La *Privacy* e il controllo dell'identità algoritmica

Raffaella Messinetti

Sommario: 1. "Reinventare" la *privacy*. – 2. *Data Protection* e *Data Analytics*. – 3. Le inferenze valutative e predittive. – 4. *Data Protection* e *Algo-Created Data*. – 5. L'identità della persona digitale. – 6. Il diritto a inferenze ragionevoli. – 7. Il *design* giuridico dell'infosfera.

Abstract

This Article aims to answer to the following question: Is the Data Protection Law able to protect data subject from the novel risks of inferential analytics in automated decision-making? As a matter of fact, AI, by means of Big Data analytics, draw non-intuitive inferences and predictions about individuals, which pose the greatest risks in terms of privacy and discrimination. Despite that, GDPR does not address the issue expressly. This Article argues that, in light of a systematic and axiologic interpretation, GDPR grants individuals meaningful control over the algorithmic process that reshapes their identity as digital persons. In particular, a right to reasonable inferences must be derived from the right to privacy, as a tool aimed to protect identity, according to Stefano Rodotà' s masterly reconstruction theory.

1. "Reinventare" la *privacy*

Nell'introduzione alla seconda edizione del volume *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Stefano Rodotà ci consegna, tra i suoi molteplici, insuperati insegnamenti, un'indicazione decisiva per orientarci nel tempo della rivoluzione digitale: «le trasformazioni determinate dalla tecnolo-

gia possono essere comprese, e governate, solo se si è capaci di mettere a punto strumenti prospettici e se questo avviene ridefinendo i principi fondamentali delle libertà individuali e collettive»[1].

La posta in gioco è alta; secondo il Maestro, «Se non si segue questa strada, la promessa tecnologica rischia di trasformarsi nel più pesante dei vincoli, dando evidenza sociale alla tesi che vuole ormai la tecnica portatrice di una potenza irresistibile, destinata ad imporre ovunque la propria logica»[2].

Alla stregua di questa indicazione, la letteratura scientifica internazionale riflette oggi la centralità di un problema trans-disciplinare: adeguare la tutela giuridica della persona umana alla g*rande trasformazione*[3] implicata dalla digitalizzazione del mondo e dall'evoluzione dell'Intelligenza artificiale.

Un sintagma – quest'ultimo – comunicativamente potente: da un lato, reinterroga il ruolo del pensiero razionale come categoria distintiva dell'umano; dall'altro, ripropone il tema dell'autonomia individuale, nel quadro di una inedita relazione tra uomo e macchina. I due aspetti rinviano intuitivamente alla stessa immagine, sfidandola: quella di persona umana, al centro della costruzione giuridica moderna. Da questa prospettiva, il problema della tutela della persona nel tempo della rivoluzione dell'informazione viene riformulato così: «salvare l'umanità dalla schiavitù dell'intelligenza artificiale»[4].

---

[1] Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Roma-Bari, 2004, p. XLI s.

[2] Rodotà, *Tecnopolitica,* cit., XLII.

[3] È il titolo della notissima opera di Polanyi, *La grande trasformazione. Le origini economiche e politiche della nostra epoca*, Torino 1974. L'analisi dei processi sociali ed economici effettuata dall'illustre Autore è riferimento fondamentale per comprendere l'esperienza giuridica occidentale moderna e contemporanea.

[4] Pasquale, T*he Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard University Press, 2015; Hildebrandt, *The Dawn of a Critical Transparency Right for the Profiling Era*, in *Digital Enlightment Yearbook 2012*, a cura di Hildebrandt et al., Amsterdam, 2012.

La sintesi – volutamente enfatica e provocatoria – riflette la difficoltà di governare le conseguenze aporetiche della modernità: liberare l'individuo dalla forza e dai vincoli della tradizione ma consegnarlo a quelli dell'apparato tecnologico. Secondo una tesi largamente condivisa, infatti, il dominio della tecnica sarebbe la forma in cui la contemporaneità presenta il proprio carattere originale[5]. A stabilirne l'attuale connotazione sarebbero le ICT. Se «ogni età è stata un'età dell'informazione» e se «i sistemi di comunicazione hanno sempre foggiato gli eventi»[6], le caratteristiche della società dell'informazione come società contemporanea sarebbero inedite alla stregua del ruolo peculiare delle ICT[7]: ricreare e reinterpretare la realtà in modo autoreferenziale, con un esito rivoluzionario: «ciò che è informazionale è reale e ciò che è reale è informazionale»[8]. Una radicale trasformazione del modo in cui gli esseri umani vedono e pensano sé stessi e il mondo in cui vivono, a partire da una nuova dimensione della vita: il *world wide web*. Le ICT sarebbero non meri strumenti di comunicazione ma "agenti di

---

[5] Riferimenti scontati ma decisivi a Heidegger, *Saggi e discorsi*, Milano, 1991, p. 19 ss. Per l'analisi giuridica, in relazione ai profili svolti nel testo, Severino, *La tendenza fondamentale del nostro tempo*, Milano, 2008, Irti e Severino, *Dialogo su diritto e tecnica*, Roma-Bari, 2001.

[6] Darnton, *L'età dell'informazione. Una guida non convenzionale al Settecento*, Milano, 2007, p. 41 ss.

[7] Sulla "forza strutturante delle tecnologie", fondamentale Rodotà, *Tecnopolitica*, cit., p. 134 ss. Secondo l'illustre A., occorre «chiedersi, prima di tutto, quale sia il soggetto che le tecnologie della comunicazione e dell'informazione fanno emergere, come avvenga la sua costruzione».

[8] Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, p. 45.

Questa corrispondenza definirebbe un connotato fondamentale della contemporaneità, l'effetto di una nuova rivoluzione scientifica (la quarta) nella storia dell'umanità. In questa narrazione l'espressione rivoluzione risalta in una doppia comunicazione: segnalare, da un lato, che per la prima volta nella storia «il progresso e il benessere dell'umanità sono non soltanto collegati ma, soprattutto, dipendenti dall'efficace ed efficiente gestione del ciclo di vita dell'informazione»; dall'altro, la "radicale trasformazione" antropologica indicata nel testo.

ri-concettualizzazione della nostra ontologia"[9] in termini conformi al loro codice: quello informazionale. "Inforg" e "infosfera" sono le nuove parole coniate per adeguare la comunicazione alla nuova realtà e denotare la natura informazionale condivisa dall'essere umano e dal suo ambiente digitale; un ambiente che l'uomo abita insieme ad altri agenti informazionali, senza occuparne il centro[10].

La brillante rappresentazione di Luciano Floridi dà ragione di un quesito che Rodotà ha posto da tempo: siamo di fronte a una nuova antropologia[11]? O – addirittura – alla fine di ogni narrazione antropologica con il declino dell'Umano[12]?

È – questo – un nodo ineludibile anche per la riflessione del giurista, se è vero che la dimensione antropologica dà la matrice al cambiamento sociale. Scioglierlo, allora, appare indispensabile per comprendere il senso del cambiamento e, di conseguenza, governarne i problemi normativi.

Ad orientarci, in questo percorso, un'altra intuizione di Rodotà[13]: «si sta delineando un ordine sociale e giuridico delle macchine che rivendica la propria autonomia» e che – perciò – «può determinare conflitti con la tradizionale autonomia delle persone».

Con altre parole: le trasformazioni indotte dall'innovazione tecnologica, realizzando la «separazione tra il mondo delle persone e il mondo degli oggetti dotato di una propria crescente autonomia»[14], coinvolgono il principio fondativo della società moderna e costitutivo del suo ordine giuridico: l'autonomia dell'individuo. Una puntualizzazione – questa – decisiva: la relazionalità

---

[9] Floridi, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, 2009, p. 185 ss.

[10] Floridi, *Infosfera*, cit., in particolare p. 106 ss. Resta ineludibile il riferimento a Anders, *L'uomo è antiquato, II. Sulla distruzione della vita nell'epoca della terza rivoluzione industriale*, 1992, p. 3 secondo cui: «la tecnica è ormai diventata il soggetto della storia con la quale noi siamo soltanto costorici».

[11] Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 312 ss.; Id. *Antropologia dell'homo dignus*, in R*iv. crit. dir. priv.*, 2010, p. 547 ss.

[12] Rodotà, *Il diritto di avere diritti*, cit., p. 340

[13] Rodotà, *Il diritto di avere diritti*, cit., p. 315.

[14] Rodotà, *Il diritto di avere diritti*, cit., p. 323.

del termine manifesta la questione fondamentale che sottende: quella del potere e della condizione umana ad esso esposta. La rivoluzione dell'informazione la riconfigura secondo la sua forma: la vulnerabilità della persona di fronte al potere digitale[15].

Un potere inedito, la cui presa è tanto pervasiva quanto sfuggente. Per definirla, anche l'analisi giuridica si è avvalsa della forza comunicativa di metafore letterarie: la distopia di Orwell ha fornito una rappresentazione icastica degli effetti individuali e sociali della *dataveillance*[16]. Da questa prospettiva, la sorveglianza generalizzata definirebbe un connotato originale ma non conclusivo della società digitale.[17]

Secondo una convincente riflessione, infatti, la velocità dell'evoluzione tecnologica e delle correlate trasformazioni della prassi esasperano la "liquidità"[18] della società contemporanea: irriducibile ad un'unica rappresentazione formale, la nuova complessità digitale coinvolgerebbe una pluralità multiforme di immagini, riflesse dalle diverse prospettive da cui essa viene osservata. Quella – ora egemonica – dei c.d. *big data* e dell'intelligenza artificiale paleserebbe l'inadeguatezza della metafora della sorveglianza per evocare quella del processo di Kafka[19]: la vulnerabilità dell'individuo esposto, nell'infosfera, a infiniti e indefiniti trattamenti dei dati personali «che lo riguardano»; a processi ininterrotti di ricostruzio-

---

[15] Rodotà, *Il diritto di avere diritti*, cit., p. 335

[16] Clarke, *Information Technology and Dataveillance*, in *Communication of the ACM*, 1988, p. 498 ss.

[17] Rodotà, *Tecnopolitica*, cit., p.164 ss. Ampio panorama del tema in Lyon, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, Milano, 1997; ID., *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002.

[18] Scontato il riferimento al pensiero di Zygmunt Bauman e, in particolare, alle riflessioni contenute nei volumi seguenti: Bauman, *La società individualizzata. Come cambia la nostra esperienza*, Roma-Bari, 2002; Id., *Modernità liquida*, Roma-Bari, 2003; Id., *Vita liquida*, Roma-Bari, 2006.

[19] Solove, *The Digital Person. Technology and Privacy in the Information Age*, New York-London, New York, 2004, p. 30 ss.; sulla relazione uomo-macchina nella prospettiva dell'analisi giuridica, fondamentale la riflessione di Rodotà, ora riportata in *Il diritto di avere diritti*, cit., in particolare p. 312 ss.

ne e utilizzazione della sua identità sui quali egli – come, forse, nessuno – non esercita alcun controllo.

Questa, allora, è la doppia forza della metafora: restituire sia il senso del problema fondamentale posto dalla rivoluzione dell'informazione: "salvare l'umanità dalla schiavitù dell'AI"[20], sia il principio della sua soluzione: il potere della persona di controllare i processi aventi ad oggetto la sua identità. Per riassumere: controllare l'identità personale è il nodo della questione del potere e della libertà nella società digitale. Ed è – notoriamente – la questione al centro della riflessione e del contributo fondamentale di Rodotà alla tutela della persona e della sua dignità nel «tempo dell'identità inconoscibile"[21]: la "reinvenzione della *privacy*»[22].

Reinventare la *privacy* è la «via che deve essere percorsa per mantenere condizioni di libertà della persona e garantire condizioni di esercizio democratico del potere. Le trasformazioni tecnologiche dell'organizzazione sociale, infatti, non producono soltanto asimmetrie nella distribuzione e nell'esercizio del potere ma determinano una frattura sociale tra individui sempre più trasparenti e poteri sempre più opachi e incontrollabili»[23].

Qui si radica il conflitto tra l'autonomia dell'individuo e quella dell'apparato tecnologico (delle macchine): nello spazio di quella frattura, si realizza lo slittamento dell'autonomia dal mondo delle persone a quello delle macchine.

Per «ridefinire i principi fondamentali delle libertà individuali e collettive», occorre allora esplorare questo processo, partendo da un profilo solo in apparenza scontato: trasparenza delle persone e opacità delle macchine sono gli effetti – opposti – della stessa matrice: il codice tecnologico dell'infosfera; una funzione del suo connotato organizzativo essenziale: l'autoreferenzialità[24].

---

[20] *Retro*, nt. 4

[21] Rodotà, *Il diritto di avere diritti*, cit., in particolare p. 318 ss.

[22] Rodotà, *Il diritto di avere diritti*, cit., p. 319 ss.

[23] Rodotà, *Il diritto di avere diritti*, cit., p. 337 ss.

[24] Come vedremo, è questa la chiave per accedere a due cardini dell'architettura dell'infosfera: l'ordine della comunicazione tra uomo e macchina come agenti informazionali dell'ambiente digitale e quello della relazione tra diritto e tecnologia.

Questa qualità del codice ha una ragione evidente: digitalizzare il mondo implica ridefinirlo dal punto di vista della macchina; tutto il reale deve essere riducibile a dati operazionali; ad input processabili dalla macchina. Nel «mondo che si fa macchina»[25], questo è un condizionamento sistemico, in certo senso, universale. Anche l'essere umano vi soggiace, in virtù della scomposizione (e ricomposizione) della sua identità in dati informativi: i dati personali che lo riguardano. Questa "ristrutturazione" della personalità condiziona soggettività e cittadinanza nella società digitale: infatti, è solo come "organismo informazionale" che l'uomo ha accesso all'infosfera.

