei crescenti rischi per la sicurezza di carattere globale.

[8] Con il termine "*Ausland-Ausland-Fernmeldeaufklärung*" si intende l'attività di informazione svolta nei confronti delle comunicazioni tra cittadini stranieri residenti all'estero, attività che, per comodità e per evidenziare la differenza con la sorveglianza nazionale e internazionale, si definirà sorveglianza estero-estero.

[9] Sottolinea il rilievo della sentenza per i profili attinenti alla dogmatica generale dei diritti fondamentali M. Sachs, *Grundrechte: Geltung für Ausländer im Ausland*, in *Juristische Schulung*, 2020, 706.

dal punto di vista del fondamento legislativo.

Il primo vizio riscontrato è di carattere formale. L'art. 19, c. 1, GG, stabilisce infatti che, in caso di limitazione di un diritto fondamentale apposta con legge, «la legge deve individuare il diritto fondamentale indicando l'articolo interessato». La limitazione dell'art. 10, c. 1, GG, è menzionata solo nell'art. 3, non anche nelle altre disposizioni della legge impugnata (punto 134)[10]. Tale carente individuazione – osserva il Tribunale - denota una scarsa consapevolezza della limitazione da parte del legislatore, che, così agendo, si sottrae anche a un dibattito pubblico.

Dal punto di vista materiale sono invece le disposizioni contenute, in particolare, negli artt. 6, 7, 13-15 della legge a non essere conformi agli artt. 10, c. 1, e 5, c. 1, GG. Il giudice costituzionale muove da un assunto pragmatico secondo cui l'attività di *intelligence* possiede delle caratteristiche di segretezza irrinunciabili. Ciò non vuol dire, tuttavia, che la disciplina legislativa di tale attività possa sottrarsi all'esigenza di previsioni normative improntate alla chiarezza e alla determinatezza (137-8) e al rispetto del principio di proporzionalità (visto che tali previsioni legislative giustificano interventi limitativi del segreto delle telecomunicazioni e della libertà d'informazione) [11].

I punti da 142 a 153 sono infatti volti a evidenziare proprio i rischi della sorveglianza elettronica rispetto al principio di proporzionalità. A proposito della straordinaria latitudine di tale tipologia di controllo è interessante notare come il Tribunale, nell'enfatizzare le differenze rispetto alle precedenti forme di controllo effettuate dai servizi di *intelligence*, sottolinei il carattere ubiquo della sorveglianza elettronica, capace di intercettare, attraverso la Rete, le forme private e spontanee della comunicazione quotidiana e di penetrare così nel tessuto comunicativo della società civile («*die gesamte Kommunikation auch der Zivilgesellschaft*») (151).

Per meglio afferrare la posizione del giudice costituzionale, è opportuno rammentare i caratteri della sorveglianza strategica, la quale, a differenza della sorveglianza orientata verso singoli determinati soggetti, non muove da sospetti concreti, è caratterizzata da un raggio di indagine estremamente ampio ed è diretta ad ottenere informazioni per permettere l'azione del governo e la conoscenza di possibili pericoli. Ciò implica una selezione per luoghi geografici e per nazionalità. Di conseguenza, in una prima fase, sono messi a disposizione dei servizi segreti tutte le comunicazioni intercettate, che vengono successivamente filtrate attraverso sistemi elettronici capaci di selezionare le informazioni rilevanti. Interviene poi un ulteriore livello di cernita attraverso selettori di natura formale (numeri telefonici e email) e sostanziale (nomi, codici). Al termine vengono verificati i risultati così ottenuti attraverso la catalogazione e l'identificazione ed è in questa ultima fase che vengono cancellati i dati che non avrebbero dovuto essere rilevati o trattati[12].

[10] Da ora in poi, per comodità, verrà indicato solo il numero, senza l'indicazione "punto".

[11] Un contrasto della legge con l'art. 10 GG e con il principio di proporzionalità, oltre che con l'art. 19, c. 3, GG, era già stato individuato da C. Marxsen, *Strategische Fernmeldeaufklärung*, in *Die öffentliche Verwaltung*, 2018, 225-226, che scrive prima della sentenza in esame.

[12] Per l'identificazione di queste fasi cfr. C. Marxsen, ivi, 219-220.

3. I principi elaborati dal Tribunale per il Legislatore

E tuttavia, nonostante i rischi del controllo strategico, esso può essere reso conforme al dettato costituzionale. A tal fine, e con specifico riguardo alla sorveglianza strategica estero-estero, il Tribunale fornisce al legislatore una serie di principi da osservare per una disciplina legislativa costituzionalmente conforme, partendo dal principio per cui la sorveglianza svolta all'interno della Repubblica federale va considerata in maniera differente rispetto a quella estero-estero: nel primo caso il controllo deve essere motivato da precise circostanze e deve essere mirato, nel secondo il raggio dell'azione di controllo può essere ad ampio raggio e privo di un obiettivo predeterminato (*anlasslos*, scrive il Tribunale) (159-160). In estrema sintesi i criteri che il giudice costituzionale fornisce al legislatore sono i seguenti[13].

In primo luogo, il legislatore deve indicare criteri restrittivi per la trasmissione di dati e assicurarsi che l'ambito geografico sottoposto a sorveglianza rimanga delimitato (169).

In secondo luogo, per mantenere la sorveglianza strategica nei confini di uno strumento di informazione, appare poi necessario una disciplina chiara della selezione (ed esclusione) dei dati provenienti dalle comunicazioni interne e dall'interno verso l'estero (170 ss.). Anche gli scopi della sorveglianza devono essere definiti normativamente in maniera sufficientemente precisa e chiara. A tal fine vengono in primo piano le finalità rivolte alla tutela di interessi rilevanti (*hochrangiger Gemeinschaftsgüter*), la cui violazione avrebbe effetti negativi per la sicurezza esterna ed interna o per gli interessi dei singoli. A questo principio si può derogare solo se l'adozione della misura di sorveglianza delle comunicazioni estere occorra al Governo federale e alla preparazione di sue decisioni (175-177).

Siccome non può escludersi la legittimità di una sorveglianza strategica senza obiettivi determinati, assumono rilievo regole procedurali, capaci di delimitare anche temporalmente le misure di sorveglianza, per quanto non siano derivabili dalla Legge fondamentale. Ciò che invece può essere ricavato, per analogia, dal dettato costituzionale, è la previsione di un controllo di tipo giurisdizionale (*gerichtsähnliche Kontrolle*), sulla falsariga della riserva di giurisdizione prevista in via generale per le misure di limitazione delle comunicazioni (178-181).

Il Tribunale non esclude poi la conformità alla Legge fondamentale di misure che permettano l'uso di selettori formali (*formaler Suchbegriffe*), anche se orientate verso singole persone. Per avere tale conformità, sono tuttavia necessarie regole legislative che delimitino tale potere. Il giudice di Karlsruhe suggerisce nuovamente la previsione di controlli di tipo giurisdizionale *ex ante* (186-188).

Limiti legislativi devono essere previsti inoltre per la conservazione dei dati derivanti dalla sorveglianza strategica. Il flusso di dati va delimitato, non dovendosi superare i sei mesi come termine massimo per la conservazione (191). Per le singole fasi della valutazione dei dati così raccolti, il legislatore può limitarsi a porre i principi lasciando l'ulteriore dettaglio ai servizi di *intelligence*, a condizione che l'ambito lasciato ai servizi sia sottoposto ad un controllo indipendente e oggettivo (192).

[13] Ritiene casuali e vaghi i criteri indicati dal Tribunale per distinguere la tutela dei diritti tra interno ed estero W. Durner, *Schiffbruch der BND-Novelle 2016*, in *Deutsches Verwaltungsblatt*, 2020, 953.

Il Tribunale sottolinea l'affidamento da garantire a giornalisti e avvocati e ai loro informatori e clienti. La sorveglianza mirata di questi gruppi deve essere limitata in via legislativa. Non può essere addotta a giustificazione del controllo, in nome di interessi legati alla sicurezza, la tipologia di persone con le quali giornalisti ed avvocati entrano in contatto, fatta eccezione per le fattispecie penali particolarmente gravi. Spetta sempre al legislatore prevedere che l'affidamento sia tutelato da controlli di tipo giurisdizionale *ex ante* (193-194).

L'ambito più intimo degli stili di vita individuali deve poi essere tutelato dal legislatore anche nelle ipotesi di sorveglianza verso l'estero (199 ss.). Le indicazioni del Tribunale si chiudono ricordando che il rispetto del principio di proporzionalità impone che siano previsti termini precisi per la distruzione dei dati personali. A tal fine vanno previsti protocolli ben determinati (208 ss.).

Il Tribunale passa poi all'indicazione dei principi in tema di trasmissione dei dati personali ad altri soggetti ed istituzioni nell'ambito della sorveglianza strategica, partendo, anche questa volta, dalla fissazione del principio per cui la trasmissione costituisce una nuova ingerenza nei diritti fondamentali; per questo motivo esso richiede una disciplina normativa chiara (211 ss.). Sia la disciplina legislativa che le singole misure dirette alla trasmissione devono, da un punto di vista materiale, essere orientate al principio di proporzionalità, ispirandosi al criterio della ipotetica nuova rilevazione dei dati (*hypothetische Datenneueerhebung*) (216). In pratica, la trasmissione potrà avvenire se anche rispetto alla mutata finalità i dati che si intende trasmettere avrebbero potuto essere comunque rilevati.

In ogni caso, se i dati in possesso dei servizi tedeschi provengono da una sorveglianza non diretta alla prevenzione di pericoli (*Gefahrenfrüherkennung*), allora essi non potranno essere trasmessi ad altre autorità, se non nei casi eccezionali, da prevedere in via legislativa, in cui i dati permetterebbero di venire a conoscenza di rischi per la vita delle persone e per la sicurezza del paese (228)[14].

Per la trasmissione ad autorità pubbliche straniere dei dati ottenuti dalla sorveglianza estero-estero, in particolare a servizi segreti stranieri, è necessaria una verifica della rispondenza delle loro prassi ai principi dello Stato di diritto (*Rechtsstaatlichkeitsvergewisserung*) (233), al fine di evitare che lo Stato estero possa violare diritti e principi collegati alla dignità dell'uomo (237). Nel caso di contatti con Stati non sicuri da tale punto di vista, ci si dovrà accertare che le informazioni non vengano utilizzate per perseguitare le minoranze presenti, colpire le opposizioni, uccidere o torturare, privare i detenuti dei loro diritti (238). La verifica dello *standard* non può essere rimessa a una decisione di natura politica, ma deve basarsi su informazioni corrispondenti alla realtà, oltre che essere documentata e aperta ad un controllo indipendente (241).

