Dati personali e decisioni automatizzate: quale trasparenza?*

Gianluca Fasano

Abstract

Le tecnologie basate sull'intelligenza artificiale sono incredibilmente diffuse nelle società contemporanee e i vantaggi derivanti sono evidenti in qualsiasi settore dell'attività umana. Trattandosi di meccanismi in grado di condizionare la vita delle persone, essi sollevano numerosi interrogativi sul piano sociale, etico e giuridico. Nel campo delle decisioni automatizzate, in particolare, molto è stato fatto per la protezione dei dati personali e, in tale scenario, un ruolo fondamentale è stato riconosciuto al principio di trasparenza. Principio che, oggi, andrebbe rafforzato con nuovi contenuti e garanzie, abbandonando la narrazione di strumento per la mera comprensione del funzionamento dei sistemi automatizzati – sofisticati e alle volte incomprensibili - e ricostruendolo invece come mezzo per acquisire consapevolezza circa i condizionamenti derivanti dal loro utilizzo e per garantire la partecipazione attiva dell'interessato allo sviluppo della sua identità digitale.

Technologies based on artificial intelligence are incredibly widespread in contemporary societies and the resulting benefits are evident in any sector of human activity. Since these are mechanisms capable of conditioning people's lives, they raise numerous questions on a social, ethical and legal level. In the field of automated decisions, in particular, much has been done for the protection of personal data and, in this scenario, a fundamental role has been recognized to the principle of transparency. A principle that, today, should be strengthened with new contents and guarantees, abandoning the narrative of a tool for the mere understanding of the functioning of automated systems - sophisticated and sometimes incomprehensible - and reconstructing it instead as a means of gaining awareness about the conditioning deriving from their use and to ensure the active participation of the interested party in the development of his digital identity.

Sommario

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

automatizzata. - 4. Le eccezioni al principio di non esclusività: il consenso. - 5. Conclusioni

Keywords

consenso – trasparenza - intelligenza artificiale - decisione automatizzata - trustworthy AI.

1. Introduzione

L'utilizzo di sistemi intelligenti porta vantaggi evidenti in molti settori dell'attività umana: l'intelligenza artificiale (IA)[1] riconosce il volto di una persona identificando un soggetto per esigenze di sicurezza, supporta i medici nella lettura delle immagini radiografiche migliorando le diagnosi e la prevenzione, offre maggiore sicurezza alla guida di automobili e nei trasporti, concorre alla tutela dell'ambiente ed altro ancora. Può anche facilitare l'accesso all'informazione, all'istruzione e alla formazione: con l'epidemia di COVID-19 l'apprendimento a distanza è diventato una necessità.

Le ragioni per sostituire, in alcune attività, gli esseri umani con sistemi automatizzati solitamente vengono ricondotte a vantaggi di elaborazione dati su larga scala, velocità, volume e alle aspettative di tassi di errore inferiori rispetto agli esseri umani. Di fondo, viene riconosciuta loro una maggiore efficienza rispetto alle capacità analitiche umane: gli algoritmi predittivi sono infatti in grado di analizzare quantità elevatissime di dati, anche fra loro eterogenei sotto il profilo qualitativo, individuandone preziose correlazioni, rapporti, inferenze che nessuna valutazione umana sarebbe in grado di rilevare. Queste qualità destano immancabilmente riconoscimento e apprezzamento ma, ciò nonostante, v'è da considerare che esse pongono all'uomo moderno considerevoli sfide, per alcune comprensibili ragioni. Innanzitutto, i sistemi intelligenti sono legati al crescente sviluppo del fenomeno dei cd. *Big Data*[2], il substrato di alimentazione degli

[1] Per Intelligenza Artificiale (IA) si intende «la scienza che sviluppa modelli computazionali del comportamento intelligente, e quindi fa sì che gli elaboratori possano eseguire compiti che richiederebbero intelligenza da parte dell'uomo», così G. Sartor, *Intelligenza artificiale e diritto*, Milano, 1996, 10. Tra le definizioni più accreditate spicca quella dell'Università di Stanford, che la identifica come «una scienza e un insieme di tecniche computazionali che vengono ispirate - pur operando tipicamente in maniera diversa - dal modo in cui gli esseri umani utilizzano il proprio sistema nervoso e il proprio corpo per sentire, imparare, ragionare e agire». Si veda *Artificial Intelligence and life in 2030, One hundred year study on Artificial Intelligence*, Stanford University, 2016, 5. L proposta di regolamento sull'utilizzo dei sistemi di intelligenza artificiale (IA) diffusa dalla Commissione europea il 21 aprile 2021 *[Proposal for a Regulation laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain unions legisative act,* COM(2021)206 final*]*, all'art. 3 reca la definizione di «sistema di intelligenza artificiale (sistema di IA): un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