Il legame tra l'individuo e i dati che lo riguardano è perciò costitutivo e, sotto il profilo che stiamo osservando, non potrebbe apparire più stretto: l'identità personale tende a coincidere con la sintesi dei dati informativi che "parlano" della persona nella multiforme pluralità dei luoghi dell'interazione sociale[26]. È ormai esperienza comune che a determinare la rappresentazione sociale della persona è il «corpo profondamente modificato dall'immersione nel flusso delle comunicazioni elettroniche»; che – con altre parole – sono le ICT a costituirci «persone digitali»[27].

D'altro canto, il legame tra la persona, i suoi dati e la sua identità è indebolito proprio dai nuovi processi tecnologici di costruzione dell'identità personale: processi "separati" dall'individuo nella misura in cui vengono consegnati alla potenza computazionale dell'apparato tecnologico e quindi alla cifra autoreferenziale del suo codice informatico-statistico. Nel mondo che «si fa macchina»[28], «il punto chiave, infatti, è rappresentato dall'emergere di una nuova razionalità, che coincide con una progressiva ritirata dell'intervento umano, sostituito dall'affidare una quantità crescente di dati personali all'autonoma capacità di elaborazione di computer che, sulla base di programmi statistici e attuariali, di modelli probabilistici, rendono possibili non semplice predizioni

---

[25] Rodotà, *Il diritto di avere diritti*, cit., p. 323.
[26] Rodotà, *Tecnopolitica*, cit., p. 139 ss.
[27] Solove, *The Digital Person*, cit.
[28] Rodotà *Il diritto di avere diritti*, cit., p. 323

sui comportamenti futuri delle persone, ma vere e proprie costruzioni di identità. E queste possono diventare la rappresentazione che, poi, viene considerata vincolante ai fini delle decisioni che riguardano la persona da parte dei soggetti che producono questa rappresentazione o a essa possono avere accesso»[29].

Quello tra la persona e i suoi dati è, dunque, un legame ambivalente: la rivoluzione che le ICT avrebbero realizzato riconfigurando la natura informazionale dell'identità dell'uomo e ridimensionandone, di conseguenza, la posizione nell'universo digitale sembra infatti definire, nell'attualità, l'approdo del processo, radicato nella modernità, cui Rodotà allude[30]: l'istituzione della tecnica quale soggetto forte dell'ordine sociale contemporaneo e la riduzione dell'uomo a "materia prima del processo tecnologico"[31]. Questa immagine restituisce l'altro senso del condizionamento sistemico cui l'essere umano soggiace nella società digitale: la «oggettivazione informazionale-informatica» dell'identità funzionale alla inclusione dell'uomo nell'apparato tecnologico che "avvolge" il mondo.

Sotto questo profilo, la natura informazionale dell'identità personale dà immediata ragione della nuova vulnerabilità della persona digitale[32]. Infatti, se nella prassi della società della comunicazione noi "siamo" le nostre informazioni, due conseguenze sono palesi: la prima: di fronte al potere digitale siamo trasparenti; la seconda: «tutto ciò che è fatto alle nostre informazioni è fatto a noi e non a ciò che possediamo»[33].

Dalla prospettiva dei principi fondamentali la lettura di questo doppio effetto è univoca: controllare i processi che hanno ad oggetto i "propri" dati personali e, perciò, la propria identità è il nucleo essenziale della tutela giuridica della persona umana nella

---

[29] Rodotà *Il diritto di avere diritti*, cit., p. 324 s.

[30] *Retro*, nt. 2.

[31] Anders, *L'uomo è antiquato*, cit., p. 3.

[32] Sulla «nuova vulnerabilità sociale», Rodotà, *Il diritto di avere diritti*, cit., p. 35; Hildebrandt, *Slaves to Big Data. Or are we?,* in *Revista de Internet, Derecho y Politica*, 2013, p. 7 ss.

[33] Floridi, *Infosfera*, cit., p. 148; Id., *La quarta rivoluzione*, cit., p. 135.

società dell'informazione contemporanea; strumento per preservarne la libertà nel tempo della sorveglianza globale e della digitalizzazione del mondo[34].

2. *Data Protection* e *Data Analytics*

Come Rodotà ha conclusivamente dimostrato, il diritto alla protezione dei dati personali innova la categoria semantica della privacy per «trasferire nella dimensione tecnologica la garanzia di fondamentali libertà» della persona umana.[35] Il *medium* di questa finalizzazione è reso evidente dal ruolo comunicativo dell'espressione "diritto alla protezione dei dati personali" nel discorso giuridico: «formula riassuntiva di nuovi diritti e della nuova dimensione di vecchi diritti»[36]; questi ultimi riletti alla luce dell'innovazione tecnologica e tutti sinergicamente correlati per garantire un potere "dinamico" della persona: controllare i processi di costruzione e utilizzazione della propria identità personale, quale dispositivo essenziale di socializzazione nell'infosfera. Un dritto fondamentale della persona umana perché è «strumento indispensabile per

[34] Il nesso tra controllo sulla macchina e principio democratico non potrebbe essere più evidente: Rodotà ha dimostrato che nella società dell'informazione il problema dell'identità personale – quale identità informazionale – è connesso *naturaliter* a quello dell'organizzazione del potere in virtù di un fatto: il vincolo inscindibile e qualificante tra esercizio del potere e uso delle informazioni. Infatti, se l'esercizio del potere implica l'uso strategico delle informazioni personali, la conseguenza in un sistema democratico è necessaria: garantire all'individuo il controllo sull'uso dei propri dati personali da parte dei poteri. È chiaro – cioè – che controllare la costruzione e la circolazione della propria identità è aspetto essenziale anche del problema del controllo democratico sul potere. Se ne ricavano due conseguenze decisive nel nostro discorso: la prima: l'apparato tecnologico, quale apparato di potere, deve essere reso trasparente; la seconda: i suoi processi devono risultare intelligibili nella misura in cui operano sull'identità della persona umana e perciò ne incidono la sfera vitale.

[35] Rodotà, *Tecnopolitica*, cit., p. XXX.

[36] Rodotà, *Tecnopolitica*, cit., p. XXIX.

il libero sviluppo della personalità e per definire l'insieme delle relazioni sociali,[37] rafforzando «la costituzionalizzazione della persona grazie a un insieme di poteri che davvero caratterizzano la cittadinanza del nuovo millennio»[38].

Questo inquadramento dà ragione di un quesito ricorrente nella – già amplissima – letteratura scientifica sul GDPR: se la disciplina europea di nuovo conio soddisfi o non la suddetta istanza di controllo rispetto ai processi di definizione dell'identità personale governati dall'intelligenza artificiale. Con altre parole: se il sistema giuridico della c.d. *Data-Protection* (che protegge i dati per proteggere la persona)[39] sia adeguato ai processi tecnologici che restituiscono la persona umana alla società dell›informazione come persona digitale.

Tra gli studiosi del tema più attenti all'esigenza del dialogo interdisciplinare, critiche e perplessità non sono affatto isolate. È diffuso il convincimento di una disfunzionalità della relazione tra GDPR e AI che pregiudicherebbe obiettivi primari del Regolamento Europeo[40]: favorire lo sviluppo della società digitale assicurando e contemperando due esigenze fondamentali – e, apparentemente, antitetiche – della contemporaneità: la libera circolazione delle informazioni e la protezione dei dati personali[41].

A riprova di questa disfunzionalità viene addotta la contrapposizione tra le *rationes* che orientano, da un lato, i principi fon-

---

[37] Rodotà, *Il diritto di avere diritti*, cit., p. 321.

[38] Rodotà, *Il diritto di avere diritti*, cit., p. 321.

[39] Che il sintagma – incentrato sui dati - possa essere fuorviante nella comunicazione del suo significato e della sua finalità è ben osservato da Watcher e Mittelstadt, *A Right to Reasonable Inferences*, in *Columbia Business Law Review*, 2019, p. 82.

[40] Zarsky, *Incompatible: The GDPR in the Age of Big-data*, in *Seton Hall Law Review*, 2017, p. 995;

[41] Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, in *Persona e mercato dei dati*, *Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019, p. 35 ss; Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà fondamentali tra mercato e persona: nuovi assetti nell'ordinamento europeo*?, in *Contratto e Impresa*, 2018, p. 190 ss.; Danaher, T*he Threat of Algocracy: Reality, Resistance and Accommodation*, in *Philosophy and Technology*, 2016.

damentali del GDPR e, dall'altro, quelli operazionali dell'AI. Per esemplificare: se, per un verso, il successo "computazionale" del processo automatizzato e l'affidabilità dei suoi output presuppongono la massimizzazione dei dati informativi, per l'altro, il Regolamento impone la minimizzazione di quelli personali (art. 5, lett. "c") E ancora: se, da un lato, il Regolamento impone il principio di limitazione della finalità (art.5, lett. "b"), dall'altro, l'AI non "tollera" finalizzazioni né limitazioni: le promesse dell'AI sono affidate proprio all'imprevedibilità delle connessioni e degli output che restituisce, inverando possibilità di utilizzazione dei dati inedite e, correlativamente, prefigurando vantaggi inimmaginati dall'intelligenza umana[42].

La prospettiva che guarda all'intelligenza artificiale come al banco di prova dell'adeguatezza digitale del GDPR restituisce una criticità più radicale: la dinamica (operazionale) dell'intelligenza artificiale, fondata sulla c.d. *data-driven analytics*, minerebbe categorie fondamentali del GDPR: quella di dato personale[43] e, in quest'ambito, la stessa distinzione tra dati ordinari e dati sensibili[44]. La ragione – un'informazione elementare per gli studiosi di *Computer Sciences* – è iscritta in un connotato basilare dell'AI: la sua capacità – in virtù dei *big-data* – di generare nuove informazioni personali a partire da dati che non sono personali, nonché

---

[42] D'Acquisto e Naldi, *Big-data e Privacy by Design. Anonimizzazione, Pseudonimizzazione. Sicurezza*, Torino, 2017.

[43] Quella di dato personale sarebbe nozione "fluida", mutevole con l'evoluzione delle tecnologie, secondo Korff, *Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments* (European Commission Directorate-General Justice, Freedom and Security, Working Paper n.2/2010). Stabilire cosa sia dato personale o non è ritenuta questione "oscura" anche nell'articolata analisi di Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 87 ss.

[44] Watcher, *Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination and the GDPR*, in *Computer L. & Security Rev.*, 2018, p. 436 ss.; Id., *Data Protection in the Age of Big-data*, in *Nature Electronics*, 2019.

quella di derivare dati sensibili da dati che non lo sono[45] e persino da dati che sono anonimi[46].

Le conseguenze sulla efficacia della strategia complessivamente elaborata dal GDPR sono intuitive: il concetto giuridico di dato personale è il codice del riconoscimento da parte del Regolamento e perciò la chiave per accedere al suo sistema di protezione della «persona digitale»[47]. È la qualificazione di un'informazione come dato personale (art. 4) a respingere dal varco della disciplina giuridica i dati anonimi e quindi – in larga parte – i *big-data*.

D'altro canto, *big-data* e AI formano un binomio inscindibile. È chiaro, infatti, che quando sia utilizzata per profilare e prendere decisioni sulle persone, l'AI si avvale sia di dati personali sia di *big-data* (la "materia prima" indispensabile al suo funzionamento) per generare nuovi dati informativi sulle persone soggette al processo decisionale. Sono – questi – gli *output* "costruiti" dalla *big-data analytics*[48] (c.d. *algo-created data*).

In queste ipotesi, il "trattamento" algoritmico delle informazioni restituisce proiezioni dell'identità personale all'esito di un'interazione tra dati personali e *big-data* che è realizzata dall'AI alla stregua – principalmente – dei modelli e delle logiche dell'analisi inferenziale.

---

[45] «La profilazione può creare dati appartenenti a categorie particolari desumendoli (*by inference*) da dati che di per sé non appartengono a categorie particolari ma che diventano tali se combinati con altri dati. Ad esempio, può essere possibile desumere lo stato di salute di una persona associando le registrazioni dei suoi acquisti di alimenti a dati sulla qualità e sul contenuto energetico di tali alimenti»: Art. 29 Working Party, *Guidelines on Automated Decision Making and Profiling for the Purposes of Regulation 2016/679*, p.15; Id., *Advice Paper on Special Categories of Data (Sensitive Data)*.

[46] Barocas e Selbst, *Big-data's Disparate Impact*, in *California Law Review*, 2016, p. 671 ss.

[47] Per una critica originale, v. Purtova, T*he Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law Innovation & Tech*, 2018, p. 48 ss.

[48] Su questo aspetto dei «*derived or inferred data*», chiarissime le osservazioni dell'Art. 29 Working Party, *Guidelines on Automated Decision Making and Profiling for the Purposes of Regulation 2016/679.*

È evidente che il contributo dei *big-data* a questi processi (di trattamento dei dati personali) è fondamentale nella misura in cui la ricostruzione dell'identità personale, posta alla base della decisione, si fondi sui c.d. dati inferiti e/o derivati: quelli – con altre parole – "costruiti" e restituiti dalla *big-data analytics*[49].

L'importanza di questi dati nella (ri)costruzione "informatica" dell'identità personale e, per converso, la loro (pretesa) irrilevanza nel sistema del GDPR è il nodo dell'accusa che viene mossa al Regolamento europeo: avere costruito regole non aggiornate alla realtà digitale e perciò inadeguate sia alla "natura" informazionale della persona digitale[50], sia a quella computazionale e – in larga parte – eterodeterminata della sua identità sociale[51].