L'art. 13 della legge regola nel dettaglio la cooperazione dei servizi tedeschi con altri servizi stranieri nell'ambito della sorveglianza estero-estero, al fine di realizzare gli obiettivi di cui all'art. 1 della legge medesima. Il primo Senato osserva che la Costituzione tedesca è strutturalmente aperta a tale collaborazione tra servizi di *intelligence*; vanno tuttavia predisposte regole legislative a tutela dei diritti fondamentali anche nell'ambito

[14] Per una critica a questa limitazione, perché limitante la sfera d'azione della Repubblica federale sul piano internazionale, J.H. Dietrich, *Ausland-Fernmeldeaufklärung nach §§ 6 ff BNDG (Anmerkung)*, cit., 180.

di tale collaborazione (244). Soprattutto deve evitarsi che i risultati della sorveglianza interna vengano scambiati con servizi di *intelligence* stranieri. Tale scambio di informazioni privo di regole (*Ringtausch*) non sarebbe conforme a Costituzione (248). Le medesime regole s'impongono per la sorveglianza svolta dai servizi tedeschi all'estero, indicate nel § 253. Regole specifiche devono valere sia nel caso in cui il servizio di *intelligence* tedesco utilizzi selettori elaborati da servizi stranieri e i relativi riscontri vengano trasmessi ai partner senza una valutazione contenutistica (254) sia nel caso in cui i dati ricavati attraverso determinati selettori dai servizi tedeschi vengano trasmessi a servizi esteri (262). Il Tribunale ritiene che i servizi esteri possano essere destinatari di informazioni provenienti dalla Germania in occasioni determinate (*bestimmter Anlass*) e comunque sulla base di un dettagliato fondamento normativo capace di garantire l'efficacia dei diritti fondamentali sia dal punto di vista materiale che procedurale (249).
Altro profilo degno di nota riguarda le questioni procedurali, regolate dall'art. 22 della legge in maniera ritenuta non soddisfacente dal Tribunale costituzionale, il quale indica, in sostanza, due tipologie di controllo da apprestare (274). Con la prima il Tribunale chiede che sia previsto un collegio giudicante indipendente, chiamato a giudicare sulle misure di sorveglianza estero-estero attraverso forme di tipo giurisdizionale (*gerichtsähnliche Kontrolle*) (275). Accanto a questo organo il Tribunale auspica l'istituzione di un'istanza amministrativa indipendente, in grado di controllare la legalità di tutte le fasi del processo di sorveglianza strategica (276). Entrambe le istanze di controllo devono avere accesso completo ai documenti (290) e devono essere sostenute da adeguati mezzi finanziari (288)[15]. Nulla osta, afferma il giudice costituzionale, a che l'organo di controllo sia inserito all'interno della funzione esecutiva (271).
Tale ultima affermazione del Tribunale è di rilievo in quanto diretta a porre un freno alla prassi fondata sulla cd. *Third Party Rule*, in base alla quale le informazioni provenienti da servizi esteri non potrebbero essere sottoposte ad istanze di controllo interne (292). In tal maniera si è impedito di fatto un effettivo controllo sull'attività informativa dei servizi. Questa regola, fondata esclusivamente sulle prassi delle autorità amministrative, non trova giustificazione dal punto di vista costituzionale (294). Va inoltre assicurato che il controllo possa estendersi anche alle informazioni che i servizi di *intelligence* ricevono da servizi esteri (295). Eccezioni possono essere previste nel caso di istituzione di commissioni parlamentari d'inchiesta sull'attività informativa di autorità tedesche (298).

4. I profili della sentenza relativi all'efficacia dei diritti fondamentali nello spazio

Riassunti in maniera estremamente sintetici i contenuti della sentenza, è ora possibile dedicare attenzione ai profili relativi all'efficacia dei diritti fondamentali nello spazio. Profili che potrebbero apparire marginali rispetto alle questioni sostanziali affrontate

[15] Diffusa nella dottrina è la constatazione che il modello cui si ispira il Tribunale è quello inglese dell'*Investigatory Powers Act*: B. Huber, *Das BverG und die Ausland-Ausland-Fernmeldeaufklärung des BND*, cit., 8.

nella decisione e che, invece, giocano un ruolo centrale non solo ai fini dell'ammissibilità dei ricorsi ma anche ai fini del *decisum*. Non si dimentichi infatti che la legge censurata disciplina espressamente l'attività di sorveglianza estero-estero e che i ricorrenti erano per lo più residenti al di fuori della Repubblica federale.

4.1. Sulla legittimazione dei ricorrenti

Conviene partire proprio dalla diversa natura soggettiva e dai diversi luoghi di residenza dei ricorrenti: un'organizzazione non governativa con sede in Francia, giornaliste e giornalisti residenti in Azerbaijan, in Germania, nel Regno Unito, in Slovenia, in Messico e in Macedonia del Nord, un avvocato di cittadinanza tedesca ma residente in Guatemala. Tutti erano caratterizzati dal fatto di svolgere la propria attività professionale a favore della tutela dei diritti umani e, perciò, spesso a contatto con persone suscettibili di divenire oggetto di attenzione da parte della sorveglianza estero-estero. Da qui la probabilità, sostenuta da tutti i ricorrenti, di essere stati intercettati da parte dei servizi di *intelligence*.

Di particolare interesse si rivelano quindi le decisioni assunte in materia di legittimazione al ricorso da parte del Tribunale, che, oltre a ritenere ammissibili i ricorsi individuali, ha ritenuto in particolare ammissibile sia il ricorso di 'Reporter senza frontiere', la ONG con forma di persona giuridica sita a Parigi (62), sia il ricorso dell'avvocato tedesco attivo professionalmente in Guatemala. Il fatto che quest'ultimo agisse in qualità di funzionario di una persona giuridica straniera non fa venir meno la sua legittimazione giacché esso, sottolinea il giudice costituzionale, agisce per la difesa dei suoi diritti fondamentali e non di quelli della persona giuridica per la quale svolge attività professionale (68-69). L'eccezione di inammissibilità, respinta dal Tribunale, si spiega alla luce dell'art. 19, c. 3, GG, che limita la titolarità dei diritti fondamentali alle persone giuridiche nazionali [16].

Va anche evidenziato che il Tribunale individua una legittimazione diretta dei ricorrenti nei confronti delle misure strategiche di sorveglianza estero-estero previste dalla legge censurata. Trattandosi di misure segrete di cui si viene a conoscenza *ex post* solo in casi eccezionali, deve infatti presumersi una legittimazione diretta dei ricorrenti (72).

4.2. Società civile e sorveglianza elettronica

Venendo ora più da vicino alle argomentazioni del Tribunale in tema di efficacia extraterritoriale dei diritti fondamentali, conviene prestare attenzione allo scenario dipinto dal giudice tedesco in funzione preliminare e introduttiva rispetto al contenuto argomentativo.

Le informazioni provenienti dall'estero sono divenute da tempo un elemento importante della politica estera e di sicurezza. Con lo sviluppo dei mezzi di comunicazione

[16] Il punto è enfatizzato da quasi tutti i commentatori: cfr. in particolare S. Muckel, *Fernmeldeaufklärung im Ausland im BND-Gesetz verfassungswidrig geregelt*, cit., 633.

elettronici la situazione è tuttavia profondamente mutata. Prima le informazioni dell'*intelligence* sull'estero miravano ad ottenere notizie in funzione di difesa verso attacchi armati nei confronti del territorio tedesco. Oggi il potenziale di pericolo proveniente dall'estero si è moltiplicato sia perché le informazioni viaggiano attraverso i confini con grande facilità di coordinamento sia perché determinate attività provenienti dall'estero possono avere effetti destabilizzatori (come mostrano gli esempi degli attacchi cibernetici, della criminalità internazionale organizzata, del terrorismo internazionale). È questo il motivo per cui l'attività di sorveglianza elettronica verso l'estero ha acquistato una progressiva e rilevante importanza (il Tribunale cita i crescenti stanziamenti di bilancio federale a favore di questa parte dei servizi segreti) (107).

Viene così a crearsi un nuovo campo di tensione in cui le esigenze della sicurezza devono essere bilanciate con la garanzia della libertà, a sua volta costruita, secondo i principi dello Stato di diritto, sui diritti fondamentali. Le nuove tecnologie informatiche fanno sì che il flusso di dati penetri i confini statali per distribuirsi a livello globale. Ciò ha come conseguenza che oramai è possibile intercettare dall'interno comunicazioni provenienti dall'estero. Ma è proprio grazie a questo flusso privo di confini, grazie ai servizi di comunicazione che non sono costruiti sulla differenza tra interno ed esterno, che si sviluppa la comunicazione tra cittadini in quanto titolari di diritti fondamentali, una comunicazione che si svolge all'interno ma anche all'esterno dello Stato. A questo punto il Tribunale evoca la storica categoria della società civile (*Zivilgesellschaft*), pericolosamente sottoposta a diverse forme di interferenze, sia in quanto oggetto di sorveglianza estera da parte dei servizi tedeschi sia in quanto oggetto di sorveglianza da parte di servizi stranieri (109).

Da questa situazione fattuale il Tribunale perviene ad una valutazione teorica di estremo impegno, ritenendo che una concezione dei diritti fondamentali, che ne limitasse l'ambito ai confini statali, lascerebbe i diritti fondamentali privi di tutela nei confronti degli accennati sviluppi tecnologici, facendo indietreggiare l'ambito della tutela rispetto alle condizioni attuali dell'internazionalizzazione. Ne va dell'effettività della tutela dei diritti, che potrebbe girare a vuoto in questa sfera dell'azione statale. Di contro, è proprio il vincolo posto dall'art. 1, c. 3, GG, nei confronti dello Stato che obbliga a tener conto di questo potenziale di rischio e a ricondurlo nella cornice dello Stato di diritto (110)[17].