[2] A. Mantelero, Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo, in *Il diritto dell'informazione e dell'informatica*, 2012, 135 ss. *Per una prospettiva internazionale volta alla tutela dei diritti* G. Della Morte, *Big Data e protezione internazionale dei diritti umani*, Napoli, 2018. Il concetto di big data è tradizionalmente spiegato facendo ricorso alla teoria delle cc.dd. 5V per indicare che tali dati sarebbero caratterizzati da: Volume (ossia grandi quantità di dati), Velocità (ossia la rapida disponibilità

algoritmi che, pur rappresentando una miniera di informazioni, ha bisogno di strumenti adeguati per poter essere sfruttato in tutto il loro potenziale, quali ad esempio «*modelli e metodi di recupero e filtraggio delle informazioni fondati su tecnologie semantiche e ontologie condivise*»[3].

Peraltro, molte delle nuove tecnologie sono in fase di sviluppo iniziale e non se ne conoscono appieno le implicazioni per individui, ambiente e società. Trattasi di un tema in magmatica evoluzione che mette in crisi il legislatore, per la difficoltà di poter intervenire con una regolamentazione efficace, al netto dell'incertezza sulla capacità dei concetti giuridici tradizionali di cogliere adeguatamente le sfide inedite poste dalle nuove tecnologie[4].

Quanto poi al carattere dell'efficienza, occorre indugiare su un suo aspetto determinante, inerente ai canoni rispetto ai quali possa fondarsi l'assunto della maggiore efficienza della decisione algoritmica. In linea generale, l'efficienza esprime una capacità di rendimento e di rispondenza a determinati fini, quelli scelti in fase di progettazione e sviluppo del sistema intelligente, in quanto tale misurabile con strumenti e metodi oggettivi. In tale prospettiva potremmo ritenere che le finalità impresse ai sistemi intelligenti ne sanciscono anche l'efficienza.

Ma, se spostiamo l'angolo visuale su un altro fronte, ponendoci dalla parte di coloro che sono destinatari, sia individualmente come diretti interessati sia collettivamente come gruppo che subisce gli effetti di decisioni automatizzate, ci rendiamo conto dei limiti di tale assunto: l'efficienza perseguita dai progettisti non sempre collima con i bisogni e le aspettative dei destinatari.

In effetti, nella progettazione degli algoritmi la modellazione prende avvio con la scelta degli obiettivi, in tal senso potremmo dire che gli algoritmi sono ideologicamente orientati, secondo target di efficienza in linea con gli interessi di sviluppatori e progettisti piuttosto che di giustizia, equità o di interesse della comunità[5].

Peraltro, occorre considerare che essi non riflettono in modo incorrotto la realtà anzi, essendo progettati allo scopo di ottenere determinati risultati attesi, si fondano su una pre-determinata rappresentazione della realtà, sotto forma di problemi da risolvere, di variabili incidenti e di parametri opportunamente categorizzati[6].

Siffatto limite si presenta ancor più critico quando i sistemi decisionali automatizzati vengono sviluppati per dare attuazione ad una determinata disposizione legislativa o

---

e analisi degli stessi), Varietà (ossia, da un punto di vista qualitativo, l'enorme tipologia di dati presenti), Variabilità (il contenuto dei dati muta di significato a seconda dell'analisi a cui è sottoposto) e Valore (dipende dal crescente potenziale economico e dalla valenza sociale dei dati).

[3] Sul punto il Libro Bianco dell'Agenzia per l'Italia Digitale del marzo 2018, *L'intelligenza artificiale al servizio del cittadino,* p. 52.

[4] Sul tema M. Bassini - L. Liguori - O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 334. Gli autori riflettono sulle difficoltà dei regolatori nel tenere il passo di questa rapidissima evoluzione tecnologica, evidenziando che occorre «valutare se sia opportuno, per i legislatori, coniare delle regole ad hoc, nuove, ovvero persistere, non senza possibili forzature avallate, magari, sul piano giurisprudenziale, nell'applicazione delle norme preesistenti».

[5] C. O'neil, *Armi di distruzione matematica*, Firenze-Milano, 2017, 190.