Da questa prospettiva, la funzione normativa del Regolamento sarebbe "sterilizzata" dalla metrica del suo discorso, riflettendo un vizio – non banale – dell'impostazione strutturale: la mancata attenzione per la fase del trattamento consistente nell'elaborazione e interpretazione dei dati[52]. Detto altrimenti: la mancata regolamentazione della fase dell'analisi dei dati e perciò della "produzio-

---

[49] Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 22 ss.; L. Edwards e Veale**,** *Slave to the Algorithm? Why a Right to an Explanation is Probably Not the Remedy You are Looking for*, in *Duke Law & Technology Review*, 2017 p. 37 s.: «*But if ordinary data about purchase are collected and algorithmically transformed into insights that are sensitive, such as those related to health, or "protected", such are those relating to pregnancy, what is the correct standard of safeguard? For additional complication, the GDPR lays down a basic rule that profiling "shall not be based" on the special categories of personal data, unless there is explicit consent. Does this apply to ML systems where the inputs are non-sensitive but the output inferences may be, as was the case in the Target profiling? Should explicit consent be given where personal data is gathered from public social media posts using "legitimate grounds" and transformed into data about political preferences which is "sensitive" data in the GDPR (article 9(1))? What about when ordinary data collected via a wearable like a Fitbit is transformed into health data used to reassess insurance premiums?*».

[50] Floridi, *Infosfera*, cit., in particolare p. 133 ss.

[51] Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 9 ss.

[52] Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 1 ss.

ne" dei significati che definiscono il contenuto dell'identità della persona profilata e soggetta al processo decisionale automatizzato.

Alla luce dell'insegnamento di Rodotà, questa disattenzione sarebbe davvero sorprendente: non soltanto perché «la costruzione della nostra identità individuale e sociale è affidata ad algoritmi»[53] ma anche perché «siamo di fronte a una raccolta di informazioni che, a parte la sua ampiezza e pervasività, non è statica, ma in sé dinamica, nel senso che è continuamente produttiva di effetti senza bisogno di mediazioni. Sono i sistemi automatici a elaborare i dati secondo la propria logica. E l'utilizzabilità dei risultati di questa forma del trattamento dei dati da parte di una molteplicità di soggetti non fa soltanto crescere la possibilità di una soddisfazione diretta di bisogni ma la trasparenza complessiva della persona. E questo significa che, allo stesso tempo, viene disegnato non solo lo spazio "interno" della persona, ma pure quello "esterno"»[54].

È chiaro, quindi, che alla pretesa irrilevanza del tema secondo il GDPR non corrisponde la sua irrilevanza giuridica[55]. Al contrario, la centralità "strategica" di questa fase del trattamento e dei problemi che essa pone al diritto si manifesta con peculiare evidenza nel contesto fenomenico dei processi decisionali automatizzati; una pratica fondamentale della società digitale, che il Regolamento disciplina nell'art. 22, alla stregua delle *rationes* delineate nel *considerando* n. 71.

Una rapida lettura di queste disposizioni palesa che il "fatto" del trattamento dei c.d. dati derivati e/o inferiti intercetta principi giuridici che sono fondamentali nel sistema del GDPR; per fare un esempio: il principio di trasparenza[56]. Il trattamento dei dati costruiti, "normale" nei processi dell'art. 22, pone il problema della "trasparenza" della decisione algoritmica, prospettando, in particolare, che per conoscere le ragioni della decisione (*considerando*

---

[53] Rodotà, *Il diritto di avere diritti*, cit., p. 402.

[54] Rodotà, *Il diritto di avere diritti*, cit., p. 336

[55] Mittelstadt, Allo, Taddeo, Watcher e Floridi, *The Etichs of Algortithms*: *Mapping the Debate*, *Big-data & Society*, 2016, p.1 ss.

[56] Art. 29 Working Party, *Guidelines on Automated Decision Making and Profiling for the Purposes of Regulation 2016/679.*

n. 71) e poterla contestare (art.22, par. 3) occorre riconoscere e comprendere le inferenze che la giustificano[57].

Come vedremo, l'interpretazione dell'art. 22 nel sistema del GDPR è cruciale per rispondere a una domanda: il diritto (oggettivo) tutela la persona umana nei processi di costruzione dell'identità personale governati dall'AI? La persona umana dispone – o non – di un potere giuridico di controllare la definizione algoritmica della sua immagine sociale?

Queste pagine sono dedicate ad argomentare la risposta affermativa, in virtù dei processi dell'interpretazione sistematica ed assiologica. In particolare, si propongono di palesare che la risposta è chiara nell'opera di Stefano Rodotà: la costruzione teoretica del c.d. diritto alla *privacy* e dei suoi nessi con l'identità personale nel tempo della datificazione della persona umana e della digitalizzazione del mondo.

3. Le inferenze valutative e predittive

Ad una lettura restrittiva del Regolamento, l'analisi dei dati potrebbe risultare irrilevante per una ragione formale: i dati derivati e/o inferiti (costruiti in virtù dell'analisi) non sarebbero «personali» – ai sensi e per le finalità del Regolamento medesimo[58]. Non potendo essere qualificati «dati personali», essi sarebbero al di fuori dell'ambito di applicazione della *Data-Protection*: la tutela della persona umana in virtù della tutela dei dati che la riguardano[59]. Il

---

[57] Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 1 ss.

[58] Questa lettura è attentamente analizzata da Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 22 ss., ed è ripercorsa alla stregua della giurisprudenza europea in tema di *Data Protection*.

[59] Nella grammatica del GDPR – e secondo le linee guida elaborate dall'*Article* 29 *Data Protection Working Party* – i c.d. dati inferiti (o derivati) hanno una propria, peculiare identità nel *genus* "dati personali", non essendo riconducibili né a quelli «raccolti presso l'interessato» (art.13; C. 60-62), né a quelli «osservati sull'interessato», né a quelli comunicati da altri e diversi titolari del trattamento (art.14): – come abbiamo visto – sono dati "naturalmente" ignoti all'inizio del trattamento, generati dalla macchina nello svolgersi "autonomo" del processo computazionale.

discorso si concentra sulle inferenze valutative e predittive, le quali costituiscono, empiricamente, gli elementi cruciali del "*reasoning artificiale*" (delle macchine) e perciò dei processi decisionali di cui all'art. 22. Punto di partenza è l'osservazione che, differentemente dai dati «raccolti» ai sensi del GDPR, questi dati costituiscono output analitici (costruiti da processi analitici inferenziali orientati da modelli matematico-statistici) e consistono – essenzialmente – non di fatti ma di "valutazioni" e "previsioni" di aspetti della personalità e comportamenti individuali. Per questa ragione "intrinseca" essi non sarebbero verificabili, difettando perciò di una qualità logico-giuridica che sarebbe normativamente prevista come essenziale alla *Data Protection*: l'esattezza (art. 5, par. 2, lett. "e" GDPR).

A ben vedere, il nodo del problema sarebbe l'incompatibilità tra due aspetti: da un lato, la peculiare natura comunicativa dei dati derivati: non informare su fatti ma esprimere valutazioni soggettive e previsioni; dall'altro, un requisito che viene ritenuto costitutivo dello schema di qualificazione fornito dal GDPR: la verificabilità del dato alla stregua del codice vero – falso. L'argomentazione postula, infatti, che esattezza – nel senso dell'art. 5 – equivalga a veridicità[60].

In questa ricostruzione, la necessità giuridica che il dato personale sia fattuale (*rectius*: la fattualità dell'informazione che esso fornisce) viene desunta dalla prescrizione dell'esattezza (art. 5, par. 2, lett "e" GDPR) in virtù di una interpretazione articolata in un doppio passaggio. Il primo è strategico, riguardando il ruolo dell'art. 5, par. 2, lett. "e" nel sistema di protezione dei dati personali costruito dal GDPR: prescrivere la necessità che il dato personale sia esatto definisce un aspetto essenziale del "controllo" sulla circolazione dei propri dati: la verificazione. Detto altrimenti: il potere di controllare la propria identità (nucleo del diritto alla protezione dei dati personali) includerebbe essenzialmente la verificazione dei dati personali oggetto di trattamento[61].

---

[60] Sull'accuratezza delle inferenze predittive come verosimiglianza secondo il calcolo probabilistico, D'Acquisto e Naldi, *Big-data e Privacy by Design*, cit., p.140 ss.

[61] Di contrario avviso, Art. 29 Working Party, *Opinion 4/2007 on the*

Il secondo è interpretativo: l'attribuzione di significato all'espressione "esatto" in quanto riferita sia all'entità "dato personale", sia al modello della sua verificabilità.

Per semplificare, l'argomentazione può essere sintetizzata così:

– i dati personali devono essere esatti;
– esatto significa vero, cioè rispondente alla realtà fattuale;
– solo i fatti possono essere veri;
– i dati personali (dovendo essere veri) devono essere/rappresentare fatti.

Questa argomentazione, applicata alle inferenze valutative e predittive, produce esiti scontati: queste non possono essere considerate dati personali perché, non rappresentando fatti, non sono verificabili[62]. Infatti, le valutazioni come tali non sono né vere né false; le previsioni riguardano fatti futuri, i quali – per definizione – non possono essere verificati se e finché non accadano.

La conclusione è chiara: in quanto – appunto – non personali, i dati derivati non sarebbero oggetto della protezione giuridica fornita dal GDPR.

L'argomentazione non è conclusiva e le sue conseguenze risultano disfunzionali rispetto a finalità primarie del GDPR: favorire

---

Concept of Personal Data, alla stregua del modello di qualificazione proposto e della rilevanza, in quest'ambito, del parametro del "risultato": «*A third kind of "relating" to specific persons arises when a "result" element is present. Despite the absence of a "content" or "purpose" element, data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case. It should be noted that it is not necessary that the potential result be a major impact. It is sufficient if the individual may be treated differently from other persons as a result of the processing of such data*».

[62] Come abbiamo visto nella nota procedente, nella interpretazione dell'Art. 29 *Working Party*, i dati non debbono corrispondere a fatti oggettivi ed essere di conseguenza verificabili per essere qualificati come "personali" ai sensi del diritto europeo. L'interpretazione è condivisa da Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 27 ss.

lo sviluppo della società digitale e proteggere i diritti e le libertà fondamentali della persona umana[63].

La prima richiede che l'AI fornisca output affidabili; che le inferenze restituite dalla *big-data analytics* siano accurate secondo standard oggettivi[64]. Analogamente la seconda. Sotto questo aspetto, l'esito è paradossale: respingere le inferenze dalla *Data-Protection* non comporta escluderle dalla ricostruzione della persona digitale ma, al contrario, che esse siano liberamente trattate e perciò non controllate. Con altre parole: non sarebbero "personali" secondo il diritto dati che, al contrario, sono "fattualmente" decisivi per la definizione dell'identità personale. La conclusione è che l'identità personale resterebbe incontrollata – in un suo formante essenziale[65]. La persona umana non avrebbe, infatti, alcun potere giuridico di controllare il processo di costruzione della sua immagine sociale in aspetti cruciali; gli stessi che, rappresentandone le ragioni, permettono di comprendere la decisione algoritmica che – secondo l'art. 22 – incide nella sua sfera giuridica o produce effetti analogamente significativi sul piano sociale.

Se questa interpretazione fosse corretta, la frattura tra la realtà e la sua formalizzazione giuridica sarebbe stridente, invertendo l'ordine della comunicazione tra il mondo della vita e il diritto[66]: il primo pone i problemi che il secondo è chiamato a risolvere. Nel nostro caso, il fatto della costruzione algoritmica dell'identità umana interpella il diritto con una questione che chiama subito in causa un principio fondamentale: la tutela della persona umana.

---

[63] Riferimenti scontati ai *considerando* n. 2 e n. 4 e all'art. 1 GDPR.

[64] Chiari riferimenti anche per l'analisi giuridica in D'Acquisto e Naldi, *Big-data e Privacy by Design*, cit., p. 117 ss.

[65] Floridi, *Four Challenges for a Theory of Informational Privacy*, in *Ethics & Info. Tech*., 2006, p.109; La necessità di «reinventare la privacy» «nel tempo dell'identità inconoscibile da parte dello stesso interessato» è riscontrata da Rodotà, *Il diritto di avere diritti*, cit., in particolare p. 318 ss.

[66] Sul principio di adeguatezza dell'effetto al fatto – come su ogni altro aspetto della dinamica giuridica – riferimento scontato ma sempre fondamentale è Falzea, *Efficacia giuridica*, in *Enc. dir.*, XIV, 1965, p. 432 ss., ora in *Voci di teoria generale del diritto*, Milano, 1985, p. 241 ss. e a M. Barcellona, *Diritto, sistema e senso: lineamenti di una teoria*, Torino, 1996.

Un principio – questo – sistematico ed evolutivo, che sovrasta la fonte regolamentare e ne orienta le qualificazioni[67]. Da questa prospettiva, negare il controllo sui dati costruiti dall'AI significa disattendere la tutela della persona umana proprio dove quest'ultima è più vulnerabile[68]: è intuitivo che la natura "artificiale" e – in certo senso – soggettiva delle inferenze accresca il rischio di arbitrio del potere dell'appartato tecnologico-digitale. Con altre parole: la vulnerabilità della persona (digitale) ad esso esposta[69]. È chiaro perciò che «l'imputazione impersonale del potere a una entità esterna non può divenire la via per esercitare un potere senza responsabilità»[70].