Lo sforzo ricostruttivo appare degno della massima attenzione. Il Tribunale riscontra le differenze tra un prima e un dopo dell'*intelligence*, richiama l'attenzione sulla porosità dei confini statali, è attento a non chiudersi in una concezione dei diritti fondamentali che potrebbe lasciarli priva di tutela. Anche il lessico, che il Tribunale sceglie con la massima attenzione, pare condividere lo sforzo habermasiano di riconsiderare l'intera società civile non più come il luogo dell'economia (del diritto privato e del mercato del lavoro) bensì come sfera pubblica dove è proprio la comunicazione -che prende forma grazie ad associazioni, organizzazioni, movimenti- a definire il mondo di vita della società [18]. Il Tribunale, insomma, non lascia cadere l'occasione che gli si presenta per

[17] L'art. 1, c. 3, GG, afferma che i diritti fondamentali previsti nei successivi articoli «vincolano la legislazione, il potere esecutivo e la giurisdizione come diritti direttamente applicabili».

[18] J. Habermas, *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*

una riconsiderazione dello sfondo in cui ripensare alcuni aspetti centrali della teoria dei diritti fondamentali. Il che, per un organo chiamato a risolvere problemi eminentemente pratici, non è per nulla scontato[19].

4.3. I diritti fondamentali vincolano tutti i poteri dello Stato

Punto di partenza e di arrivo del ragionamento del giudice costituzionale tedesco è il seguente: i diritti fondamentali vincolano tutti i poteri dello Stato tedesco. L'affermazione di principio è immediatamente calata nel contesto del caso specifico attraverso la seguente specificazione del Tribunale: tale vincolo vale, in ogni caso (*jedenfalls*), per i diritti fondamentali in quanto diritti di difesa nei confronti di misure di sorveglianza (88) [20]. In questa fattispecie ricadono anche gli artt. 10, c. 1 e 5, c. 2, GG, la cui tutela si estende anche alla sorveglianza estero-estero (87). La posizione espressa dal Tribunale è in netta contrapposizione con quanto sostenuto dalle parti costituitesi in giudizio, *in primis* il Governo federale, ed è in ampia sintonia con la maggioranza della dottrina costituzionalistica tedesca che ha preso posizione sul punto [21].

In poche parole, il vincolo costituzionale dei diritti fondamentali sussiste anche se la limitazione del diritto avviene al di fuori del territorio tedesco, bastando, a tal fine, che essa consegua all'esercizio di poteri statali. In questo modo, pur con la delimitazione riguardante la dimensione difensiva dei diritti, il Tribunale risponde al quesito che aveva lasciato in sospeso nel precedente del 1999, in occasione del quale, pur non negando la possibile efficacia extraterritoriale dei diritti, non si era pronunciato sulla necessaria sussistenza di un collegamento col territorio dell'azione in violazione del diritto [22]. Il Tribunale sviluppa una serie di argomenti a sostegno della sua conclusione. Il primo riguarda il vincolo sulle tre funzioni statali dei diritti fondamentali, vincolo che non soffre limitazioni territoriali e che comunque non è ricavabile dalla lettera della disposizione. Conviene soffermarsi su questo argomento. In effetti, proprio perché la Costituzione tedesca non delimita territorialmente l'ambito di efficacia dei diritti fondamentali, sarebbe stato possibile dire che tali diritti valgono solo all'interno del territorio tedesco [23]. D'altronde che la validità e la conseguente applicazione dei diritti

(1992), trad.it. *Fatti e norme. Contributi a una teoria discorsiva del diritto e della democrazia*, Milano, 1996, 391 ss.

19 In proposito H.P. Aust, *Auslandsaufklärung durch den Bundesnachrichtendienst*, cit., 724, sottolinea come l'intento del Tribunale di assoggettare l'attività estera ai vincoli derivanti dallo Stato di diritto e dai diritti fondamentali non sia mai disgiunto dalla considerazione del contesto in cui tali vincoli devono praticamente realizzarsi.

20 La specificazione è rilevante e su di essa si tornerà nelle conclusioni. Si riporta l'originale: «*Das gilt jedenfalls für die Grundrechte als Abwehr gegenüber Überwachungsmassnahmen, wie sie hier in Frage stehen*».

21 C. Marxsen, *Strategische Fernmeldeaufklärung*, cit., 226, fornisce utili indicazioni sulla dottrina in materia.

22 Nel precedente del 1999 [BverfGE 100, 313 (363 ss.)], il Tribunale aveva già riconosciuto l'efficacia extraterritoriale dei diritti fondamentali, proprio con riguardo all'art. 10 GG. Non aveva però precisato se il vincolo costituzionale sussistesse anche in assenza di una relazione tra l'azione dei pubblici poteri e il territorio della Repubblica federale.

23 M. Löffelmann, *Anmerkung*, cit., 516, suggerisce un argomento simile, osservando che dai lavori di redazione della Legge fondamentale non è possibile ricavare una risposta alla questione dell'efficacia

siano riferite all'ambito territoriale nazionale è una caratteristica naturale, implicita, incontroversa dei diritti fondamentali. Il silenzio della Costituzione, insomma, avrebbe giustificato anche un'opzione interpretativa differente. E invece il giudice tedesco rifiuta categoricamente questa possibilità, escludendo che ci sia un'accezione tacita della norma costituzionale in tal senso. Gli artt. 1, c. 2, 24 e 25 testimoniano, in particolare, l'apertura internazionale del testo costituzionale e la collocazione della Repubblica federale nel consesso delle nazioni (89).

Se il paragone è consentito, la scelta del Tribunale può essere accostata a quella della Corte costituzionale con la sent. 1/1956: nel caso italiano era in gioco l'efficacia della Costituzione indipendentemente dal tempo, nel caso in esame era in gioco l'efficacia della Costituzione tedesca indipendentemente dallo spazio.

La garanzia che la Costituzione tedesca offre tramite i diritti fondamentali tutela l'individuo nei confronti delle tre funzioni dello Stato sia dal punto di vista soggettivo sia dal punto di vista oggettivo. Non c'è spazio per eccezioni o domini riservati. Su tale ulteriore profilo il Tribunale afferma espressamente che il vincolo dell'art. 1 GG riguarda il potere esecutivo indipendentemente dall'uso della forza. Anzi, il giudice tedesco evoca la modifica costituzionale del 1956 con cui, nell'art. 1, c. 3, il termine "amministrazione" (*Verwaltung*) fu sostituito dal termine 'potere esecutivo' (*vollziehende Gewalt*), per dimostrare che l'intento non era quello di restringere il vincolo all'esercizio di alcune determinate funzioni bensì di ricomprendere nel vincolo anche le forze armate (*Bundeswehr*). Una limitazione dell'efficacia dei diritti fondamentali agli atti d'imperio dell'Esecutivo non corrisponderebbe, secondo il Tribunale, al senso dell'art. 1, c. 3, GG (90). L'organo giurisdizionale rafforza il suo argomento riprendendo anche una classica distinzione della dogmatica tedesca sui diritti fondamentali, e cioè la distinzione tra dimensione soggettiva (riguardante le singole persone fisiche e giuridiche) e dimensione oggettiva (per intendersi, quella in cui lo Stato si fa garante dei diritti e delle libertà) degli stessi, per dire che il vincolo derivante dall'art. 1, c. 3, GG, è generale, abbracciando entrambe le dimensioni (92).

4.4. Diritti dell'uomo e diritti fondamentali

Si giunge così ad altra questione di grande interesse. La si introduce osservando che è oramai constatazione comune quella sulla porosità dei confini degli Stati e del territorio. La Rete ne è la dimostrazione forse più plastica. Ebbene, a fronte di questo assottigliamento dei confini nella prospettiva interna la sentenza apre prospettive nuove sulla proiezione esterna non tanto del territorio nazionale quanto delle funzioni statali nel momento in cui esse producano effetti su soggetti stranieri residenti su territorio straniero. In tale evenienza i diritti fondamentali diventano, per esprimersi in termini metaforici, delle corazze che possono essere indossate anche all'estero da cittadini stranieri per difendersi da attacchi del potere statale tedesco.

Il Tribunale intesse un interessante collegamento tra diritti dell'uomo e diritti fondamentali, entrambi menzionati rispettivamente al c. 2 e 3 dell'art. 1 GG. Il giudice tede-

territoriale.

sco è attento a prevenire una possibile obiezione diretta a limitare l'ambito di efficacia dei diritti dell'uomo. La Costituzione tedesca distingue infatti tra i diritti dei tedeschi e i diritti dell'uomo. Ciò tuttavia non deve portare, secondo quanto argomentato nella sentenza, a limitare l'efficacia dei diritti dell'uomo alla dimensione interna. Ciò contrasterebbe con il tenore letterale della Costituzione, in particolare con il preambolo che rimanda ad una responsabilità del popolo tedesco in una Europa unita e più ampiamente nel mondo. Neppure rileva il fatto che i diritti dell'uomo siano qualificati come inviolabili e inalienabili (c. 2), a differenza dei diritti fondamentali privi di tale qualificazione (c. 3). Non è possibile ricavare dal dato letterale e dalla sistematica della Costituzione tedesca alcun appiglio per ambiti di applicazione territoriali differenti. Il Tribunale, a tale proposito, cita se stesso per sottolineare di avere sempre interpretato i diritti fondamentali alla luce delle garanzie internazionali offerte dai diritti dell'uomo (94-95). Da questa proiezione internazionale dei diritti fondamentali il tribunale di Karlsruhe trae la conclusione che una interpretazione dei diritti fondamentali della Costituzione tedesca che ne limitasse l'ambito di validità (*Geltung*) al territorio tedesco e che svincolasse le autorità tedesche dagli obblighi loro derivanti dai diritti fondamentali e dai diritti dell'uomo nei confronti di cittadini stranieri all'estero, non sarebbe conciliabile con l'intimo legame che la Costituzione stabilisce tra diritti fondamentali e diritti dell'uomo.

L'argomentazione del giudice costituzionale, per quanto calata nel contesto ordinamentale tedesco, rileva in via generale. In effetti il testo costituzionale tedesco, contenendo al proprio interno il richiamo ai diritti dell'uomo, potrebbe rafforzare l'idea di una netta distinzione tra i due ambiti, quello dei diritti dell'uomo e quello dei diritti fondamentali. Tra l'altro, la dogmatica tedesca dei diritti fondamentali ha enfatizzato il riferimento letterale distinguendo diritti fondamentali riservati ai tedeschi e diritti fondamentali spettanti ad ogni uomo. Nella sentenza in commento, il Tribunale, dando per assunta questa distinzione, interviene nello spazio nel quale la titolarità dei diritti fondamentali è generale o universale, cioè non riservata ai tedeschi, per affermare una generale e tendenziale attrazione dei diritti fondamentali nell'orbita dei diritti dell'uomo. È il rafforzamento della presenza dello Stato tedesco all'estero ad esigere un ampliamento dell'efficacia dei diritti fondamentali. La tutela dei diritti fondamentali segue da vicino l'azione dei poteri pubblici, anche se questa si sposta all'estero. L'attrazione dei diritti dell'uomo facilita questo ampliamento del raggio di azione (96). Consapevole dei rischi dogmatici derivanti da un troppo stretto avvicinamento tra diritti dell'uomo e diritti fondamentali (in quanto diritti costituzionali), il Tribunale è attento a porre la questione nei termini dell'interpretazione conforme, per usare un termine ben noto alla dogmatica costituzionale italiana e tedesca: il legame che la Costituzione tedesca istituisce tra diritti fondamentali e diritti dell'uomo deve spingere a un'interpretazione dei primi alla luce dei secondi.