[6] A.C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in Rivista di filosofia del diritto, 1, 2019, 109.

amministrativa. Siamo nel campo della dell'informatica giuridica[7], scienza che studia, tra l'altro, se e come si possa pervenire all'applicazione automatica delle norme da parte del computer stesso o, quanto meno, come il computer possa aiutare il legislatore, il giurista, e più in generale qualsiasi operatore del diritto, nella loro attività. In questo campo non si tratta di interpretare la realtà materica ma di utilizzare la regola giuridica come categoria per l'interpretazione della realtà e degli interessi amministrati, non prima di averla tradotta "una volta per tutte" in codici e criteri - privi di ambiguità - che possono esser digeriti da un sistema decisionale automatizzato. Ebbene, tale attività interpretativa determinerà il nascere di una quasi-legislazione "nascosta"[8], con evidente rischio di allontanarsi dal bagaglio di valori, condivisi dalla società in un determinato contesto storico, sintetizzato nella regola giuridica.

Inoltre, quando entrano in gioco algoritmi di *machine learning*, o anche di *deep learning*, capaci del cd. autoapprendimento, le decisioni vengono prese utilizzando dati prodotti dalla macchina medesima, per i quali l'uomo ha difficoltà ad individuare punti di connessione con la realtà. Nel caso delle cd *black box* alcuni passaggi sono invisibili all'esterno e resta imperscrutabile l'uso effettivo che viene fatto degli algoritmi e dei dati[9].

In definitiva, gli esiti di un processo algoritmico derivano da una molteplicità di fattori, non ultimo quello derivante dalla qualità dei dati coinvolti nel training del procedimento automatizzato, per cui discutere di efficienza dei sistemi decisionali automatizzati è riduttivo, così come motivare il loro utilizzo esclusivamente da considerazioni di efficienza o efficacia, se non addirittura in termini di rapporti costi benefici, è arbitrario. Piuttosto, occorre interrogarsi sulle conseguenze che tali sistemi producono sulla vita dell'uomo, sulla salute, sull'ambiente e sulla società, interpretando così l'innovazione tecnologica non soltanto come trasformazione di un processo esistente in chiave di maggiore efficacia ma come sviluppo etico e sostenibile[10] dell'innovazione medesima[11].

È questa la prospettiva per costruire una IA affidabile, in cui un ruolo chiave viene

---

[7] In tal senso vengono alla mente le parole di Borruso che nel delineare i tratti salienti e distintivi della nuova materia di studio "*informatica giuridica*", che si veniva a delineare dagli anni '60 in poi, la indicò come quella in cui il "*diritto diventa oggetto dell'informatica*".

[8] D.W. Schartum, *Law and algorithms in the public domain, in Etikk i praksis*, in *Nordic Journal of Applied Ethics*, 1, 2016, 15 ss. L'autore dimostra che nello sviluppo di un algoritmo deputato a dare attuazione a una norma di legge l'algoritmo finisce per contenere un livello normativo clandestino.

[9] F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge - London, 2015; D. Pedreschi et al., *Meaningful Explanations of Black Box AI Decision Systems*, 33rd AAAI Conference on Artificial Intelligence (AAAI 2019), 33, 9780 ss.; L. Vigano - D. Magazzeni, *Explainable Security*, 2018.

[10] Indispensabile, anche se non sufficiente, un approccio che dia rilevanza all'etica come argine alle criticità dei sistemi intelligenti. In tal senso si veda la Risoluzione del Parlamento Europeo del 20 gennaio 2021 sull'intelligenza artificiale, secondo cui «…gli orientamenti in materia di etica, quali i principi adottati dal gruppo di esperti ad alto livello sull'intelligenza artificiale, costituiscono un buon punto di partenza ma non sono sufficienti per garantire che le imprese agiscano in modo equo e assicurino una protezione efficace degli individui».

[11] Il Consiglio per i diritti umani delle Nazioni Unite, il 22 marzo 2017, ha osservato con preoccupazione «…che il trattamento automatico dei dati personali per la profilazione individuale può portare a discriminazioni o decisioni che altrimenti potrebbero incidere sul godimento di diritti umani, compresi i diritti economici, sociali e culturali».

riconosciuto al principio di trasparenza[12]. Nelle pagine a seguire si procederà ad una disamina di tale principio in chiave di rivisitazione, abbandonando la tentazione di interpretarlo come mero strumento per la comprensione del funzionamento dei sistemi automatizzati[13] - spesso indecifrabili per l'uomo - e ricostruendolo invece come mezzo per acquisire consapevolezza circa le conseguenze del loro utilizzo[14] e per garantire che il consenso diventi un momento di partecipazione dell'interessato allo sviluppo della sua identità digitale.