Sotto questo aspetto, il collegamento tra il principio di tutela della persona umana e la categoria semantica della *privacy* è assai nitido: «se io sono i miei dati, tutto ciò che è fatto ai miei dati è fatto a me, non a ciò che possiedo». E si palesa che "*privacy*" intercetta il doppio, paradossale problema di tutela posto dalla datificazione della persona umana nella società digitale: le ICT ci costituiscono come abitanti dell'infosfera in virtù di dati tanto pervasivi quanto riduttivi: per un verso, possono "denudare" l'intimità delle nostre vite, persino negli aspetti più sensibili[71]; per l'altro ci tipizzano: ci semplificano in profili insensibili – per definizione – all'irripetibile singolarità delle nostre identità individuali[72] ma – ciò nonostante

---

[67] Su questo aspetto, l'approfondita e acuta analisi di Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, cit., p. 35 ss.

[68] Rodotà, *Il diritto di avere diritti*, cit., p. 312 ss.; Hildebrandt e Gutwirth, *Profiling the European Citizens: Cross-Disciplinary Perspectives*, Berlino, 2010.

[69] Rodotà, *Il diritto di avere diritti*, cit., p. 328.

[70] Rodotà, *Il diritto di avere diritti*, cit., p. 403.

[71] Che, sotto questo aspetto, sia in gioco l'eguaglianza è chiarito conclusivamente da Rodotà, *Il diritto di avere diritti*, cit., p. 321.

[72] «Se si considera il punto di partenza dei sistemi delle macchine, questo sembra costituito proprio da una attenzione minuta, da una registrazione quasi senza precedenti di qualsiasi caratteristica individuale. Tutto è raccolto, ma non per esaltare la persona nella sua individualità, per accrescerne l'autonomia, ma per consegnarla a dispositivi tecnologici che prescindono da singolarità e libertà. La costruzione di profili individuali, familiari, di gruppo costituisce una gabbia ancor più costrittiva di quella degli *status*. L'autodeterminazione diventa irrilevante di fron-

– volti a prevedere i nostri comportamenti e perciò anticipare sviluppi e modificazioni dell'identità. Come dire – sotto quest'ultimo profilo – che le ICT, in virtù dei nostri dati, ci rendono trasparenti ma, allo stesso tempo, ci distorcono[73]. Per sintetizzare: l'idea di *privacy* comunica un'esigenza comune alla pluralità delle sue "anime": il distacco tra la persona e la sua identità sociale, amplificato dalle ICT, non può comportare la consegna dell'identità all'arbitrio del potere digitale[74]. Questo è, infatti, il suo ruolo strategico nella tutela giuridica della persona umana nella società della comunicazione: disciplinare e limitare il potere degli altri di ricostruire la nostra identità sociale: l'immagine attraverso cui la società ci conosce e sulla cui base assume le decisioni che ci riguardano.

Sotto questo aspetto, la centralità dell'AI nella ricostruzione "informazionale" delle identità personali, alla base delle pratiche fondamentali della società digitale (profilazioni e decisioni automatizzate), produce una esigenza tanto evidente quanto ineludibile: coniare categorie giuridiche adeguate ai processi "epistemologici" delle macchine, che non seguono la logica causale ma quella inferenziale; non verificano ipotesi ma stabiliscono correlazioni e restituiscono previsioni[75]. I meccanismi di controllo debbono essere conseguentemente adattati. Verificare l'accuratezza del dato costruito dall'AI è decisivo per la strategia giuridica di tutela della persona, alla stregua del potere fondamentale che il diritto conia: controllare i processi di (etero)costruzione della propria identità.

---

te all'identità assegnata attraverso procedimenti automatici, La nuova astrazione produce uno svuotamento dell'umano, sì che diventa problematico pure l'affermare che siamo di fronte a una nuova "antropologia"». Così Rodotà, *Il diritto di avere diritti*, cit., p. 340.

[73] L'immersione della vita umana in un ambiente digitale intelligente accresce «il rischio di fraintendimenti dell'identità per effetto del divorzio tra mondo delle determinazioni consapevoli e mondo dell'elaborazione automatica»: Rodotà, *Il diritto di avere diritti*, cit., p. 325.

[74] Rodotà, *Il diritto di avere diritti*, cit., in particolare p. 327 ss.

[75] Burrell, *How the Machine «Thinks»: Understanding Opacity in Machine Learning Algorithms*, in B*ig-data & Society*, 2016, www.journals.sagepub.com; Anderson, *Deliberative, Agnostic and Algorithmic Accountability*, in *New Media & Society*, 2017.

4. *Data Protection* e *Algo-Created Data*

La tesi che nega al titolare dei dati personali il potere giuridico di controllare le inferenze che lo riguardano prospetta un altro argomento, incentrato sull'ambito di applicazione del Regolamento e sull'oggetto della *Data-Protection*. L'interpretazione fornita è restrittiva: la disciplina giuridica della protezione dei dati personali non riguarderebbe l'accuratezza dei processi decisionali né – conseguentemente – quella delle decisioni che ne costituiscono output[76].

In questa ricostruzione, l'accuratezza dei dati derivati e/o inferiti non sarebbe problema di *Data-Protection* per una ragione intrinseca alla "natura artificiale" di queste informazioni, palesata dal modello della loro "verificazione": controllare il "ragionamento" in cui l'inferenza consiste; con alte parole: controllare lo svolgersi del processo decisionale. Un'attività – questo è il punto – che non sarebbe disciplinata per una ragione non occasionale ma cruciale: l'estraneità all'ambito di applicazione e alla finalità del Regolamento. Per sintetizzare: lo spostamento del focus dal dato all'analisi che lo genera collocherebbe di per sé il problema del controllo dei dati costruiti al di fuori del contesto giuridico della protezione dei dati personali.

Neppure questa conclusione è condivisibile: è smentita dalla lettura logica ed assiologica del Regolamento che, nell'art. 22, attribuisce alla persona umana il potere di controllare l'accuratezza del processo decisionale che la riguarda quale processo di costruzione della sua persona digitale. Un potere – questo – che include essenzialmente il ragionamento inferenziale: la costruzione di "nuovi" dati che parlano della persona in virtù di valutazioni della sua personalità e previsioni dei suoi comportamenti[77].

---

[76] È l'attento esame della giurisprudenza europea effettuato da Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 29 ss.

[77] «*Profiling can involve an element of prediction, which increases the risk of inaccuracy. The input data may be inaccurate or irrelevant, or taken out of context. There may be something wrong with the algorithm used to identify correlations. The article 16 right to rectification might apply where,*

Anticipandone gli esiti: l'art. 22 inscrive i processi decisionali interamente automatizzati («incluse le profilazioni») nel sistema della *Data-Protection*, determinando la rilevanza, in quest'ambito, del "ragionamento artificiale" (la formazione della decisione algoritmica) in un aspetto cruciale: la elaborazione degli *output* e, quindi, le inferenze in virtù delle quali il sistema definisce l'identità della persona cui la decisione è destinata.

Ciò è chiaramente visibile da ciascuna delle due prospettive che orientano questa analisi: la logica funzionale dell'art. 22 quale regola del processo algoritmico e i principi fondamentali dell'ordinamento giuridico. La prima è centrata sulle garanzie che – secondo l'art. 22, par. 3 – condizionano la sospensione del divieto[78] – posto dal par. 1: sottoporre a persona a un processo decisionale interamente automatizzato – e perciò de-umanizzato – che produca effetti giuridici o conseguenze "analogamente significative" nella sua sfera vitale. In questi casi, la persona-titolare dei dati personali dispone di una pluralità di tutele che – come vedremo – operano *nel* procedimento automatizzato in virtù di un aspetto

---

for example, an individual is placed into a category that says something about their ability to perform a task, and that profile is based on incorrect information. Individuals may wish to challenge the accuracy of the data used and any grouping or category that has been applied to him»: Article 29 Data Protection Working Party, *Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679*, p. 17.

[78] Non può non osservarsi una peculiare simmetria: tra il divieto – appunto – di assoggettare l'individuo a un processo decisionale interamente automatizzato e quello di interferire nella sfera soggettiva altrui in cui si attua il comando di inviolabilità della persona umana: su questo tema, d'obbligo il rinvio a D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 348 ss.; Id., voce *Personalità (diritti della)*, in *Enc. dir.*, XXXIII, Milano, 1983, p. 355 ss.

Sulla ricostruzione del contenuto precettivo dell'art. 22, par. 1, il dibattito (risalente all'analoga formulazione linguistica contenuta nella dir. 95/46/CE) può ritenersi concluso alla stregua della persuasiva interpretazione dell'Art. 29 Working Party, *Guidelines*, cit., il divieto generale – non il diritto – è il *medium* tecnico coerente con il fine; la norma regolamentare pone perciò un divieto e identifica le sue eccezioni.

a tutte comune: controllare il "*reasoning*" della macchina; le ragioni che ne spiegano la decisione. Alla stregua dell'allineamento tra i processi decisionali considerati dal GDPR e quelli governati dell'AI, il minimo comune alle garanzie coniate dall'art. 22 risulta essere questo: riconoscere e controllare i processi inferenziali in virtù dei quali il sistema automatizzato costruisce i nuovi dati (c.d. derivati e/o inferiti), restituendo i profili dell'identità personale che "reputa" rilevanti ai fini della decisione finale.

Alla stregua dei principi fondamentali richiamati dal GDPR è chiara un'equivalenza: tra controllo delle inferenze e controllo dei processi di costruzione della propria identità. Anche da questa seconda prospettiva, il ruolo dell'art. 22 risulta centrale: regolando il processo decisionale automatizzato quale processo di costruzione algoritmica della persona digitale, la norma adegua la tutela giuridica della persona alle pratiche della società digitale in un aspetto cruciale: governare quel "distacco" tra la persona e la sua identità che la "datificazione" del mondo e la "crescente autonomia delle macchine" hanno compiuto. Questo è il *medium:* il potere della persona di controllare gli *algo-created data* quali dati costitutivi della sua persona digitale[79].

Le due prospettive hanno un punto comune, decisivo in questa riflessione: l'allineamento tra processi decisionali automatizzati e processi di etero-costruzione delle identità personali riflette quello tra processo decisionale e trattamento dei dati personali. È – questo – il punto di vista del GDPR: nel Regolamento, il processo decisionale automatizzato è un trattamento di dati personali e comporta la ricostruzione della personalità dell'individuo nei profili ritenuti rilevanti ai fini della decisione che lo riguarda.

---

[79] La prospettiva dell'AI rivela un altro aspetto del peculiare allineamento tra decisione (la conclusione del processo *ex* art. 22) e immagine della persona (digitale) restituita dal sistema automatizzato: per essere comprese (e controllate) entrambe richiedono un modello di spiegazione diverso e più complesso della mera *disclosure* dei dati personali trattati (la c.d. *data explanation*): un modello capace di spiegare le ragioni degli output ai quali il processo è finalizzato.

Nella fattispecie dell'art. 22, l'identità personale ha infatti un doppio valore: non solo costituisce il punto di applicazione finale della decisione: si tratta – per definizione – di decisioni capaci di produrre effetti giuridici che riguardano la persona o di incidere «in modo analogo significativamente» nella sua sfera vitale[80]; ma definisce le ragioni giustificatrici della decisione: la «valutazione di aspetti personali concernenti una persona fisica determinata» e la previsione di «aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione e gli spostamenti»[81].

---

[80] La decisione rilevante ai sensi dell'art. 22 GDPR è quella che «produca effetti giuridici» riguardanti l'interessato «o che incida in modo analogo significativamente sulla sua persona». Rispetto alla formulazione contenuta nella dir. 95/46/CE, il GDPR ha aggiunto alle parole «*significantly affects*» l'espressione «*similarly*». L'Art. 29 Working Party tenta sia di definire il criterio generale di qualificazione, sia di offrirne alcune declinazioni concrete. Sotto il primo profilo: «*the decision must have the potential to: significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or, at its most extreme, lead to the exclusion or discrimination of individuals*». Sotto il secondo profilo: «*decisions that affect someone's financial circumstances, such their eligibility to credit; decisions that affect someone's access to health services; decisions that deny someone an employment opportunity or put them a serious disadvantage; decisions that affect someone's access to education, for example university admissions*» (Article 29 Data Protection Working Party, *Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679*, p. 21 ss.).

[81] È il *considerando* n. 71: «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

Questo doppio ruolo palesa che controllare la decisione implica controllare la (etero)ricostruzione della propria identità e che, in questa operazione, il controllo delle inferenze valutative e predittive è cruciale.

La questione è decisiva per il controllo giuridico dell'AI. Peculiarità del trattamento regolato dall'art. 22 è essere interamente automatizzato; nel linguaggio della società digitale: "de-umanizzato" e governato dall'AI. Sotto questo aspetto, infatti, la norma disciplina una prassi fondamentale dell'infosfera, restituendo un'equivalenza: i processi decisionali interamente automatizzati sono (quelli) realizzati dall'AI. Ciò significa che, in questi casi, la ricostruzione dell'identità personale (costitutivamente implicata dal processo) è effettuata dalla macchina in virtù della *data-driven analysis* sviluppata dai suoi algoritmi e si basa sui dati che questi ultimi costruiscono a partire dai dati personali, alla stregua delle connessioni rintracciate nei c.d. *big-data*: i c.d. dati derivati e/o inferiti[82]. Con altre parole: gli *algo-created data*.