Come è ben noto, in questo ambito un ruolo centrale è svolto dalla CEDU, cui il giudice costituzionale dedica attenzione per osservare che non risulta chiaro l'ambito di validità della Convenzione in relazione all'azione degli Stati al di fuori del proprio territorio. La giurisprudenza convenzionale utilizza il criterio del controllo effettivo (*effective control*) sul territorio straniero da parte dello Stato in questione e su questa base

ha riconosciuto un'efficacia dei diritti convenzionali al di fuori del territorio nazionale dello Stato agente. E tuttavia -osserva il tribunale che cita i casi *Big Brother Watch* e *EGMR, Centrum för Rättvisa*, già sopra richiamati- in materia di sorveglianza elettronica estero-estero non c'è ancora chiarezza. In ogni caso la Convenzione non si oppone ad una efficacia dei diritti fondamentali tedeschi oltre il territorio nazionale (art. 53 CEDU).

Volgendo poi lo sguardo al diritto internazionale generale, il Tribunale ritiene che il vincolo dei diritti fondamentali verso le autorità tedesche che agiscono nella dimensione estero-estero non si traduce in una limitazione degli altri ordinamenti giuridici statali. Il vincolo riguarda infatti solo la responsabilità degli organi statali tedeschi. I diritti fondamentali intesi come diritti di difesa procedono parallelamente ai limiti derivanti dal divieto di ingerenza nella delimitazione dell'azione del potere statale all'estero.

Il Tribunale è accorto nel distinguere la dimensione interna da quella internazionale. Per la prima ciò che rileva è che l'azione dei poteri statali tedeschi, che nella specie si esplica attraverso misure di sorveglianza verso cittadini stranieri all'estero, abbia una base giuridica conforme alla Legge fondamentale. Il vincolo dei diritti fondamentali nulla dice, però, sulla legittimità delle misure dal punto di vista internazionale. La dimensione internazionale non è toccata dalla costruzione giuridica elaborata dal tribunale di Karlsruhe, il quale esplicitamente afferma che nulla impedisce agli Stati stranieri di sollevare dubbi e perplessità (103).

5. Osservazioni conclusive

La Legge fondamentale tedesca è notoriamente terreno molto fertile per la dogmatica dei diritti e delle libertà fondamentali. Non solo distingue tra diritti fondamentali dei tedeschi e diritti fondamentali spettanti a tutti ma, come si è avuto modo di osservare, si occupa anche dei diritti umani. Le novità apportate dalla sentenza in esame vanno collocate in questo sensibile contesto costituzionale.

A tal proposito una notazione preliminare riguarda il rapporto tra dogmatica e interpretazione costituzionale. La decisione in commento si muove nell'ambito di due diritti fondamentali -segreto delle telecomunicazioni e libertà d'informazione- che sono ritenuti diritti di spettanza universale dalla dottrina giuridica. L'interpretazione del Tribunale si è così appoggiata su questo assetto dogmatico al fine di estendere l'ambito di efficacia territoriale di tali diritti anche nei confronti di cittadini stranieri residenti in territorio straniero.

Il giudice costituzionale tedesco ha poi insistito sulla necessità di distinguere tra le diverse dimensioni dei diritti fondamentali, valorizzandone la dimensione difensiva, che ben può definirsi quella originaria e primigenia di tale specie di diritti. Con il progressivo estendersi del raggio d'azione dello Stato dal punto di vista spaziale, anche la dimensione difensiva dei diritti fondamentali amplia il proprio raggio d'azione. Nel caso di specie i ricorrenti hanno fatto valere la violazione dei loro diritti fondamentali appunto in tale dimensione difensiva (*abwehrdimension*). Riconoscere un'assenza di vincolo delle autorità tedesche in ragione del loro agire in uno spazio che il Governo

federale riteneva vuoto dal punto di vista dell'efficacia dei diritti (il Tribunale sostantivizza scrivendo "*Auslandsgerichtetheit*") avrebbe significato svuotare questa dimensione della sua efficacia. Ciò sarebbe stato tanto più inammissibile in quanto lo sviluppo tecnologico aumenta il rischio di aggressione ai diritti proprio all'estero e dall'estero (105).

Nell'accentuazione della dimensione difensiva dei diritti fondamentali vanno anche cercati i limiti dell'efficacia extraterritoriale dei diritti fondamentali, sebbene il Tribunale non abbia affrontato la questione espressamente. Pare plausibile sostenere che è la dimensione difensiva a godere dell'efficacia extraterritoriale, non anche quella positiva o pretensiva. Tra l'altro, la richiesta, da parte di cittadini di uno Stato estero, di un intervento dei poteri statali tedeschi sul territorio dello Stato estero, come è stato correttamente osservato, entrerebbe in contrasto con il principio territoriale radicato profondamente nel diritto internazionale[24].

Conclusivamente pare di poter dire che, in parallelo con i mutamenti storici e sociali in corso che toccano da vicino le componenti fondamentali della tradizionale nozione di Stato, anche la dogmatica e la teoria dei diritti fondamentali registrano mutamenti significativi. Il riconoscimento di un'efficacia extraterritoriale di alcuni diritti fondamentali è conseguenza diretta dei fenomeni di de-territorializzazione e di internazionalizzazione del diritto costituzionale individuati già da tempo dalla dottrina giuridica contemporanea. Il ragionamento che il Tribunale costituzionale federale ha sviluppato nella sentenza in commento non solo rafforza questa tendenza ma, nel riportare i diritti fondamentali nell'orbita dei diritti umani, è come se avesse creato una sorta, se non di gerarchia, di forza attrattiva che i diritti umani esercitano nei confronti dei diritti fondamentali. E qui si dovrebbe avviare un più ampio ragionamento sull'integrazione tra le 'giustizie' costituzionali intorno a beni costituzionali interdipendenti e indivisibili (come sono, all'evidenza, i due diritti fondamentali di cui si è ragionato in queste pagine) che porterebbe troppo lontano rispetto ai limitati obiettivi di queste pagine[25]. Basti per ora rinviare alle prossime decisioni della Grande Chambre della Corte europea dei diritti dell'uomo che, nei casi *Big Brother Watch* e *Centrum för Rättvisa*, potrebbe consolidare questo indirizzo in materia di efficacia extraterritoriale sul versante dei diritti dell'uomo.

[24] In tal senso B. Reinke, *Rights reaching beyond Borders*, in *Verfassungsblog.de*, 30 maggio 2020, 4.

[25] G. Zagrebelsky, *Corti costituzionali e diritti universali*, in *Rivista trimestrale di diritto pubblico*, 2006, 310.

Note a sentenza

Sezione Italia

"It's free" or maybe not: the convergent enforcement of Consumer and Data Protection Laws on personal data processing

Sara Gobbato

Regional Administrative Court of Lazio, 18 December 2019, no. 260
TAR Lazio, sez. I, 18 dicembre 2019, n. 260

Regional Administrative Court of Lazio, 18 December 2019, no. 261
TAR Lazio, sez. I, 18 dicembre 2019, n. 261

In light of the economic relevance of personal data as an asset in digital markets, in the relative commercial transactions envisaging personal data as a non-monetary consideration, the undertakings shall provide the consumers with clear, complete and non-deceptive information in compliance with the applicable consumer law. Accordingly, the consumer shall be made aware of the actual commercial terms of the transaction entailing the provision of a service against personal data.
There is no incompatibility or antinomy between data protection and consumer laws, since they are complementary, imposing specific information obligations in relation to their respective protection purposes. On the one hand, data protection rules aim to protect personal data as a fundamental right of the individual; on the other hand, consumer rules ensure that correct information is provided to consumers in order to adopt informed economic choices.
For the same reasons, it can be excluded the risk of "a multi-sanctional effect" against the same conduct by the same undertaking. Indeed, data protection and consumer Authorities scrutinise different conducts of the undertaking, relating in the first case to the correct processing of personal data pursuant to data protection law, and in the second case to the clarity and completeness of the information about the exploitation of the data for commercial purposes pursuant to consumer law.

Summary

Keywords

Personal data - GDPR - consumer law - Facebook - AGCM

1. Introduction

By twin judgments released on 10 January 2020[1], the Lazio Regional Administrative Court[2] partly overturned the decision no. 27432/2018[3] of the Italian Competition and Consumer Authority (*Autorità Garante della Concorrenza e del Mercato,* AGCM), which fined Facebook Inc. and its Irish subsidiary Facebook Ireland Ltd. for 10 million euro[4] for two unfair commercial practices against the Social Network's Italian users. At the time of writing, Facebook has appealed the judgments before the Italian Supreme Administrative Court (*Consiglio di Stato*), which will have the final say on the matter.

Although still subject to final judicial review, the first instance ruling is remarkable since it highlights crucial issues with regard to personal data processing and the enforcement of consumer and data protection laws. As it will pointed out in the following, the Regional Administrative Court confirmed that, when exploited for commercial purposes, personal data correspond both to a personal right of the data subject protected by the General Data Protection Regulation (GDPR)[5], and to an economic asset amounting to a contractual consideration subject to the Italian Consumer Code[6]. The envisaged "double nature" triggers the risk of convergent proceedings and double fines issued by both the Data Protection and the Consumer Authorities against the same commercial practice of the same undertaking scrutinised from different angles.

In order to avoid that the potential convergent enforcement causes legal uncertainty and an excessive compliance burden to the detriment of undertakings, innovation and ultimately consumer welfare, we would argue that the need of more precise boundaries between applicable rules should be considered pursuant to the *ne bis in idem* principle.

---

1 Regional Administrative Court (TAR) of Lazio, 18 December 2019, nos. 260 and 261.

2 Under Italian law, the Lazio Regional Administrative Court (based in Rome) holds exclusive competence to reviewing AGCM's decisions in first instance.