2. La trasparenza delle decisioni automatizzate secondo la normativa europea del regolamento (UE) 679/2016

Attualmente il tema della trasparenza dei processi decisionali automatizzati trova una sua puntuale disciplina all'interno del Regolamento Europeo sulla Protezione dei Dati Personali, regolamento (UE) 679/2016 (da ora in poi anche GDPR), in cui rintracciamo sia principi generali validi ad orientare il comportamento degli attori della protezione dei dati, sia specifiche disposizioni sui sistemi decisionali automatizzati[15]. Il paradigma concettuale è rappresentato dagli artt. 12, 13, 14, 15 e 22 del GDPR, in cui risultano condensati i principi di trasparenza, di non esclusività della decisione auto-

[12] Si possono certamente menzionare la "*Raccomandazione sull'intelligenza artificiale*" emanata dall'Organisation for Economic Co-operation and Development nel maggio 2019, e la Carta etica sull'uso dell'intelligenze artificiale nei sistemi giudiziari, adottata nel contesto del Consiglio d'Europa dall'European Commission for the Efficiency of Justice (CEPEJ), nel dicembre del 2018, che si occupa di definire i principi che i responsabili politici, i legislatori e i professionisti dovrebbero adottare nell'affrontare il rapido sviluppo dell'intelligenza artificiale nel campo della giustizia e, più in particolare, nei sistemi giudiziari nazionali. La Commissione europea nella Communication "Building Trust in Human-Centric Artificial Intelligence", COM(2019)168 final, 8 aprile 2019, ha sostenuto i requisiti fondamentali stabiliti negli Orientamenti etici per una Intelligenza artificiale affidabile predisposto dal Gruppo di Alti esperti sull'IA.

[13] Il tema della trasparenza assume un rilievo diverso nell'ambito del processo di digitalizzazione della pubblica amministrazione, funzionale ad un'inclusione di cittadini e imprese, a garanzia della loro partecipazione democratica al funzionamento dello Stato. In tale scenario, il ricorso ad esempio all'automazione delle decisioni amministrative rende prevalente l'esigenza di poter sindacare la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della "regola" che governa l'algoritmo. Sull'argomento sia consentito richiamare a G. Fasano, *Le decisioni automatizzate nella pubblica amministrazione: tra esigenze di semplificazione e trasparenza algoritmica,* in questa *Rivista*, 3, 2019, 234 ss.

[14] Si veda, al riguardo, la recente legge francese sulla bioetica che ha imposto oneri informativi non soltanto sul funzionamento dei sistemi algoritmici ma anche «*de l'interprétation qui en résulte*», Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique, in particolare l'art. 17 che interviene a integrare il Codice della Sanità Pubblica.

[15] Sul tema delle decisioni automatizzate il GDPR può esser letto come il *trait d'union* tra la il primo trattato internazionale in materia di protezione dei dati personali, la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, nota anche come Convenzione 108, e la più recente Proposta di regolamento sull'utilizzo dei sistemi di intelligenza artificiale (IA,) diffusa dalla Commissione europea il 21 aprile 2021, cit. Il primo (con il successivo protocollo di modifica cd. Convenzione 108+) rappresenta uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali, poiché è l'unico strumento giuridicamente vincolante aperto anche a Stati non membri del Consiglio d'Europa. Il regolamento proposto in sede UE è destinato a disciplinare qualsiasi sistema di intelligenza artificiale anche qualora non sia previsto l"utilizzo di dati personali.

matizzata e del consenso, tutti collegati tra di loro al fine di consentire all'interessato un controllo sui propri dati[16].

La prescrizione generale è introdotta nell'art. 12 del GDPR, il quale comporta l'obbligo per il titolare del trattamento di fornire all'interessato le informazioni relative al trattamento «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro»[17]. Il contenuto informativo da portare a disposizione dell'interessato riguarda, in particolare, l'identità del titolare del trattamento e le finalità del trattamento nonché i rischi, le garanzie e i diritti relativi al trattamento dei dati personali che gli interessati possono esercitare.

Passando al livello ulteriore delle decisioni automatizzate, la disciplina della trasparenza diventa più rigorosa: il titolare del trattamento ha l'obbligo di notificare all'interessato alcune informazioni ulteriori, quali «l'esistenza di un processo decisionale automatizzato» nonché a fornire «informazioni significative sulla logica utilizzata» e «l'importanza e le conseguenze previste di tale trattamento per l'interessato»[18]. L'art. 22 GDPR cita espressamente la profilazione quale fenomeno da ricondurre sotto la disciplina delle decisioni automatizzate, probabilmente perché si tratta dell'applicazione più diffusa nella pratica e che viene definita dall'art. 4 del GDPR come qualsiasi forma di trattamento automatizzato di dati «effettuato per valutare aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