La doppia rilevanza di questi ultimi è scontata solo in apparenza: le inferenze, da un lato, costituiscono output algoritmici: "decisioni" prese dalla macchina sull'identità personale altrui – nella misura in cui "predicano" qualità e attributi di una persona fisica determinata; dall'altro lato, funzionano come presupposti della decisione finale cui l'intero processo risulta finalizzato: una decisione fondata – per definizione – sulla "valutazione" della personalità individuale che i dati costruiti dall'AI (derivati e/o inferiti)

---

giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona».

La medesima definizione del peculiare trattamento consistente nella profilazione è riprodotta nell'art. 4, par. 4, GDPR.

[82] Rodotà, *Il diritto di avere diritti*, cit., p. 336. La sintesi effettuata dall'A. è icastica: «L'incessante produzione di profili individuali, familiari e di gruppo, dunque la costruzione della nostra identità individuale e sociale, è affidata ad algoritmi, così come i calcoli presuntivi dei nostri consumi sulla base dei quali vengono definite le bollette da pagare» (p. 402).

ricompongono e descrivono[83]. Da questa prospettiva, gli *algo-created data* definiscono sia la decisione finale sia le sue ragioni.

Questa visione giuridica (il processo decisionale come trattamento dei dati personali), espressa dall'art. 22, definisce anche la trama razionale delle garanzie più specifiche che la norma (nel par. 3) fornisce alla persona soggetta alla decisione automatizzata: «il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione» (art. 22, par. 3). Tutte e ciascuna di quelle garanzie inverano un potere individuale di controllare il processo algoritmico che è modellato da una finalità: verificare il rispetto dei diritti e libertà fondamentali della persona umana posti in gioco della fenomenologia del trattamento ed implicati dalla *Data Protection* (art.1, par. 2, GDPR), alla stregua della corrispondenza che la *privacy* esprime: «se io sono i miei dati, tutto ciò che è fatto ai miei dati è fatto a me e non a ciò che possiedo»[84].

Anche l'ambito del controllo ne risulta definito, includendo come parte essenziale il "ragionamento" in virtù del quale la macchina restituisce la sua immagine della persona digitale – composta da "dati". È – questa inclusione – conseguenza del modello funzionale delle garanzie e dell'esigenza della loro effettività: i "diritti" definiti dal par. 3 risultano strumentalmente (ed essenzialmente) collegati a quello di conseguire informazioni significative sulla logica concretamente applicata dal processo automatizzato nella produzione dei suoi *outputs*[85]. Infatti, se il "ragionamento" prodotto dal sistema informatico resta incognito, risulta difficile contestare due conseguenze: per un verso, che l'intervento umano

---

[83] Ciò – come abbiamo ripetutamente osservato – è esplicitato nel *considerando* n. 71.

[84] Floridi, *Infosfera*, cit., p. 137.

[85] «*The data subject will only be able to challenge a decision or express their view if they fully understand how it has been made and on what basis*»: Art. 29 Working Party, *Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679*.

"pensato" proprio per governarlo ed eventualmente correggerlo risulti *ab origine* frustrato; per l'altro, che la decisione (*output*) finale, non manifestando le proprie *rationes*, non possa essere, nel merito, razionalmente contestata[86]. La rete delle connessioni funzionali interne all'art. 22 fornisce, quindi, indicazioni decisive per l'interpretazione: le garanzie coniate dall'art. 22, par. 3, GDPR, implicano, per la persona-titolare dei dati personali, la possibilità di comprendere[87] la logica e le *rationes* che hanno governato il processo decisionale quale processo avente ad oggetto e termine di riferimento finale la sua identità. È un aspetto essenziale del controllo della decisione. È la forza di questa implicazione a spiegare la peculiare configurazione della relazione comunicativa tra titolare dei dati personali e titolare del trattamento[88]: il diritto del

---

[86] Watcher, Mittelstadt e 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, p. 105 s.: «*The right to contest a decision, to obtain human intervention or to express views granted in Article 22 (3) may be meaningless if the data subject cannot understand how the contested decision was made. To this end, a right to explanation can be introduced requiring data controllers to provide information about the* rationale *of the contested decision*».

[87] Malgieri e Comandè, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017; Goodman e Flaxman, *EU Regulations on Algoritmic Decision-Making and a Rigt to Explanation*, in *AI Magazine*, 2017; Selbst e Powles, *Meaningful Information and the Right to Explanation*, in *International Data Privacy Law*, 2017.

[88] «*The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision. The GDPR requires the controller to provide meaningful information about the logic involved, not necessary a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be sufficiently comprehensive for the data subject to understand the reasons for the decision*» per Article 29 Data Protection Working Party, *Guidelines on Automated decision-making and Profiling for the purposes of Regulation 2016/679*, p. 25. Per critica dell'attività interpretativa del WP art. 29, Veale e Edwards, *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, in *Computer Law & Security Review*, 2018, p. 398 ss. Gli autori

primo di ottenere una spiegazione della decisione «conseguita dopo la valutazione degli aspetti personali che lo riguardano». Quale presupposto indispensabile dei diritti che condizionano la possibilità giuridica del processo decisionale interamente automatizzato, il diritto di conoscere le ragioni della decisione è – esso stesso – un pilastro del *due process* algoritmico[89].

Non è dunque vero che nel sistema del GDPR il "ragionamento" sviluppato nel processo decisionale non sia considerato: l'art. 22 restituisce la rilevanza giuridica dell'interesse della persona a controllare la costruzione degli output dei sistemi automatizzati[90]. Il discorso è tanto semplice da apparire scontato: l'art. 22 riconosce e tutela l'interesse della persona al controllo della decisione quale output di un processo algoritmico; di conseguenza, controllare la decisione non può non significare controllare il processo che la produce. Che questo interesse abbia ad oggetto le inferenze è chiaro sia dal profilo pragmatico sia da quello teorico. Il primo riflette la centralità delle inferenze nel modello di "*reasoning*" sviluppato dagli algoritmi dell'AI. Come abbiamo visto, i dati costruiti

---

rilevano non soltanto mancanza di chiarezza nel discorso interpretativo del WP ma ampi sconfinamenti nell'attività creativa di diritto.

[89] Alla stregua dell'art. 22, par. 1, «l'interessato ha diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato»: il quale, cioè, sia interamente governato dalla macchina, senza alcuna reale e significativa supervisione umana. Il par. 2 introduce tre categorie di eccezioni al divieto di decisione totalmente algoritmica stabilito dal par. precedente. Il par. 3 conia le garanzie minime per l'individuo sottoposto alla decisione algoritmica. Il rapporto tra le tre norme è chiaro: il divieto di sottoporre una persona fisica a una decisione basata unicamente sul trattamento automatizzato è la regola generale; le situazioni descritte dal par. 2 introducono l'eccezione: quando si verificano, il divieto posto dal par. 1 viene sospeso, e sottoporre una persona fisica a processo decisionale interamente algoritmico è possibile giuridicamente (lecito) a condizione che siano garantiti alla persona i diritti individuati dal par. 3. In questo senso, per la loro forza condizionante, i diritti previsti dall'art. 22, comma 3 costituiscono i pilastri del "*due process*" algoritmico e "de-umanizzato".

[90] Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., in particolare, p. 50 ss.

dall'AI costituiscono output – intermedi o conclusivi – del processo automatizzato che identificano nodi cruciali tanto del processo decisionale applicato a una persona fisica, quanto della ricostruzione della sua personalità posta alla base della decisione. Per sintetizzare: contestare la decisione implica innanzitutto conoscerne le ragioni, ciò che significa identificare e comprendere le inferenze in virtù delle quali la decisione viene "prodotta"[91].

D'altro canto, il profilo teorico restituisce la centralità delle inferenze nella costruzione della persona digitale, manifestando che l'interesse al controllo delle inferenze attiene al modo in cui la persona è "vista" e valutata dall'intelligenza artificiale[92]. Abbiamo già visto che questo aspetto è decisivo: il GDPR regola il processo decisionale in quanto (e nella misura in cui) è processo di costruzione della persona digitale. Da questa prospettiva, il controllo delle inferenze (*algo-created data*) risulta momento essenziale del controllo individuale sui processi di costruzione della propria identità in cui si invera la "seconda anima" della privacy. Possiamo trarre una prima conclusione e delimitare l'ambito dell'indagine: è quello dei diritti fondamentali della persona umana il piano del nostro quesito: *come* controllare le inferenze valutative e predittive che disegnano l'identità della persona digitale? [93]

5. L'identità della persona digitale

L'art. 22 riconosce alla persona umana, soggetta al *potere* decisionale digitale, il *diritto* di ottenere una spiegazione del ragionamento inferenziale, quale momento cruciale della costruzione

---

[91] Zarsky, *The Trouble with Algorithmic Decisions. An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making* in *Science, Technology, & Human Values,* 2016.

[92] Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit.

[93] Secondo Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., è un aspetto decisivo perché il diritto al controllo sia sensato: «*if there are no standards for making decisions. decision-makers will never be in violation of the law*» (p. 81).

algoritmica della sua identità (implicata dalla decisione)[94]. Con le parole del *considerando* n. 71: il diritto ad una spiegazione della decisione «conseguita dopo la valutazione di aspetti personali che lo riguardano» (*right to ex post explanation*).

È palese, tuttavia, che l'informazione garantita da quel diritto (conoscere le ragioni della decisione) abbia valore necessario ma non conclusivo per la realizzazione della sua finalità; la trasparenza è *medium*[95] per l'effettività di un diritto fondamentale della persona umana: controllare i processi di costruzione e utilizzazione della propria identità quale "dispositivo di socializzazione". Come abbiamo visto, l'oggetto dell'informazione è modellato dalla norma proprio in funzione del controllo. È il sistema della *Data Protection* – che tutela i dati per tutelare la persona umana – a definirne ambito e finalità: occorre poter "vedere"[96] ciò che serve a verificare il rispetto dei diritti, libertà e principi fondamentali posti *naturaliter* in gioco dalla *fenomenologia* del trattamento dei dati personali. Il senso del controllo è questo: verificare che la ricostruzione interamente automatizzata della personalità individuale, anche negli aspetti valutativi e predittivi, rispetti il valore giuridico della persona umana e il principio formale della sua tutela: il divieto di interferenze lesive nello spazio di esplicazione della persona umana – come esistenzialità[97].

---

[94] Secondo Kaminsky e Malgieri, *Algorithmic Impact Assessment under the GDPR: Producing Multi-layered Explanations*, il controllo del ragionamento artificiale è aspetto centrale anche della valutazione d'impatto (DPIA).

[95] Le modalità dell'informazione "trasparente" sono prescritte dall'art. 12, par. 1, GDPR. Che il problema della trasparenza delle informazioni non consista semplicemente nella disponibilità delle informazioni medesime ma anche in quello della loro utilità rispetto a finalità definite è il dato posto alla base delle riflessioni svolte in EPRS, *A governance framework for algorithmic accountability and transparency*, 2019.

[96] Malgieri e Comandè, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, cit.

[97] Scontato quanto fondamentale il riferito a D. Messinetti, *Personalità,* cit., Id., *Recenti orientamenti sulla tutela della persona. La moltiplicazione dei diritti e dei danni*, in *Riv. crit. dir. priv.*, 1992, p. 173 ss; Id. *Circolazione dei dati personali*, cit., p. 339 ss. Secondo la conclusiva interpretazio-

Nel discorso prescrittivo del GDPR, il riferimento ai diritti fondamentali della persona umana esprime, infatti, un'esigenza cruciale: definire le condizioni di liceità dell'intromissione nella sfera giuridica della persona realizzata in virtù del "trattamento" dei dati che la riguardano.[98] Con altre parole: rinvia alla questione del bilanciamento tra principi antagonisti nell'infosfera e alla selezione dei criteri che, di volta in volta, permettono la soluzione del conflitto[99].

Esemplare di questa operazione è il requisito dell'esattezza dei dati personali – prescritto dall'art. 5, par. 1, lett. "e" del Regolamento. Come abbiamo visto, "esattezza" definisce uno standard di liceità dell'attività di trattamento che ha natura oggettiva: la rispondenza tra l'informazione fornita dal dato personale (il contenuto informativo del dato) e la situazione della realtà rappresentata dal dato medesimo.

Se ne comprende, di conseguenza, il doppio effetto: orientare il potere di controllo del titolare dei dati personali (sulla veridicità

---

ne di questo Autore, la forma della rilevanza giuridica della personalità umana è oggettiva: inclusa nel comando di inviolabilità della persona, si esprime in maniera autosufficiente in virtù del divieto di interferenze lesive negli spazi di autodeterminazione della identità, come "bisogno" di differenziazione e di conservazione della propria differenza dagli altri. Si comprende che la tutela è forte perché l'esplicazione della personalità individuale non avviene in virtù di poteri che siano conferiti dalla norma giuridica al soggetto ma di libertà che sono dati esistenziali, modi dell'essere. Con altre parole: la persona non ha bisogno dell'attribuzione normativa di poteri attivi di realizzazione per esplicarsi nelle sue proiezioni esistenziali, ma si svolge da sé: nella dimensione dell'essere non sono comprensibili poteri giuridici di soddisfazione degli interessi connessi ai vari e diversi profili dell'esistenzialità.

[98] Come abbiamo ripetutamente osservato, la concezione "autofondativa" della *privacy* palesa che il trattamento è, di per sé, una intromissione nella sfera della persona.

[99] L'architettura del GDPR è articolata intorno al problema del conflitto tra polarità assiologiche contrapposte; su questo aspetto cruciale per l'interpretazione, si veda l'acuta analisi di Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà fondamentali tra mercato e persona*, cit.; Id., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2019, in particolare, p. 10 ss.

delle informazioni utilizzate ed elaborate nel trattamento) e individuare la funzionalità dello strumento rimediale appropriato al caso (la rettificazione dei dati inesatti).