3 AGCM, decision no. 27432 of 29 November 2018, PS11112 – Facebook – Condivisione dati con terzi, in Boll. 46/2018.

4 Pursuant to the Italian Consumer Code, AGCM is allowed to issue administrative fines up to 5 million euro for each envisaged unfair commercial practice realised by an undertaking against consumers. In the case under review, therefore, AGCM issued the highest fine allowed by Italian law in respect of the two commercial practices ascribed to Facebook. Please note that by means of the new Directive (EU) 2019/2161, the European Union requests Member States to increase to at least 4% of the annual turnover of the undertaking concerned, the administrative fines to be issued starting from 2022 for unfair practices with an EU dimension (i.e. affecting more than one Member State). In this respect, see 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, OJ L 328, 18.12.2019, 7–28.

5 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), OJ L 119, 4.5.2016, 1–88.

6 Legislative Decree no. 206/2005 that implemented in Italy Directive 2005/29/EC on unfair commercial B2C practices to the detriment of consumers.

2. The challenged AGCM decision

By decision no. 27342/2018, the AGCM found that Facebook engaged in a first misleading commercial practice, prohibited by Arts. 21 and 22 of the Italian Consumer Code. The conduct consisted of the insufficient information provided to the Italian users during their first registration to the Platform. In that phase, by means of the claim «Sign up, it's free and it will be forever», Facebook highlighted the free nature of the service without specifying that the personal data collected would have been processed for commercial purposes. According to AGCM, the lack of information was not overcome by the link to the data protection notice available on the registration page, since «the absence of an alert on a relevant element of the contract such as the commercial use of user data, determines a serious information incompleteness that cannot be remedied by a mere references to further details»[7].

The AGCM has also ascertained a second aggressive practice, prohibited by Arts. 24 and 25 of the Italian Consumer Code. According to the evidence gathered by the Authority, Facebook automatically pre-set the transmission of the user data, for profiling and commercial purposes, from the Social Platform to third party websites/apps and vice versa without the prior express consent of the data subject. The latter had a mere opting-out option, which was discouraged by Facebook by alleging consequent difficulties in the use of the services.

In the course of the proceedings, Facebook argued that the provision of "free" services, in the absence of monetary compensation, does not constitute a relevant economic activity within the meaning of the Consumer Code. In addition, according to Facebook, AGCM acted «beyond its competence in so far as it uses consumer protection rules to analyse conduct that should be assessed on the basis of privacy and data protection legislation»[8]. Hence, the case pertained to the competent Data Protection Authority pursuant to GDPR, namely the Irish Data Protection Commission (in view of the EU State of establishment of Facebook's subsidiary), rather than AGCM.

In rejecting both arguments, in line with the conclusions reached in the 2017 WhatsApp case[9], the AGCM first confirmed that the processing of user data for marketing purposes entails a «consumer relationship […], even in the absence of a monetary compensation», since user data are in effect a «non-monetary consideration»[10].

In addition, AGCM confirmed its competence on the case, clarifying that «the fact that the company's conduct is subject to privacy law does not exempt it from complying with the rules on unfair business practices». While the enforcement of data protection law pertains to the Data Protection Authority, the Consumer Code has a different

[7] AGCM decision no. 27432/2018, § 56. Unofficial translation from the Italian official text.

[8] Ivi, § 34. Unofficial translation from the Italian official text.

[9] AGCM, decision no. 26597 of 11 May 2017, PS10601 – WhatsApp – Trasferimento dati a Facebook, in Boll. 18/2017. In that proceedings, AGCM sanctioned WhatsApp 3 million euro for an unfair commercial practice of an aggressive nature pursuant to arts. 20, 24 and 25 of the Italian Consumer Code, concerning the modification of the general terms and conditions. AGCM confirmed that WhatsApp's conduct amounted to an unfair commercial practice due to the economic value of the users' personal data, which constitute a "non-pecuniary consideration".

[10] AGCM, decision no. 27342/2018, § 54. Unofficial translation from the Italian official text.

scope, which is to protect the consumer from economic choices induced by misleading and aggressive practices that are not covered by other specific regulations. According to AGCM, therefore, «the two legal frameworks have a different material scope of application and pursue different interests. Consequently, there is no conflict between the two set of rules, but rather they complement each other»[11].

3. The Administrative Court ruling

By the twin judgments released on 10 January 2020, the Lazio Regional Administrative Court annulled the AGCM decision no. 27342/2018 as regards the second aggressive conduct relating to the alleged data sharing without the user' express consent. The Court found that, in light of the evidence provided by Facebook, the envisaged data sharing mechanism correctly required the user's express consent "on a granular basis" for each individual third party app/website.

The Court confirmed the first unfair commercial practice relating to the insufficient information provided to the consumer at the time of the first registration to the Social Network. This conclusion was reached by the Court by providing useful compliance clarifications, applicable to all offers apparently provided "for free" in the absence of a monetary compensation.

First, the Court confirmed that personal data might have a "double nature". Indeed, they are the object of a fundamental right of the individual fulfilled by data protection laws, but they can also be an exploitable economic asset amounting to a contractual compensation. Accordingly, economic services provided against user data must comply with the Consumer Code as regards the duty to provide clear, complete and non-deceptive information on the actual commercial use of the personal data. Such information shall be available to the users from the first phase of registration to the platform, and shall effectively enable them to understand the terms of the agreement.

The Court confirmed also that, as pointed out by the AGCM, the mere link to Facebook's Data Policy, Terms of Use and Cookie Policy (available on the registration page) is not an effective remedy, since the information accessible through links is «neither clearly nor immediately perceived» by the consumer.

In any case, the undertakings cannot claim that the economic relevance of personal data is something new. Indeed, in addition to the aforementioned WhatsApp case of 2017, this principle is recognised in the 2016 Guidelines for the implementation/application of Directive 2005/29/EC, where the European Commission points out that «personal data, consumer preferences and other user-generated content have a '*de facto*' economic value»[12].

[11] Ivi, § 46. Unofficial translation from the Italian official text.

[12] European Commission, Staff working document, Guidelines for the implementation/application of Directive 2005/29/EC on unfair commercial practices, 25.05.2016, SWD(2016) 163 final. In this respect, we could also note that the economic relevance of personal data has been codified, for instance, by 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, OJ L 136, 22.5.2019, 1–27. Directive (EU) 2019/770 expressly protects consumers in those contractual relationships where

The "dual nature" of personal data has further consequences for companies under a compliance point of view. Indeed, depending on the business model of the undertaking concerned, the data protection policy pursuant to Art. 13 GDPR may result not sufficient in order to avoid further responsibilities regarding the commercial exploitation of their personal data pursuant to the Consumer Code. In other terms, personal data processing triggers the risk of two concurrent (or convergent) sanctions for the same data processing activity: one for any violation of the GDPR (with penalties up to 4% of the annual turnover)[13], and another for breach of the Consumer Code (with penalties that, currently in Italy[14], are up to 5 million euro for each unfair conduct ascertained by AGCM).

Taking into account the different scope of data protection and consumer regulations, in the judgements at hand the Regional Administrative Court expressly excluded the risk that such an approach could lead to "a multi-sanctional effect" ("*effetto pluri-sanzionatorio*") against the same conduct by the same undertaking. Indeed, according to the Court, the Italian Data Protection Authority and the AGCM would scrutinise «different conducts of the undertaking, relating in the first case to the correct processing of personal data for the purposes of using the platform, and in the second case to the clarity and completeness of the information about the exploitation of the data for commercial purposes»[15].

4. The obligation to inform the data subject between the Consumer Code and GDPR

At the time of the 2018 AGCM decision, Facebook's registration page displayed the claim «Sign up, it's free and it will be forever».

Subsequently, in light of the AGCM's remarks, Facebook changed the wording in «It's fast and simple», thus eliminating any reference to the free nature of the service provided. When accessing the registration page where this further claim was displayed, after having filled-in certain identification data, users were informed by a general notice that, by clicking on «Sign up», they were going to accept Facebook's Terms and Conditions. The same notice provided *a link* to the Data Policy, inviting the users to find out how Facebook collected, used and shared their information; a further link was

a digital content/service is provided against user data (see Art. 3 of Directive (EU) 2019/770: «This Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price. This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose»).

[13] See Art. 83 GDPR.

[14] See Art. 27 of the Italian Consumer Code.

[15] Tar Lazio, judgements nos. 260/2019 and 261/2019, § 9 (*on the law*). Unofficial translation from the Italian official version.

provided to the Cookies Policy[16]. In other words, by clicking on «Sign up», by means of a single action on the part of the users, they were going to accept the Terms and Conditions as well as the Data and Cookie Policies.
According to the AGCM decision and Court ruling at hand, in conjunction with a first claim inviting to join the service and in any case before signing up a contract, the consumers shall be provided with two distinct sets of information: according to the Consumer Code, the consumer shall understand the economic relationship between the services received and the personal data to be processed; in addition, they should be provided with the information listed by Art. 13 GDPR.
The existence of two distinct informative obligations (one pursuant to the Consumer Code and one pursuant to GDPR) seems to have been confirmed by a more recent proceedings initiated by AGCM against Facebook for non-compliance with the decision no. 27342/2018, with respect to the first unfair practice upheld by the Court. In this further proceeding, AGCM stated that the removal of the claim «It's free» is not sufficient to comply with the Consumer Code. Indeed, according to the Authority, the consumer who wants to register to the Social Network is still not informed clearly and immediately about the commercial purposes of their data exploitation[17].

5. Looking for boundaries: the *ne bis in idem* principle

A question arises: what is the impact of the aforementioned potential convergent enforcement of consumer and data protection rules?
On the one hand, for big players such as Facebook, the convergent enforcement does not prove particularly effective due to the fragmented and lengthy procedures launched at national level and the relatively limited amount of the fines. This first shortcoming is going to be addressed by the new Directive (EU) 2019/2161[18] that requires Member State to increase the sanctions applicable from 2022 to infringements with an EU dimension, pursuant to Regulation (EU) 2017/2394 on cooperation between EU National Consumer Authorities[19].
On the other hand, the convergent interventions by data protection and consumer authorities may enhance legal uncertainty and the related compliance costs (especially

[16] Source: *it-it.facebook.com*, accessed on 31 January 2020. The Italian wording said: «[c]*liccando su Iscriviti, accetti le nostre Condizioni. Scopri in che modo raccogliamo, usiamo e condividiamo i tuoi dati nella nostra Normativa sui dati e in che modo usiamo cookie e tecnologie simili nella nostra Normativa sui cookie. Potresti ricevere notifiche tramite SMS da noi, ma puoi disattivarle in qualsiasi momento*».