La prescrizione per cui il dato deve essere esatto definisce perciò un aspetto cruciale della disciplina giuridica dell'attività di elaborazione di informazioni relative alla persona: porre un limite ragionevole al potere di ridefinire l'identità personale altrui. È chiaro infatti che, in tal modo, il diritto regola la costruzione dell'immagine attraverso cui la società conosce la persona e sulla cui base assume le decisioni che la riguardano.

Il tipo di problema normativo governato dal requisito dell'esattezza rinvia perciò al c.d. diritto all'identità personale *stricto sensu*[100] e alla sua funzione sistemica: tutelare l'individuo nelle situazioni in cui lesione della sua personalità (*rectius*: la violazione del comando di inviolabilità della persona umana)[101] è realizzata comunicando immagini della persona significativamente difformi da quella oggettivata nella prassi[102].

Il riferimento alla teorica del diritto all'identità personale appare perciò intuitivamente utile, nella nostra riflessione, in molteplici aspetti. In primo luogo, manifesta che il diritto oggettivo riconosce l'architettura relazionale dei processi di costruzione

---

[100]Nella prospettiva della "moltiplicazione" dei diritti della persona (sulla quale, D. Messinetti, *Recenti orientamenti*, cit.) la giurisprudenza ha costruito il diritto all'identità personale (su questo aspetto, l'approfondita analisi di Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003, p.127 ss.) per tutelare l'interesse «a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc., quale si era estrinsecato od appariva in base a circostanze concrete e univoche destinato a estrinsecarsi nell'ambiente sociale»: Cass. 22 giugno 1985, n. 3769, in *Foro it*., 1985, I, p. 2211 ss., con note critiche di Pardolesi.

[101]D. Messinetti, *Personalità*, cit.

[102]«È l'interesse del soggetto ad essere rappresentato nella vita di relazione con la sua vera identità così come questa nella realtà sociale generale o particolare è conosciuta o poteva essere conosciuta con l'applicazione dei criteri della normale diligenza e della buona fede oggettiva» (Cass., 22 giugno 1985, n. 3768).

dell'identità personale; il fatto – cioè – che l'identità è un "oggetto sociale complesso"[103] e la socializzazione dell'individuo avviene in virtù di "immagini" della sua identità delle quali egli non è autore esclusivo: queste infatti restituiscono anche la percezione che "gli altri" hanno della persona ed includono, di conseguenza, i "significati" generati dalla interpretazione del suo agire sociale[104].

In questo aspetto si palesa il doppio significato dell'espressione «diritto all'identità personale» nel contesto della tutela giuridica della persona: esprimere l'esigenza che la rappresentazione dell'identità personale altrui risponda a criteri oggettivi[105] e sia, di conseguenza, controllabile; definire una strategia rimediale adeguata alla natura comunicativa dell'evento lesivo[106].

---

[103] Rodotà, *Il diritto di avere diritti*, cit., p. 312.

[104] Berlin, *Two Concepts of Liberty*, in *Four Essays on Liberty*, New York and London, 1969, p.118: «Perché, in un certo senso, non sono io quel che sono in virtù di ciò che gli altri pensano o hanno l'impressione che io sia? Quando chiedo a me stesso cosa sono, e mi rispondo: un inglese, un cinese, un mercante, un uomo di nessuna importanza, un milionario, un condannato – mi accorgo, dopo aver analizzato la questione, che il fatto di possedere questi attributi comporta l'essere riconosciuto come appartenente ad un determinato gruppo o classe da parte di altre persone della mia società, e che tale riconoscimento fa parte del significato della maggior parte dei termini che denotano alcune mie caratteristiche più personali e immutabili. Io non sono una mente priva di corpo, né sono Robinson Crusoe solo sulla sua isola. Non soltanto la mia vita materiale dipende dall'interazione con altri uomini ed io sono quel che sono quale risultato di certe relazioni sociali, ma alcune, forse tutte, le mie idee su me stesso, ed in particolare il senso della mia identità morale e sociale, sono intellegibili soltanto nell'ambito dell'ambiente sociale di cui costituisco un elemento (la metafora non deve essere spinta troppo in là)».

[105] L'alterazione rileva in sé in quanto produce difformità non già in quanto sia peggiorativa o addirittura eventualmente migliorativa dell'immagine del soggetto secondo standard condivisi di apprezzamento sociale. D'obbligo il riferimento a Gambaro, *Falsa luce negli occhi del pubblico (False light in public eye)*, in *Riv. dir. civ*., 1981, p. 84 ss.

[106] La più autorevole dottrina ha conclusivamente chiarito che i c.d. diritti della personalità non costituiscono fattispecie attuative di specifici, differenziati interessi ma rappresentano «formule descrittive dei poteri (rimedi) attribuiti al soggetto in conseguenza dell'illecito; poteri che si

Sebbene nella sua elaborazione originaria questo "diritto della personalità" riguardi la rappresentazione della persona effettuata dai media tradizionali, il tipo di problema normativo che essa esprime si rispecchia in quello che le ICT ripropongono e amplificano in virtù del distacco tra l'individuo e la sua persona sociale[107].

Osserva Rodotà che: «La progressiva immersione in un "ambiente intelligente", popolato da oggetti "intelligenti", produce uno slittamento ulteriore rispetto a quello che ha determinato una progressiva separazione/contrapposizione tre il sé e gli altri per quanto riguarda la costruzione dell'identità[108]. Si va verso una sempre

---

specificano in relazione al singolo comportamento da reprimere ed ai suoi effetti». La valutazione di antigiuridicità del comportamento non deriva infatti dalla contrarietà ai singoli aspetti nominati, ma «dalla non conformità al valore giuridico fondamentale della persona, come tale» [D. Messinetti, *Personalità (diritti della)*, cit.; Id., *Recenti orientamenti*, cit., p. 179 ss.].

[107]Quale espressione esistenziale della persona umana, la tutela dell'identità personale viene ricondotta ai "diritti inviolabili" riconosciuti dall'art. 2 Cost: «è certamente vero che, tra i diritti che formano il patrimonio irretrattabile della persona umana, l'articolo 2 Cost riconosce e garantisce anche il diritto all'identità personale. Si tratta – come efficacemente è stato affermato – del diritto ad essere se stesso, inteso come rispetto dell'immagine di partecipe della vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano e, al tempo stesso, qualificano l'individuo. L'identità personale costituisce quindi un bene per sé medesima indipendentemente dalla condizione personale sociale, dei pregi e dei difetti del soggetto, di guisa che a ciascuno è riconosciuto il diritto a che la sua individualità sia preservata» (Corte cost., 3 febbraio 94, n.13). Su questi aspetti, l'analisi di Zatti, *Il diritto all'identità personale e l'applicazione diretta dell'art. 2 Cost.*, in *Il diritto all'identità personale*, a cura di Alpa, Bessone e Boneschi, Padova, 1981, p. 53 ss.

[108]Su questo aspetto, Rodotà, *Il diritto di avere diritti*, cit., p. 318 ss. La legge non protegge l'idea che il soggetto ha di sé ma l'immagine del soggetto che si è oggettivata nella prassi. L'identità in senso giuridico ha perciò una consistenza oggettiva: «deve essere verificata e definita con riscontri obiettivi in relazione a posizioni accertabili ed emergenti dell'individuo nella società con esclusione della tutela di idee e convinzioni o patrimoni culturali che rimangano nella sfera intima del soggetto, che il soggetto ritiene ma non ha manifestato»: Trib. Roma, 27 marzo 1984, in

più marcata separazione tra mondo delle persone e mondo delle macchine, per la crescente autonomia di quest'ultimo. Si accentua il trasferimento del potere di definizione della persona e della sua identità dall'ambito della valutazione umana a quello della decisione automatica»[109].

È – questo – un punto cruciale per intercettare il peculiare potenziale di lesività della persona: quel distacco definisce lo spazio che è "aperto" e reso disponibile all'arbitrio dell'AI. L'eventualità di costruzioni arbitrarie della personalità umana da parte dell'AI è intuitivamente correlata alla natura "costruita" dei c.d. dati derivati e/o inferiti e, perciò, dell'immagine algoritmica della persona[110]. Per semplificare: l'AI non si limita a ricostruire ma costruisce; innova il campo dei significati che definiscono l'identità personale[111].

A questa scontata puntualizzazione corrispondono questioni delicate. In primo luogo: come coniugare il potere digitale di definire la persona umana con quello individuale di autodeterminare la propria identità?[112] Il potere algoritmico interferisce infatti su un potere soggettivo che è un diritto fondamentale della persona umana; lo sfida proprio nel suo nucleo intangibile, ri-forgiato dalla contemporaneità: garantire all'individuo "datificato" il controllo sui processi di costruzione della propria identità[113].

Foro it., 1985, I, p. 1687 ss.

[109]Rodotà, *Il diritto*, cit., p. 328

[110]Una creatività connotata da due elementi critici: l'opacità che avvolge i processi dell'AI (la fallacia del paradigma della trasparenza in particolare rispetto agli algoritmi dell'apprendimento autonomo – *Machine-Learning*) e la scarsa verificabilità delle inferenze valutative e predittive – per le ragioni che abbiamo già evidenziato.

[111]D. Messinetti, *Recenti orientamenti*, cit., p.185 ss.

[112]Come abbiamo detto, è scontato che non «sia sempre e soltanto l'interessato a definire le condizioni per la definizione dell'identità. Non è mai stato così, la costruzione dell'identità non può essere confusa con un diritto all'autorappresentazione. Ma il mutamento tecnologico delle modalità di trattamento delle informazioni personali ha progressivamente alterato il rapporto tra l'identità liberamente costruita dal soggetto e l'intervento di terzi, attribuendo all'attività di questi ultimi un peso crescente»: Rodotà, *Il diritto*, cit., p. 318.

[113]Sulla relazione tra identità e privacy, d'obbligo il rinvio alla ricostru-

È – questo – un nodo cruciale del problema del limite al potere digitale in una società liberale e democratica. Sotto questo aspetto, è scontato che la capacità creativa dell'AI non possa costituire un potere assoluto sulla persona: determinare senza limiti chi la persona sia, le sue capacità di essere e di fare nella società. Il potenziale creativo della tecnologia invera il conflitto – intuito e prefigurato da Rodotà – tra autonomia della persona umana e autonomia della macchina, rafforzando l'esigenza etica e giuridica di proteggere la persona umana dall'arbitrio della decisione algoritmica[114].

Il problema, allora, è evitare risultati arbitrari allorché l'eterodeterminazione dell'identità implichi la peculiare forma di creatività propria dell'AI (l): creare informazioni che parlano della persona in virtù di valutazioni della sua personalità e previsioni del suo comportamento futuro. Per adeguare la tutela della persona al nuovo "formante tecnologico" della sua identità[115] occorre – perciò – definirne lo standard di accuratezza normativa[116].

---

zione teoretica di D. Messinetti, *Circolazione dei dati personali*, cit., in particolare p. 348 ss. Secondo l'A. «l'identità della persona ha sempre la forma della riservatezza come dato di comunicazione linguistica» (p. 350).

[114] Rodotà, *Il diritto di avere diritti*, cit., p. 319 ss.

[115] È chiaro, infatti, che la genesi peculiare dei dati personali "derivati" reagisce profondamente sui processi di configurazione dell'identità, riscrivendone il carattere in termini "computazionali" e rideterminando, di conseguenza, anche il problema giuridico fondamentale per la tutela della persona umana: coniare strumenti capaci di garantire forme di controllo dell'identità adeguate al carattere "artificiale" e, in larga parte, eterodeterminato della sua costruzione digitale.

[116] È il problema affrontato da Watcher e Mitteldstadt, *A Right to Reasonable Inferences*, cit. In un sistema fondato sul valore della persona e della sua autonomia, la forza dell'AI (tecnologia) non può certamente elidere l'esigenza di oggettività espressa dal c.d. diritto all'identità personale *stricto sensu*; ma questa esigenza deve essere riformulata coerentemente con la genesi del dato e la sua proprietà comunicativa (valutazione e previsione). È chiaro infatti che la lesione dell'identità (del valore giuridico della persona) è determinata dall'output – dal risultato comunicativo – del processo automatizzato ma in quanto la produzione dell'*output* sia "viziata".

6. Il diritto a inferenze ragionevoli

Come abbiamo già visto, la peculiarità comunicativa delle inferenze valutative e predittive non ne dimidia la "personalità": sono costitutive della persona digitale, definendo chi essa sia nella rete di relazioni e informazioni che compongono l'infosfera. In questo senso, le inferenze disegnano l'immagine alla stregua della quale vengono assunte le decisioni che riguardano la persona. Si comprende che debbano essere "accurate": inferenze inaccurate inficiano sia l'affidabilità della decisione sia quella della immagine della persona che descrivono. Come abbiamo visto, sono le facce di una stessa moneta.

Questa evidenza nasconde una questione tanto fondamentale quanto complessa: che cosa significa, nel linguaggio giuridico, "accuratezza" di previsioni e valutazioni? Qual è lo standard normativo di questa "verificazione"[117] ?

Per rispondere, è decisiva la prospettiva indicata da Rodotà: «le trasformazioni determinate dalla tecnologia possono essere comprese, e governate, solo se si è capaci di mettere a punto strumenti prospettici e se questo avviene ridefinendo i principi fondamentali delle libertà individuali e collettive»[118].

Esplorando questo orizzonte, una recente dottrina ha riscontrato un "nuovo" diritto della persona umana: ad "inferenze ragionevoli"[119]. È un interesse centrale nella società digitale: esse-

---

[117] Come abbiamo visto (*retro*, par. 3), la natura valutativa e i connotati comunicativi di questi output pongono delicati problemi che non sono riconducibili immediatamente alle soluzioni coniate in modo esplicito dall'art. 5 GDPR.

[118] Rodotà, *Tecnopolitica*, cit., p. XLI.

[119] Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit. Secondo questa dottrina, alla stregua di una concezione "olistica" della privacy e di un percorso analogo a quello tracciato dal diritto all'oblio, dovrebbe essere riconosciuto un diritto della persona "a come essere vista" dall'AI. È palese che il diritto ad inferenze ragionevoli riguardi il modo in cui la persona è vista e rappresentata dall'AI. Occorre chiedersi, invece, che cosa significhi dire che quel diritto debba essere riconosciuto, sciogliendo l'alternativa che segue: è il legislatore che deve riconoscerlo oppure è

re "visti" dall'AI in virtù di inferenze ragionevoli, nell'ambito delle situazioni – "ad alto rischio" – assimilabili ai processi di cui all'art. 22 GDPR[120]. La sua formalizzazione giuridica ne evidenzia la strategia nella categoria semantica della *privacy*: l'efficacia del potere di controllare la costruzione algoritmica della propria identità – effettuata con le inferenze. Il vincolo di compenetrazione tra il problema della ragionevolezza delle inferenze e il tema del controllo sulla eterocostruzione dell'identità personale è infatti palese ed ha significato univoco: nei processi governati dall'AI controllare l'identità significa controllare le inferenze e la ragionevolezza definisce il *quomodo* del controllo. La lettura ermeneutica del diritto ad inferenze ragionevoli fornisce perciò soluzione alla delicata questione della verificazione delle inferenze, completando un doppio passaggio, cruciale nella strategia giuridica di protezione della persona digitale. Il primo: assicurare l'effettività del diritto di contestare la decisione algoritmica (art. 22); il secondo: assicurare l'effettività del diritto di controllare la (costruzione sociale della) propria identità. In sintesi: il "diritto ad inferenze ragionevoli" risponde all'esigenza di "prendere sul serio" il nucleo intangibile del diritto alla *privacy* come strumento di tutela dell'identità personale.

---

l'interprete che non può non riconoscerlo nella trama del diritto europeo? In sintonia con la dottrina richiamata, non si dubita dell'opportunità di una ampia e partecipata discussione trans e multi-disciplinare per sviluppare tutte le possibilità "tecnologiche" che si offrono al discorso giuridico per conseguire l'obiettivo di una AI *trustworthy*. Neppure si dubita del contributo che il legislatore europeo può fornire alla certezza del diritto e all'esigenza di una tutela uniforme nello spazio dell'Unione. Tuttavia, alla stregua del carattere aperto ed elastico della tutela della persona e della concezione della privacy sviluppata da Rodotà, quel diritto risulta già esistente; come ho già anticipato, mi propongo di mostrare come rintracciarlo all'esito di una lettura sistematica ed assiologica del GDPR.

[120]Osservano giustamente Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 39 ss.; p. 49 ss. che il peculiare impatto delle decisioni di cui all'art. 22, unitamente alla pervasività e alla invasività dei processi algoritmici spiegano e giustificano la limitazione di attività riconducibili ai poteri di autonomia dei soggetti. Come abbiamo visto, l'avvento dell'AI comporta una radicale differenziazione dei problemi giuridici posti dai processi decisionali.

In questa ricostruzione, il significato attribuito all'espressione "ragionevole" identifica lo standard di controllo dell'accuratezza giuridica delle inferenze: un giudizio di "accettabilità normativa", rilevanza e affidabilità alla stregua di regole giuridiche, etiche e scientifiche che sono richiamate dal GDPR[121].

L'interpretazione ricerca la coerenza con le proprietà semantiche dell'espressione "*reasonable*" nel linguaggio comune per svilupparle in una doppia direzione: il contesto del GDPR e quello del principio fondamentale della tutela della persona umana.

Il primo manifesta che la risonanza tra *right to reasonable inferences* (la proposta ermeneutica) e *right to reasons explanations* (art. 22 e cons. 71) non è affatto casuale ma riflette connessioni strutturali profonde. Innanzitutto, quella tra inferenze e decisione algoritmica: il problema delle inferenze è inscritto costitutivamente nel contesto nel processo decisionale automatizzato. Come abbiamo visto, è l'art. 22 che, ponendo la regola dei processi automatizzati, definisce la rilevanza giuridica degli output, intermedi e conclusivi, elaborati nel ragionamento algoritmico.

---

[121] I primi due aspetti (accettabilità e rilevanza) rinviano a liceità e correttezza come principi del trattamento secondo l'enunciato dell'art. 5 GDPR; l'ultimo (affidabilità) rinvia alla previsione del *considerando* n. 71 nella parte in cui afferma che: «Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni».

In secondo luogo, il legame tra controllo delle inferenze e controllo della decisione automatizzata: il nucleo del modello di verificazione delle inferenze (implicato dal *right to reasonable inferences*) è quello individuato dall'art. 22 alla stregua del considerando n. 71: la *reasons explanation*. È – questo – un punto cruciale per la nostra riflessione, sul quale occorre soffermarsi. Il sintagma "*reasons explanation*" denota un processo comunicativo orientato a una doppia finalità: manifestare (rendere visibile e comprensibile)[122] l'architettura razionale del processo decisionale (la logica del ragionamento artificiale come ragionamento inferenziale) nonché giustificarla: dare conto della sua conformità a standard oggettivi, capaci di permettere un'intesa sulla sua accettabilità.

Con altre parole: fornire ragioni significa non solo disvelare ed esplicitare[123] ma anche giustificare.

Nel modello di "*reasons-explanation*" proposto, dare conto della ragionevolezza delle inferenze equivale, infatti, ad argomentarne l'accuratezza in virtù di un processo comunicativo peculiare: «*explain* 1) *why certain data are a normatively acceptable basis to draw inferences*[124]; 2) *why these inferences are normatively and relevant*[125] *for the chosen processing purpose or type of automated*

---

[122]La trasparenza deve implicare questa finalità; altrimenti è "inutile".

[123]Zarsky, *Transparent Predictions*, in *University of Illinois Law Review*, vol. 2013, p. 1521, il quale propone una «*call for mapping transparency*» basata sui seguenti elementi: «*(1) the collection of data and aggregation of datasets, (2) data analysis, and (3) actual strategies and practices for using the predictive models, effectiveness of which could be measured by both the way they are applied ex ante and their final impact ex post*».

[124]Secondo l'esemplificazione di Watcher e Mittelstadt, *A Right to Reasonable Inferences*, p. 128, è un problema di proporzionalità: «*The aim of the inference to be drawn should justify the means or sources of data being used in terms of invasiveness: inferring gambling or alcohol addiction to drive targeted advertising, for example, may actively harm the data subject*».

[125]«*Such as the relevance of Facebook profiles and friend network to loan decision*»: Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 128. Questo della rilevanza è profilo attentamente considerato da Art. 29 Working Party, *Guidelines on Automated Decision Making and Profiling for the Purposes of Regulation 2016/679.*

decision; and 3) *whether the data and methods used to draw the inferences are accurate and statistically reliable*».

Come abbiamo anticipato, la proposta ermeneutica trova saldo punto di ancoraggio nella teorica della tutela giuridica della persona umana. Sotto questo profilo, essa valorizza il legame tra privacy e identità secondo il senso – chiaro alla dottrina italiana – per cui la prima è lo strumento fondamentale per tutelare la seconda[126]. La concezione autofondativa della *privacy* – per cui «se io sono i miei dati tutto ciò che è fatto ai miei dati è fatto a me» – ne palesa la funzionalità: controllare i processi di elaborazione dei dati che mi riguardano significa controllare la costruzione della mia identità. È in questo orizzonte che il diritto della persona ad essere "vista" e rappresentata dall'AI in virtù di inferenze ragionevoli si riporta al principio della *privacy*[127]: ne riproduce il senso sistemico (controllare i processi di costruzione della propria identità) proprio nel profilo messo in gioco dalle nuove tecnologie: l'etero-costruzione della persona digitale in virtù delle inferenze mediante le quali si realizza, tipicamente, il "ragionamento" dell'AI. Il "diritto ad inferenze ragionevoli" definisce, infatti, un aspetto cruciale della risposta del diritto alla vulnerabilità della persona esposta al potere digitale: segnalare che l'immagine algoritmica della persona costruita in virtù di inferenze irragionevoli ne lede l'identità.

Questo inquadramento sistemico del problema delle inferenze (nel sistema della tutela giuridica della persona) mette in luce un doppio gioco di corrispondenze; il primo: tra controllo delle inferenze, controllo degli output del processo automatizzato (le decisioni algoritmiche) e controllo della persona sui processi di (etero) costruzione della sua identità.

Il secondo: tra oggetto del potere soggettivo di controllare le inferenze e limite oggettivo del potere algoritmico di definire l'i-

---

[126]«*One of the greatest risk of inferential Big-data analytics and automated decision-making is the loss of control over how individuals are perceived, and the predictability or intuitive link between actions and the perceptions of others*»: Watcher e Mittelstadt, *A Right to Reasonable Inferences*, cit., p. 97.

[127]Come abbiamo visto, ciò è esito di una interpretazione "olistica" della privacy: Watcher e Mittelstadt, *A Right*, cit., p. 88.

dentità personale. Sotto questo profilo, il controllo sulle inferenze ha ad oggetto la loro ragionevolezza perché l'immagine algoritmica della persona che sia restituita da inferenze irragionevoli è lesiva della sua identità.

"Ragionevolezza" definisce infatti contestualmente sia il criterio di "verificazione" dell'accuratezza normativa delle inferenze sia l'indicatore sistemico della violazione del principio della tutela della persona umana.

Nel primo ruolo, l'espressione rinvia ad un modello applicabile al ragionamento inferenziale in quanto tale: indipendente sia dalla natura giuridica personale o non dei dati che vengono processati al suo interno, sia dalla vocazione comunicativa del dato; sotto quest'ultimo profilo, è capace di ricomprendere i peculiari problemi di accuratezza posti dalle inferenze valutative e predittive le quali, non essendo fattuali, non si prestano per definizione ad essere verificate alla stregua del codice vero-falso. Il canone risulta perciò adeguato ai processi decisionali dell'intelligenza artificiale che sviluppano la *Big-data analytics*[128].

Proprio quale "misura" dell'accuratezza normativa della costruzione algoritmica dell'identità personale, nel secondo aspetto, la ragionevolezza costituisce il criterio di soluzione del conflitto tra l'autodeterminazione identitaria della persona esposta al potere di definizione dell'algoritmo e l'autonomia valutativa e decisionale di chi detiene l'apparato tecnologico. Come abbiamo già visto, essa governa questa relazione marcando il limite giuridico del potere digitale. In questo aspetto si manifesta il senso sistemico del diritto ad inferenze ragionevoli come diritto della personalità: intercettare le forme fenomeniche della patologia della prassi che producono la lesione del valore giuridico della persona nei processi di

[128] In queste ipotesi è l'applicazione delle inferenze alla persona a giustificare sul piano giuridico il potere soggettivo di controllarle secondo ragionevolezza. Come abbiamo osservato, le inferenze divengono "personali" nella misura in cui siano utilizzate per definire aspetti della persona; per inferire caratteristiche, qualità, comportamenti riferiti alla sua identità. Questa interpretazione – come abbiamo già visto – è in linea con la posizione dell'Art. 29 *Working Party*.

ricostruzione dell'identità individuale mediati dall'AI. Per realizzare questa funzione, il principio personalistico dispiega la sua autosufficienza in virtù della sua forma giuridica oggettiva.

Sul piano dei poteri individuali, invece, il GDPR fornisce un aggiornamento importante alle nuove esigenze della società digitale che la lettura logico-assiologica rende evidente. In questa prospettiva, l'espressione "diritto ad inferenze ragionevoli" interseca le varie norme che regolano la fattispecie di trattamento dei dati personali individuata dall'art. 22, configurando il paradigma fondamentale della relazione comunicativa tra titolare dei dati personali e titolare del trattamento. In primo luogo, essa ridefinisce e modula le diverse istanze cognitive protette dagli artt. 14 e 15 in virtù del comune riferimento lessicale alla "logica utilizzata" nel trattamento automatizzato. Ma realizza la sua funzione originale nel dialogo con il diritto di contestare la decisione. Nel contesto delle garanzie minime del processo algoritmico, il diritto ad inferenze ragionevoli condiziona in doppio modo quello di contestare la decisione: da un lato, collegandosi *naturaliter* al diritto di conoscerne le ragioni[129]; dall'altro, fornendo lo standard per verificare se la decisione abbia leso o non i diritti fondamentali della persona umana. Per sintetizzare: orientando in concreto il diritto di contestare la decisione, l'irragionevolezza delle inferenze funziona come *proxy* per la violazione dei diritti e libertà fondamentali della persona implicati dal trattamento dei dati che la riguardano.

7. Il *design* giuridico dell'infosfera

Con le regole (minime) delle decisioni algoritmiche inerenti la persona umana, il Regolamento Europeo definisce l'architettura dell'infosfera in un formante essenziale: la comunicazione tra uomo e macchina quali organismi informazionali. Come abbiamo osservato, regolando il processo decisionale automatizzato come processo di (ri)costruzione della persona digitale, il diritto discipli-

[129] Ciò nella misura in cui – come abbiamo già visto – le inferenze siano le ragioni della decisione.

na l'interazione comunicativa tra agente informazionale umano e quello artificiale configurandone *sub specie iuris* entrambi i poli: la comprensione umana della macchina e quella "macchinale" della persona umana[130].