[17] AGCM, decision no. 28072 of 21 January 2020, IP330 - Facebook-Raccolta utilizzo dati degli utenti, in Boll. 4/2020, spec. § 7: «*[c]on particolare riferimento all'unica modifica attuata in relazione alla pagina di registrazione al social network, ossia la rimozione del claim di gratuità, si osserva come essa non sia sufficiente a rimuovere gli accertati profili di illegittimità. Il consumatore che si voglia registrare al social network continua a non essere informato con chiarezza e immediatezza in merito alle finalità commerciali della raccolta e utilizzo dei suoi dati da parte della società*».

[18] See *supra* note 4.

[19] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004, OJ L 345, 27.12.2017, 1–26.

for small and medium-sized enterprises), to the detriment of economic development, innovation and ultimately consumer welfare. To avoid this second shortcoming, the need of more precise boundaries between the applicable rules should be considered pursuant to the *ne bis in idem* principle, enshrined by Art. 4 of Protocol no. 7 to the Convention for the Protection of Human Rights and Fundamental Freedoms and by art. 50 of the Charter of Fundamental Rights of the European Union[20]. As clarified by the European Court of Human Rights (ECHR), the *ne bis in idem* principle applies to the administrative Authorities, such as the Italian AGCM and Data Protection Authority, which may issue administrative fines that, although not formally "criminal" under national law, have a substantial punitive nature with both preventive and repressive functions[21].

The *ne bis in idem* principle does not preclude national legal systems from providing for complementary repressive responses, by different autonomous authorities, in relation to the same conduct that infringes different legal provisions[22]. On the contrary, as clarified by the ECHR, the imposition, by different authorities, of different sanctions on the same conduct is compatible with the *ne bis in idem* principle if certain conditions are met. In particular, the different proceedings shall pursue complementary objectives not only in an abstract sense, but also in concrete terms, i.e. having regard to the different aspects that are the object of the investigation with regard to the illegal conduct in question[23].

To comply with this criterion, in the decision to start an enforcement proceeding, each Authority should therefore clearly provide not only *in abstracto* but also *in concreto* the

[20] Art. 50 (Right not to be tried or punished twice in criminal proceedings for the same criminal offence): «No one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law».

[21] ECHR, *A. Menarini Diagnostics Srl c. Italia*, app. no. 43509/08 (2011).

[22] ECHR, *A and B v Norway*, apps. nos. 24130/11 and 29758/11 (2016), § 121: «In the view of the Court, States should be able legitimately to choose complementary legal responses to socially offensive conduct (such as non-compliance with road-traffic regulations or non-payment/evasion of taxes) through different procedures forming a coherent whole so as to address different aspects of the social problem involved, provided that the accumulated legal responses do not represent an excessive burden for the individual concerned».

[23] *A and B v Norway*, cit., §§ 131-132: «As regards the conditions to be satisfied in order for dual criminal and administrative proceedings to be regarded as sufficiently connected in substance and in time and thus compatible with the *ne bis* in idem criterion in art. 4 of Protocol no. 7, the relevant considerations deriving from the Court's case-law, as discussed above, may be summarised as follows. Material factors for determining whether there is a sufficiently close connection in substance include: (i) whether the different proceedings pursue complementary purposes and thus address, not only *in abstracto* but also *in concreto*, different aspects of the social misconduct involved; (ii) whether the duality of proceedings concerned is a foreseeable consequence, both in law and in practice, of the same impugned conduct (idem); (iii) whether the relevant sets of proceedings are conducted in such a manner as to avoid as far as possible any duplication in the collection as well as the assessment of the evidence, notably through adequate interaction between the various competent authorities to bring about that the establishment of facts in one set is also used in the other set; (iv) and, above all, whether the sanction imposed in the proceedings which become final first is taken into account in those which become final last, so as to prevent that the individual concerned is in the end made to bear an excessive burden, this latter risk being least likely to be present where there is in place an offsetting mechanism designed to ensure that the overall amount of any penalties imposed is proportionate».

factual elements that underpin its action and its competence according to the law. In conclusion, in this respect, a substantial compliance with the duty to state reasons, subject to effective judicial review, confirms to be crucial to set more precise boundaries between convergent interventions and responsibilities on personal data processing.

Commenti

Schrems II: The Right to Privacy and the New Illiberalism

Francesca Bignami*

Corte di giustizia dell'Unione europea, 16 luglio 2020, C-311/18, *Data Protection Commissioner c: Facebook Ireland, Maximillian Schrems*

Summary

1. Introduction. - 2. Interference with democracy through Facebook (and other global communications actors). - 3. The Trump administration. - 4. Brexit. - 5. Expansive surveillance laws in the EU Member States.

Keywords

Facebook - data protection – Schrems II – Brexit – Trump

1. Introduction

On its face, *Schrems II* is a sequel. Decided on July 16, 2020, the Court of Justice of the EU (CJEU) found that the EU-US data protection agreement[1] ("Privacy Shield") that had served as one of the bases for Facebook's transfer of personal data to the US was invalid. Because Privacy Shield could not guarantee an adequate level of protection for EU personal data in the event of access by US intelligence agencies, the CJEU found that it was in violation of the right to data protection. This judgment was handed down five years after *Schrems I*[2], where the CJEU had ruled that Privacy Shield's predecessor agreement was invalid, in litigation involving the same parties, the same, Irish, Data Protection Authority (DPA), and the same US intelligence programs.

But for all the similarities, it is critical to appreciate that the judgment in *Schrems II* speaks to a radically changed political world. Since 2015, when *Schrems I* was decided, a lot has happed. First, as has been extensively documented in the press and official reports, Russia, Cambridge Analytica, and other bad actors have exploited the privacy vulnerabilities of US-based Facebook to interfere with elections and democratic societies. Second, in November 2016, Trump was elected US President and since then he

*Includiamo in questa speciale sezione i commenti pubblicati da Francesca Bignami e Oreste Pollicino su *Verfassungsblog.de* rispettivamente in data 29 luglio 2020 e 25 luglio 2020. I commenti sono riprodotti con il consenso degli autori.

[1] 2000/520/EC, Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

[2] CJEU Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (2015).

and his administration have undermined fundamental principles of US liberal democracy. Third, in June 2016, the UK voted to leave the EU, and on January 31, 2020, it did, taking with it its powerful security and intelligence apparatus (subject to a transitional period that expires on December 31, 2020). Fourth, all the while, EU Member States have enacted expansive surveillance laws[3], some in response to terrorist attacks like the Paris one in November 2015, others as part of a larger pattern of democratic backsliding[4].

The rest of this post unpacks the implications of *Schrems II* for this new, unstable, and in many instances, illiberal political landscape. A number of excellent posts on this blog[5] have already examined the impact of *Schrems II* on the corporate actors that transfer EU data globally. My focus here is on how *Schrems II* and the CJEU's evolving jurisprudence on the right to privacy can be read as targeting the political developments of recent years.

2. Interference with democracy through Facebook (and other global communications actors)

First, interference with democracy through Facebook: One of the important lessons of the past five years has been that privacy breaches, wherever they occur, make democracies vulnerable, wherever they are. The first part of *Schrems II* details how, under EU law, EU privacy officials should address this problem. There the CJEU discusses the EU's interlocking system[6] of standard contractual clauses (SCCs) and third-country adequacy decisions for protecting the privacy of EU personal data when it is transferred abroad by corporate actors. A SCC is what Facebook relied on for making data transfers to the US but the adequacy decision (based on Privacy Shield) was also necessary, to guarantee respect for privacy if Facebook data ended up in the hands of the US government.

What is striking is the CJEU's emphasis on the duties and powers of DPAs to enforce EU privacy standards when data is sent abroad. This has always been a secondary area of DPA activity, in my view because of the discrepancies between DPA resources and the corporate actors and the foreign jurisdictions that they are supposed to be monitoring. How exactly is the relatively small Irish DPA supposed to monitor the third-country transfers of the disproportionate number of digital multinationals that have established their EU internal market presence via Ireland? As a result, historically, most of the action on third-country transfers has been at the EU level, in the form of European Commission third-country adequacy decisions, standard contractual clauses,

[3] M. Rotenberg – E. Kyriakides, *Preserving Article 8 in Times of Crisis*, in F. Bignami (ed.), *EU Law in Populist Times. Crises and Prospects,* Cambridge, 342 ss.

[4] K.L. Scheppele - R.D. Kelemen, *Defending Democracy in EU Member States,* in F. Bignami (ed.), *EU Law in Populist Times,* cit., 413 ss.

[5] G. Chuches – M. Zalnieriute, *A Groundhog Day in Brussels: Schrems II and International Data Transfers*, in *Verfassungsblog.de*, 16 July 2020; O. Pollicino, *Diabolical Persistence. Thoughts on the Schrems II Decision,* ivi, 25 July 2020; S. Tewari, *Schrems II – A brief history, an analysis and the way forward*, ivi, 25 July 2020.

[6] European Commission, *Data Protection - International dimension of data protection*.

and binding corporate rules.

In *Schrems II*, however, the CJEU came down in favor of more DPA enforcement in the context of third-country transfers. In its detailed description of the enforcement system, the DPAs are the essential backstop for contractually-based transfers to third countries: if they find that the terms of standard contractual clauses are not being complied with in third countries, they must either suspend or prohibit the transfer (paras. 145-148). Even in the case of third-country transfers based on adequacy decisions, DPAs play an essential role: as the Irish DPA did in *Schrems II* with respect to the Privacy Shield decision, DPAs are obliged to refer any doubts as to whether a country has "adequate" privacy to their national courts, which in turn are to refer the issue to the CJEU (paras. 119, 120). Ultimately, the upshot of more DPA enforcement will be the need for more data localization by commercial actors—something that the CJEU has already indicated for law enforcement actors in its *Tele2* judgment[7].

3. The Trump administration

Second, the Trump administration: The first part of the *Schrems II* judgment and its emphasis on enforcement applies not just to data transfers to the US but to all foreign jurisdictions. As many *Schrems II* commentators[8] have correctly noted[9], ensuring adequacy is far more difficult, and unlikely, in the case of transfers to authoritarian regimes like China. But the second part of *Schrems II* concerns specifically the (in) adequacy of US privacy guarantees for EU personal data in intelligence surveillance. In assessing (in)adequacy, the CJEU's analysis was strictly limited to the US law on the books. However, it certainly didn't help that the Trump administration has relentlessly politicized and circumvented the executive branch, including the intelligence and foreign policy establishment, which in the Privacy Shield bore significant responsibility for protecting EU privacy.