L'obiettivo è chiaro: definire le condizioni di possibilità di un'intesa "ragionevole" tra le due intelligenze, correggendo la evidente asimmetria della relazione tra uomo e macchina implicata dal processo decisionale: la trasparenza dell'uomo – "datificato" – di fronte alla macchina e, per contro, l'opacità della macchina di fronte all'uomo che è "letto" dalla macchina[131].

Sotto il primo profilo – quello dell'intelligenza umana – il diritto vuole garantire alla persona la possibilità di comprendere la decisione che la riguarda e perciò – alla stregua della corrispondenza che abbiamo osservato – comprendere "come" la sua immagine sia "vista" e restituita dalla macchina. Potremmo parlare, in questo senso, del diritto della persona di comprendere, in termini "umani", la sua immagine algoritmica: è la "visione" che l'agente-macchina si costruisce della persona umana, per assumere le decisioni che riguardano quest'ultima, alla stregua del nuovo codice del mondo: la classificazione e il governo statistico della realtà[132].

Dal diritto a ricevere informazioni significative sulla logica del sistema [133] a quello di ottenere una spiegazione delle ragioni della decisione, la comunicazione è regolata dal punto di vista e per le finalità dell'intelligenza umana. È – questo – un nodo delicato: rendere umanamente comprensibile un modo di *intelligere* che è oscuro non solo per la radicale diversità da quello umano[134] ma anche perché tende a non lasciare traccia del proprio percorso. Larga parte della letteratura di Computer Science ritiene, infatti, che la logica che governa i processi algoritmici nei sistemi *Machi-*

---

[130] Per chiarire: la comprensione che la persona umana soggetta al potere decisionale della macchina deve avere di quest'ultima, da un lato; la comprensione che la macchina "acquisisce" della persona umana, dall'altro.

[131] Rodotà, *Il diritto di avere diritti*, cit., p. 337.

[132] Rodotà, *Tecnopolitica*, cit., p. 134 ss.

[133] Artt. 14 e 15 GDPR.

[134] Floridi, *La quarta rivoluzione,* citato ripetutamente nel testo.

ne Learning[135] non sarebbe attualmente conoscibile proprio relativamente alla fase – cruciale nella prospettiva del GDPR – della costruzione degli *outputs*[136]. Resterebbe incognito, specificamente, l'algoritmo "in azione"; il suo funzionamento nell'elaborazione dei nuovi dati (personali) e quindi nella costruzione delle "risposte" che il sistema intelligente restituisce all'ambiente esterno[137].

Sarebbe – questo – non un problema di mera comunicazione tra intelligenze diverse; la difficoltà di tradurre in linguaggi compatibili con la comprensione umana le logiche "autoprodotte" dell'intelligenza artificiale, ma un limite cognitivo strutturale, di natura tecnica, che allo stato attuale renderebbe praticamente impossibile, alla stregua dei modelli comunicativi sinora elabo-

---

[135]Sono i sistemi che, allo stato attuale, risultano maggiormente utilizzati nei processi decisionali automatizzati in virtù delle potenzialità dei c.d. *big data.*

[136]Siffatta impossibilità epistemica avrebbe la sua ragione nel *proprium* dei sistemi ML applicati all'AI: l'apprendimento autonomo. Si osserva, infatti, che in questi sistemi la logica del processo computazionale non sarebbe stabilita *ex ante* ma verrebbe coniata *in itinere*, dalle dinamiche peculiari dell'apprendimento concretamente realizzato; non sarebbe, cioè, predeterminata (dall'uomo) bensì verrebbe auto-definita (dal sistema) a mano a mano che il sistema apprende; ciò che, per definizione, avviene secondo modalità che non sono pre-configurate in virtù della programmazione, non risultando incluse in modo intelligibile nei suoi codici. Il limite cognitivo conseguente sarebbe insensibile alle scansioni cronologiche del processo automatizzato e, in questo senso, opererebbe come limite "assoluto": la logica effettivamente utilizzata dal sistema non soltanto non sarebbe esaustivamente rappresentabile *ex ante*, attesa l'imprevedibilità degli effetti computazionali dell'apprendimento autonomo, ma resterebbe incognita anche *ex post* per una ragione pratica: i sistemi ML e i c.d. *explanatory tools* a disposizione degli utilizzatori sarebbero stati sinora progettati non per fornire spiegazioni nel senso atteso dal GDPR ma per finalità affatto diverse, preordinate all'efficienza dei sistemi; *in primis*, curare l'affidabilità delle valutazioni predittive.

[137]Chiarissimi riferimenti in Burrell, *How the Machine «Thinks»: Understanding Opacity in Machine Learning Algorithms*, in *Big Data & Society*, 2016, www.journals.sage- pub.com; C.W. Anderson, *Deliberative, Agnostic and Algorithmic Accountability*, cit.; Danaher, T*he Threat of Algocracy: Reality, Resistance and Accommodation*, cit., p. 425 ss.

rati dall'informatica, ottenere il tipo di spiegazione richiesto dal GDPR[138]. In questa lettura, il diritto alla spiegazione della decisione algoritmica sarebbe nato già morto, ciò che fornirebbe altra prova dell'inadeguatezza digitale del GDPR[139].

Come ho cercato altrove di argomentare[140], la lettura non è condivisibile sotto il profilo dell'interpretazione giuridica. L'impatto delle regole della comunicazione uomo-macchina nell'assetto dell'infosfera è – al contrario – "costituzionale": il Regolamento inverte l'ordine tra diritto e tecnica, incorporando nell'AI principi etici e giuridici fondamentali nella società liberale e democratica. Innanzitutto, la trasparenza: la funzione prescrittiva del principio è messa in opera sia nella programmazione sia nella utilizzazione dei sistemi di AI che, per realizzare le finalità dell'art. 22 (cioè per effettuare processi decisionali interamente automatizzati e deumanizzati), devono rendersi "leggibili" – nel senso che abbiamo precisato.

Il condizionamento giuridico della tecnica è insuperabile[141], partendo da una considerazione: come abbiamo visto, nella trama complessiva del GDPR, il diritto di comprendere la produzione degli *outputs* algoritmici costituisce il *medium* necessario per l'esercizio di poteri fondamentali nei confronti dell'AI: *in primis* quello contestarne la decisione. In questo senso, il diritto alla spiegazione costituisce una garanzia che condiziona la possibilità giuridica

---

[138] Da questo punto di vista, il dibattito sulla "*feasibility*" del «*right to an ex post explanation*» ha radice nell'analoga formulazione linguistica contenuta nella dir. 95/46/CE. Su questi aspetti, Mendoza e Bygrave, *The Right Not to Be Subject to Automated Decisions Based on Profiling*, in *EU Internet Law: Regulation and Enforcement*, a cura di Synodinou, Jougleux, Markou e Prastitou, Springer, 2017, p. 77 ss.; Bygrave, *Minding the Machine: Article 15 of the Data Protection Directive and Automated Profiling*, in *Computer Law and Security Rev*., 2001; Hildebrandt, *The Dawn of a Critical Transparency Right for the Profiling Era*, cit.

[139] Edwards e Veale**,** *Slave to the Algorithm? Why a Right to an Explanation is Probably Not the Remedy You are Looking for*, cit., p. 18 ss.

[140] In *Contr. e impr.*, 2019, p. 861 ss.

[141] Rodotà, *Il diritto di avere diritti*, cit., p. 398 ss.

della soggezione della persona umana al potere decisionale della macchina[142].

È – questo – un aspetto cruciale per stabilire l'ordine della relazione tra l'impossibilità fattuale di esercitare con successo questo diritto (il limite tecnico) e la sua conseguenza giuridica: l'impossibilità di osservare le garanzie del GDPR – preservando i diritti dell'interessato – significa che non sussistono le condizioni per sospendere il divieto di sottoporre la persona al processo decisionale automatizzato posto dal primo comma dell'art. 22[143]. La significazione opera sul piano dei principi: in quelle situazioni, non può essere assicurato il "*due process*" rispetto a decisioni "ad alto rischio" per l'impatto giuridico e sociale nella sfera vitale della persona umana.

Coniando quei poteri individuali, il diritto oggettivo disegna l'architettura giuridica "minima" sia dei sistemi di AI sia dei processi decisionali che questi producono[144].

---

[142]Sottraendola perciò alla «dittatura dell'algoritmo» (Rodotà, *Il diritto di avere diritti*, cit., p. 401). Come sappiamo, la vulnerabilità della persona esposta al potere decisionale dell'apparato tecnologico è la chiave per comprendere il senso precettivo dell'art. 22 GDPR: il divieto di sottoporre la persona umana a processi decisionali interamente automatizzati è generale; può essere eccezionalmente sospeso nelle situazioni individuate dalla norma medesima e nel rispetto delle garanzie minime che questa definisce.

[143]Ritenere diversamente significa implicare che il diritto positivo possa affidare la sfera giuridica e vitale della persona umana al potere "conclusivo" della macchina; un potere, in certo senso, "assoluto" nella misura in cui si esprima in virtù di decisioni incontrollabili razionalmente: infatti – come abbiamo visto – un limite tecnologico – attualmente insuperato ma non insuperabile – non permetterebbe di decostruirle per lasciarne emergere le ragioni giustificatrici.

È chiaro che se all'autodeterminazione individuale si sostituisce l'etero-determinazione informatica, l'uomo è (divenuto) «materia prima del processo tecnologico» (Anders, *L'uomo è antiquato*, cit., p. 4); un «fantasma tecnologico» per Rodotà, *Il diritto di avere diritti*, cit., p. 199. Brillanti e originali le riflessioni di Di Raimo, *Decisione e attuazione algoritmiche delle situazioni sostanziali*, che si è potuto leggere per gentile concessione dell'A.

[144]Sull'incorporazione dei principi etici nell'AI per renderla "umano-centrica": OECD *Principles on AI* (2019); *Hambach Declaration on AI*

Dall'altro polo della relazione comunicativa, il "diritto ad inferenze ragionevoli" pone la regola fondamentale dell'intelligenza artificiale della persona umana in virtù della sua doppia, correlata funzione: individuare il limite all'autonomia della macchina nella costruzione della persona digitale[145]; configurare il potere della persona di controllare il "ragionamento" artificiale nei processi decisionali che la riguardano.

La trasparenza come *explainability* è perciò incorporata nei diritti della persona soggetta al processo algoritmico, in virtù del raccordo, che essi realizzano, tra "spiegare" le ragioni della decisione e "giustificare" la ragionevolezza delle inferenze[146]. È un punto importante: il raccordo pone in luce che quei diritti conformano una interazione comunicativa, nella quale il "controllo" garantito alla persona si realizza – a ben vedere – come partecipazione ai processi di costruzione della sua identità digitale. Con altre parole: è inverato il senso della privacy come «libertà da vincoli irragionevoli nella costruzione della propria identità»[147].

Si può dire, allora, che regolando le decisioni algoritmiche, il diritto regola i processi di costruzione della persona digitale, conformandoli come processi comunicativi tra agenti informazionali umani e artificiali[148]. In quest'ambito, la ragionevolezza "umana"

(2019) (Germany); ICO *Guidance on AI and Data Protection* (2020) (UK); *White House OMB Draft Memo on the Regulation of AI* (2020) (USA); *Rome Call for AI Ethics* (2020) e, da ultimo, *European Parliament Resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies*.

[145] È il problema del limite all'arbitrio del potere digitale – che abbiamo lungamente trattato.

[146] Abbiamo già osservato che la ragionevolezza delle inferenze integra la spiegazione delle ragioni della decisione in un aspetto decisivo includendo nell'oggetto del controllo la giustificazione delle inferenze e declinando il controllo come processo comunicativo.

[147] Agree e Rotenberg, *Technology and Privacy. The New Landscape*, Cambridge (Mass.), 2001, p. 6 s.

[148] Potremmo dire, in sintesi, che il diritto ripristina la natura comunicativa dell'identità come prodotto sociale e, attribuendo alla persona umana il potere di dialogare con l'AI, le restituisce il potere di autodeterminazione di cui le ICT la avevano privata.

costituisce la formula che media e rende possibile l'intesa comunicativa proprio allorché la distanza tra i due modi di *intelligere* l'individuo e la sua personalità appare più grande.

Uno strumento coniato per governare il "distacco" tra la persona umana e la sua persona digitale compiuto dalle ICT e preservarne la dignità. Il legame tra il principio di dignità e la privacy "reinventata" da Rodotà è palese e strettissimo: «l'integrità della persona si custodisce proprio se la persona non viene forzata entro schemi identitari che sfuggono al suo potere di costruzione o, almeno, al suo controllo»[149]. Diversamente, la persona è ridotta a un «fantasma tecnologico» e sarebbe tardivo chiedersi se la «società dell'algoritmo» possa essere democratica[150]. È – questa – la sfida che, alla stregua di una lettura sistematica ed assiologicamente orientata, il GDPR promette di vincere[151].

---

[149] Rodotà, *Il diritto di avere diritti*, cit., p. 199.

[150] Rodotà, *Il diritto di avere diritti*, cit., p. 404.

[151] Sebbene il GDPR, con l'art. 22, si occupi soltanto dei processi interamente gestiti dall'AI, le Carte etiche recentemente coniate dall'Europa lasciano immaginare che i principi fondamentali del *due process* algoritmico possano essere rimodulati ed applicati anche nei processi coadiuvati dall'AI.