As is well known, there is a legal vacuum in US constitutional law for the privacy of non-US persons[10]. (In statutory law[11], a "US person" is defined as either a citizen or a permanent resident, and a "non-US person" as everyone else; the constitutional law case[12] on point speaks of foreign citizens and residents "with no voluntary attachment" to the US.) Since 9/11, this constitutional vacuum has been used first by the President (under Article II) and then by Congress (with the enactment of Section 702 of the FISA Amendments Act) to expand the surveillance powers of the intelligence com-

7 CJEU Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB* (2016).

8 K. Propp - P. Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, in *lawfareblog.com,* 17 July 2020.

9 J. Daskal, *What Comes Next: The Aftermath of European Court's Blow to Transatlantic Data Transfers*, in *justsecurity.org,* 17 July 2020.

10 NSA PROGRAMS, Hearing Before the House Permanent Select Committee on Intelligence, *Written Testimony of Stephen I. Vladeck* - October 29, 2013.

11 50 U.S. Code § 1801.

12 *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990)

munity and, to a lesser extent, law enforcement. In the long fall out from the Snowden revelations, US diplomacy has been geared at assuring the EU that the surveillance of non-US persons in the *institutional practice* of the executive branch is far less expansive and much more privacy protective than it might seem from the *letter of the law*. This was the gist of President Obama's PPD-28 and the Office of the Director of National Intelligence, Department of Justice, and State Department annexes to the Privacy Shield. Even pre-Trump, the executive branch assurances given in PPD-28 and the Privacy Shield would likely not have convinced the CJEU. In *Schrems II*, the absence of recourse to an independent court was the major flaw with the US system that was singled out by the CJEU. Effective judicial redress has always been essential to the CJEU's data protection jurisprudence and the fact of the matter is that it doesn't exist in intelligence surveillance, especially for non-US persons. However, Trump's election and the breakdown of a variety of institutional norms, sealed Privacy Shield's fate.

In the Privacy Shield, an ombudsman within the State Department was supposed to serve as the executive branch's institutional alternative to courts. To quote from the State Department's website[13].

«The Under Secretary [i.e. the Privacy Shield Ombusdman] reports directly to the Secretary of State and is independent from the Intelligence Community. To carry out the Ombudsperson duties, the Under Secretary works closely with other United States Government officials, including independent oversight bodies such as inspectors general, as appropriate, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies»

But without any apparent legal or even significant political fallout, Trump dismissed[14] first the Inspector General for the Intelligence Community in April 2020 and then the Inspector General for the State Department in May 2020. Under such conditions, where dismissal appears to be entirely at will, it is difficult to believe the claim of independence.

In short, the credibility of the internal, executive branch safeguards detailed in the Privacy Shield has suffered during the Trump administration. The CJEU's repeated insistence in *Schrems II* on independent courts as the essential guarantors of privacy can be seen, at least in part, as a response to this experience.

4. Brexit

Third, Brexit: Once the Brexit transitional period expires on December 31, 2020, the UK will be, legally speaking, a third country. In *Schrems II*, the CJEU made it clear that, as a third country, all aspects of the UK's privacy regime, including national security, will fall under the scope of the General Data Protection Regulation (GDPR)[15], and

[13] U.S. Department of State, *Privacy Shield Ombudsperson*.

[14] J. Tillipman, *Trump's latest ethical violation: Firing the State Department's inspector general*, in *Usa Today Opinion*, 22 May 2020.

[15] 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

will be subject to the requirement of adequacy (paras. 87-88). Moreover, the CJEU said that the analysis of third-country adequacy proceeds entirely based on the GDPR, read in light of the EU Charter of Fundamental Rights (para. 101)—not the European Convention of Human Rights, which is believed by many to be less demanding on the privacy issue[16]. This is particularly significant for the UK since its security and intelligence agencies conduct extensive bulk interception, collection, and "equipment interference," i.e. hacking[17].

Beyond the UK's own surveillance capacity, it is known to collaborate extensively with foreign governments, including the US, as part of the Five Eyes Agreement[18]. For law enforcement purposes, now there is also the UK-US CLOUD Act Agreement[19] for police access to stored communications, as well as for real-time wiretaps of wire and electronic communications; this agreement specifically contemplates US access to the communications of third-country nationals[20] handled by UK providers, e.g. EU persons. As the prospect of a "hard" Brexit has become a reality, the UK government has pivoted even closer to the US, with implications for more US-UK data sharing and privacy rights—and for the adequacy of UK law from the perspective of EU personal data.

A good preview of what the Brexit future might look like is *Elgizouli v. Secretary of State for the Home Department*[21]. That case involved a UK MLAT transfer of criminal evidence to the US, without the standard assurances from the US government of (not) seeking the death penalty. The UK Supreme Court found that the UK government's transfer was unlawful because the government had failed to comply with the UK Data Protection Act 2018, which poses strict limitations on third-country transfers for law enforcement purposes. In the future however, with the many anticipated changes that will be made to statutory law, the UK courts will not be able to exercise the same judicial review powers. *Schrems II* serves as a useful affirmation and reminder that EU law, EU DPAs, and the CJEU will step in when EU personal data is at stake.

5. Expansive surveillance laws in the EU Member States

Fourth and last, crisis-fueled, expansive surveillance legislation[22] in many Member

of such data, and repealing Directive 95/46/EC.

16 K. Irion, *Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law*, in *European Law Blog*, 24 July 2020.

17 [2019] EWHC 2057.

18 S. Kim - P. Perlin, *Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance*, in *lawfareblog.com*, 25 March 2019.

19 J. Daskal, *The UK-US CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, in *justsecurity.org*, 8 October 2019.

20 A. Gidari, *The Big Interception Flaw in the US-UK Cloud Act Agreement*, in *cyberlaw.stanford.edu*, 18 October 2019.

21 [2020] UKSC 10.

22 V. Mitsilegas, *The Preventive Turn in European Security Policy*, in F. Bignami (ed.), *EU Law in Populist Times*, cit., 301 ss.

States: For various reasons, European statutory law has typically not relied on the categorical distinction between foreigners and citizens/permanent residents that is so important for US privacy law. In a set of recently decided fundamental rights cases[23] (for the European Court of Human Rights, see the German Constitutional Court's discussion at para. 271), this is becoming a matter of constitutional law too—foreigners without any physical connection to the territory of the surveilling nation nonetheless have rights if they are subject to the surveillance of that nation. What is striking, however, are the surveillance powers that are emerging in some places with respect to all persons, including resident nationals. A Swedish intelligence law that was litigated, and found to be lawful by the European Court of Human Rights[24], provides for intelligence interception, based on "tasking directives," of all "cable-based cross-border communications"—surveillance powers that do not seem far off from the National Security Agency's Section 702 programs[25], but without the safeguards that exist there for US persons. In the CJEU, there is currently a pending UK case[26] that involves intelligence orders for bulk communications data—something that is simply a more tailored version of the National Security Agency's original Section 215 program[27]. There is also a pending French case[28], where among the intelligence tools at issue is real-time algorithmic surveillance of the metadata generated by domestic communications networks to identify security threats.

In the UK and French cases, the CJEU has been called upon to evaluate privacy in intelligence surveillance *internally*, in the activities of *Member State* security and intelligence services. *Schrems II*, which has been decided first, might possibly be a first step in developing a CJEU jurisprudence on privacy in mass surveillance programs. The UK and French cases raise the threshold issue of whether EU fundamental rights law applies in the context of the activities of Member State security agencies. This is tied to the Treaty on European Union's exclusion from EU competences of national security. If the CJEU does find that EU law applies, it will have to address the question of what privacy standards govern in the context of national security surveillance. On this, it is clear from *Schrems II* that independent courts should have oversight and remedial powers but otherwise the judgment is quite vague. The unstable geopolitics and the illiberal developments of the past couple of years highlight the many competing

[23] Bundesverfassungsgericht, *In their current form, the Federal Intelligence Service's powers to conduct surveillance of foreign telecommunications violate fundamental rights of the Basic Law*, Press Release No. 37/2020 of 19 May 2020, Judgment of 19 May 2020, 1 BvR 2835/17

[24] ECtHR, *Centrum för rättvisa v. Sweden*, app. no. 35252/08 (2019).

[25] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 23 January 2014.

[26] AG Opinion, Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service* (2020).

[27] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court,* cit.

[28] AG Opinion, Joined Cases C-511/18 and C-512/18, *La Quadrature du Net (C-511/18 and C-512/18), French Data Network (C-511/18 and C-512/18), Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 and C-512/18), Igwan.net (C-511/18)* (2020).

considerations—combating election interference based on the unlawful manipulation of personal data is one of the important activities of national security agencies, yet at the same time expansive surveillance laws threaten rights and, in the case of democratic-backsliding, can be used to consolidate authoritarian rules.

Diabolical Persistence. Thoughts on the *Schrems II* Decision

Oreste Pollicino

Summary

1. Introduction. - 2. The diabolical perseverance of the European Commission (for slightly more than two decades). - 3. Judicial Manipulation of the CJEU reloaded and the training as a European Constitutional Court. - 4. Final remarks.

Keywords

Privacy Shield - Schrems II - data protection – data transfer - privacy

1. Introduction

As Genna Churches and Monika Zalnieriute wrote[1] on 16 July, the day on which the *Schrems II* decision was published, reading the judgment gives more than a simple feeling *déjà vu*; it rather looks like a full-blown Groundhog Day: One has the impression of being trapped in a time loop that forces us to relive the day – 6 October 2015 – on which the Court of Justice of the European Union (CJEU) adopted *Schrems I* and invalidated the European Commission's Safe Harbour Decision[2] (*Safe Harbour*) adopted on 26 July 2000.

Moving from cinema to the world of the classics, there is a famous Latin maxim according to which *"errare humanum est perseverare autem diabolicum"*, meaning "whilst is it human to err, it is diabolical to persist with the same mistake".

More than a week after the *Schrems II* judgment was adopted, following the hundreds

[1] G. Chuches – M. Zalnieriute, *A Groundhog Day in Brussels: Schrems II and International Data Transfers*, in *Verfassungsblog*, 16 July 2020.

[2] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

of comments made on the subject, I shall modestly attempt to consider the judgment (and the underlying saga) from two particular viewpoints, drawing inspiration from the Latin maxim mentioned above.

First of all, I shall focus on the diabolical persistence of the European Commission and secondly on judicial manipulation as the original sin of the CJEU and its (not so hidden) ambitions and frustrations (of not being a Constitutional Court).

2. The diabolical perseverance of the European Commission (for slightly more than two decades)

It is 15 May 2000 in Brussels. One of the giants of European Privacy, Stefano Rodotà, head of the Italian Data Protection Authority and the Working Party on Article 29, essentially authored the opinion in which that Working Party[3] clearly set out its concerns on the Commission's draft adequacy decision. The main concerns focused in particular on the need for clarity as regards the scope of *Safe Harbour*, the narrowing of exceptions and exemptions as well as the need for appropriate guarantees in relation to individual redress.

A few months later, on July 6, the European Parliament Report (Elena Paciotti as rapporteur and a fundamental rights defender) on the Commission's draft clearly emphasised that «adequate protection does not mean per se that the third country should have the same rules as the Union but that, regardless of the type of legislative protection in force in the third country, the data subject must be effectively protected». It then concluded solemnly, asking the European Commission «to append this resolution to its transmission letter to the United States authorities, thereby clearly emphasising Parliament's concern about the absence of an individual right of judicial appeal and the failure of an agreement to oblige companies to pay compensation for unlawfully processed data».

As can be imagined, the strong concerns were not enough to lead the European Commission to change its position, and the draft was approved without further amendment. Moreover, 15 years later the CJEU restated this basic position in *Schrems I*, pointing out exactly the same concerns as raised in 2000 by the Working Party on Article 29 and by the European Parliament.

The adequacy decision was invalidated, the *Safe Harbour* umbrella was torn, and there were reasonable expectations that a new transatlantic agreement would take on board the original concerns raised vocally by the CJEU.

The expectations became even greater after the CJEU had developed the new activist approach within its case law on the judicial enforcement of digital privacy: not only in *Schrems I* but also, less than a year before, *in Digital Rights Ireland*[4] and *Google Spain*[5].

[3] Article 29 Data Protection Working Party, *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"*, WP 32, CA07/434/00/EN.

[4] Joined Cases C-293/12 and C-594/12 (2014).

[5] CJEU Case C-131/12 (2014).

As it has been written by Giovanni De Gregorio[6] at the end of the last century, the Union adopted a liberal approach. A strict regulation of the online environment would have damaged the growth of the internal market, exactly when new technologies were going to revolutionize the entire society and promised new opportunities for the internal market. The end of this first liberal season was the consequent new activist approach by the CJEU, aiming at stricter intervention. This was the result of the Nice Charter as a bill of rights and new challenges raised by private actors in the digital environment.

In any case, the mentioned expectations essentially amounted to nothing: *Privacy Shield*, the successor of *Safe Harbour* did not fulfil them.

For the second time, the final compromise was a winning one for US commercial ambitions and a losing one for those who persisted in asking European Union negotiators to take privacy and data protection rights seriously as European constitutional rights enshrined in the European Charter of Fundamental Rights (ECFR).

Among the many weak points, two are particularly evident. They show that *Privacy Shield* did not correct the practical and legal issues associated with the Court's invalidation of *Safe Harbour* as the previous regime. First, the national security concerns of United States authorities appear to have enjoyed absolute primacy over the protection of personal data of EU citizens under the European Commission's arrangement with the United States. Secondly, there does not appear to be any mechanism for ensuring effective redress for EU citizens against such intrusions on fundamental rights. Both of these were already key arguments for the CJEU in invalidating the decision in *Schrems I* (§§ 86-90).

Against this backdrop, it would probably have been a set bet that, alongside Arts. 7 and 8, the ECFR provisions engaged by the CJEU would have been Art. 52 (proportionality) and Art. 47 (right to an effective remedy).

The Court held in relation to the former provision that U.S. surveillance programs, which the Commission assessed in its *Privacy Shield* decision, are not limited to that which is strictly necessary and proportional, as is required by EU law. With respect to Art. 47 ECFR, the Court held (surprise surprise, following the mantra of the last 20 years) that, as far as U.S. surveillance is concerned, EU data subjects lack actionable judicial redress and, therefore, do not have any right to an effective remedy in the U.S.

Before moving on to the second perspective, one question still remains as regards the diabolical perseverance of the European Commission. Would it not have been possible for the European Parliament to do more in advance, before the first and second adequacy decisions had been formally adopted?

The answer is, quite simply, "no". This is because, despite the persuasive efforts of Emilio De Capitani (executive director of the Fundamental Rights European Experts Group), the change of the relevant legal basis (from Directive 95/46 to the General Data Protection Regulation (GDPR)) did not alter the nature of the adequacy decisions taken by the Commission.

These are still executive discretional acts and not legislative acts, for which the Com-

[6] G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, forthcoming, 2020, in *ssrn.com*.

mission's power to adopt an adequacy decision would be subject to stricter limits than today. It is sufficient to say that the Parliament and Council may revoke the delegation or express objections to any delegated act. This may be an opportunity lost, but there is still a window in the next European Commission's GDPR Review. So it would be best to avoid at least this kind of diabolical perseverance.

3. Judicial Manipulation of the CJEU reloaded and the training as a European Constitutional Court

The judicial manipulation by the CJEU in *Schrems I* is still fresh in our minds: «even though an adequate level of protection does not require third countries to adopt an identical standard, individuals may nevertheless enjoy a degree of protection that is "substantially equivalent" to that offered by EU law» (§ 73). The equivalence of the degree of protection is required, according to the Court, «by virtue of an interpretation of the Data Protection Directive in light of the Charter».

The Charter thus becomes the legal device for the Court to raise the level of protection required under EU law by manipulating the parameter of "adequacy", which is transformed in the different requirement of "essential equivalence". The difference between these two criteria must not be neglected. The former does not imply a direct comparison between the EU and US level of protection, whilst the latter is based on such a comparison.

The GDPR did not codify the mentioned judicial manipulation in an explicit way. It may be the case that the same GDPR, at recital 104, states that «The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors». However, Art. 45 still clarifies that such cases only involve an evaluation as to the adequacy of the level of protection, and not a comparison.

The CJEU did not want to lose the opportunity to propose the recalled judicial manipulation once again based on the shift from adequacy to essential equivalence.

The shift (and manipulation) was easier in this case than the first time (*Schrems I*) because of recital 104 (mentioned above). It should therefore come as no surprise when the Court asserts that:

«The first sentence of Article 45(1) of the GDPR provides that a transfer of personal data to a third country may be authorised by a Commission decision to the effect that that third country, a territory or one or more specified sectors within that third country, ensures an adequate level of protection. In that regard, although not requiring a third country to ensure a level of protection identical to that guaranteed in the EU legal order, the term "adequate level of protection" must, as confirmed by recital 104 of that regulation, be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the regulation, read in the light of the Charter».

As we know from *Google Spain* and especially from *Digital Rights Ireland*, the Charter, as the European Bill of Rights, has thus far been the constitutional trump card played by the CJEU when engaging in judicial activism in order to enforce digital privacy rights. In doing so, it furthers its ambition of becoming (and reduces its frustration at not formally being) a proper constitutional Court. Let us consider the *Schrems* case with reference to the related narrative of the equivalence of protection for fundamental rights in Europe. It may come as a surprise that this narrative is appealing for the CJEU, much more than the adequacy narrative. Only the former links up the judicial frame in *Schrems (I and II)* with the broader narrative of constitutional adjudication in European constitutional law, from *Solange* through to the *Kadi*, not forgetting *Bosphorus*. Here too there is nothing new under the sun; it amounts as it were to another trial run for the CJEU in order to be fully ready to play a proper role as a pan-European Constitutional Court.

4. Final remarks

In conclusion, what needs to be properly investigated are the judgment's implications for the new roles (and new responsibilities) of data controllers and, more generally, for digital platforms in the new legal scenario related to data transfer to third countries. However, one message coming from Luxembourg seems clear enough also from a first reading: the data exporter will face a quite complex and delicate evaluation, which implies further responsibility especially for platforms with the difficult dual status of hosting provider and data controller.

Spiderman might tell us that with great power comes great responsibility; and yet as every constitutional scholar knows full well, constitutionalism concerns the limits of power, and in this case the challenge is how to face new private digital powers as the geometry of power is shifting from a vertical to a horizontal dimension. It is becoming clearer that the path will lead towards further increasing the responsibilities of intermediaries.

Elenco autori

Raffaele Bifulco
professore ordinario di diritto costituzionale, LUISS Guido Carli
Francesca Bignami
Leroy Sorenson Merrifield Research Professor of Law, George Washington University - Law School
Sofia Braschi
assegnista di ricerca, Università di Pavia
Giacomo Capuzzo
assegnista di ricerca, Università di Perugia
Marina Castellaneta
professore ordinario di diritto internazionale, Università di Bari "A. Moro"
Massimo Foglia
ricercatore di diritto privato, Università di Bergamo
Bianca Gardella Tedeschi
professore associato di diritto privato, Università del Piemonte Orientale
Sara Gobbato
avvocato in Milano
Daniele Imbruglia
ricercatore di diritto privato, La Sapienza – Università di Roma
Elena Kaiser
dottoressa di ricerca in diritto pubblico, Università di Milano
Enrico Labella
ricercatore di diritto privato, Università di Palermo
Silvia Martinelli
assegnista di ricerca, Università di Milano
Carlo Melzi d'Eril
avvocato in Milano
Sofia Monici
dottore di ricerca in diritto dell'Unione europea, Università di Milano
Erion Murati
PhD Fellow (MaaS Project), University of Hamburg - Faculty of Law
Oreste Pollicino
professore ordinario di diritto costituzionale, Università Bocconi
Giulia Priora
assegnista di ricerca, Scuola Superiore Sant'Anna - Istituto DIRPOLIS (Diritto, Politica e Sviluppo)
Serena Quattrocolo
professore ordinario di diritto processuale penale, Università del Piemonte Orientale
Agostino Sola
avvocato praticante, Avvocatura Generale dello Stato
Shaira Thobani
assegnista di ricerca, Università di Torino
Andrea Venanzoni
Ph.D. Research Assistant in istituzioni di diritto pubblico e in diritto costituzionale

Elenco autori

Lavinia Vizzoni
cultore della materia in diritto privato, Università Ca' Foscari, Venezia - Dipartimento di Economia
Giulio Enea Vigevani
professore ordinario di diritto costituzionale, Università di Milano - Bicocca

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

media LAWS

ANNO 2020 - CODICE ISSN 2532-9146