La *ratio* di tali previsioni può esser ricondotta alla libertà di autodeterminazione delle persone[19], concetto che negli ultimi tempi, per via dell'incessante diffondersi di nuove tecnologie e delle relazioni che si istaurano tra queste ultime e le persone, è andato ad arricchirsi di nuovi significati. Se tradizionalmente esso poteva esser concepito nella

---

[16] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 34. Per l'Autore «si può dire che oggi la sequenza quantitativamente più rilevante è quella "persona-informazione-circolazione-controllo", e non più soltanto "persona-informazione-segretezza", intorno alla quale è stata costruita la nozione classica di privacy. Il titolare del diritto alla privacy può esigere forme di "circolazione controllata", e non solo interrompere il flusso delle informazioni che lo riguardano». Il Gruppo di lavoro Articolo 29 lega la libertà del consenso alla possibilità di avere il controllo dei dati personali, sostenendo che «Se ottenuto nel pieno rispetto del regolamento, il consenso è uno strumento che fornisce all'interessato il controllo sul trattamento dei dati personali che lo riguardano», Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, 3.

[17] Per maggiori approfondimenti, Gruppo di lavoro Articolo 29, *Linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679*, 11 aprile 2018, 6.

[18] Art. 13, par. 2, lett. f, e dell'art. 14, par. 2, lett. g, del GDPR. In forza del considerando 63 ogni interessato deve poter ottenere dal titolare del trattamento informazioni in particolare in relazione «alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento».

[19] S. Mangiameli, *Autodeterminazione: diritto di spessore costituzionale?*, in C. Navarini (a cura di), *Autonomia e autodeterminazione - Profili etici, bioetici e giuridici*, Roma, 2011, l'autore afferma che «la Costituzione non parla di autodeterminazione in alcuna delle sue disposizioni, e ciò nonostante che la nozione di persona, nelle sue diverse aggettivazione (personale, personalità), sia richiamata 21 volte, quella di uomo (o umano) ben 9 volte, in alcuni casi in reciproca combinazione (nell'art. 3, comma 2, e nell'art. 32, comma 2, Cost.) e la dignità è richiamata due volte (nell'art. 3, comma 1, come dignità sociale, e nell'art. 41, comma 2, come dignità umana)».

prospettiva dell'esercizio di un diritto, sulla base di un rafforzato onere informazionale in capo al titolare, finalizzato a garantire la liceità del trattamento dei dati personali, oggi l'autodeterminazione deve essere intesa come consapevolezza del condizionamento proveniente dall'altrui trattamento dati, e quindi come limite ai diritti e alle libertà degli interessati[20].

Quella stessa libertà che poi sostanzia la principale eccezione al divieto di esser sottoposto a una decisione basata unicamente sul trattamento automatizzato, vale a dire il consenso dell'interessato (art. 22, par. 2, lett. c) del GDPR). Si rileva come in precedenza la deroga del consenso esplicito dell'interessato non era prevista dall'abrogato art. 15 della direttiva 95/46/CE riguardante le «decisioni individuali automatizzate» e il suo inserimento nel GDPR deve ricondursi al ruolo centrale che viene attribuito al consenso nel modello di protezione dei dati dell'Unione europea: il consenso non solo rappresenta una delle basi giuridiche per assicurare la legittimità del trattamento dei dati personali (art. 6 GDPR) ma esprime il momento di libertà in cui la persona si assoggetta a un meccanismo decisionale automatizzato.

Resta però il dubbio che il consenso , quale costrutto giuridico, sia adeguato ad assicurare una protezione efficace contro i moderni processi decisionali automatizzati, considerato il rischio per l'interessato di raggiungere quel grado di consapevolezza indispensabile per esercitare un effettivo controllo sui propri dati. E ciò, per una serie di ragioni.

Nel campo della profilazione, settore applicativo in cui è più diffuso l'uso di sistemi decisionali automatizzati, spesso le conseguenze del processo medesimo sono invisibili all'interessato, nel senso che, comunicatagli l'esistenza del processo stesso, come prescritto dall'art. 13, co. 2, lett. f), l'elaborazione dei dati porta alla creazione di dati personali "nuovi", cioè dati inferenziali, la cui caratteristica è nel non esser forniti direttamente dagli interessati ma esser da essi derivati o desunti osservandone il comportamento. E anche partendo da dati qualificati anonimi o, comunque, non personali è possibile ricavare dati personali[21]. Rispetto a tali dati derivati non può esservi alcuna consapevolezza da parte dell'interessato[22] e, per conseguenza, nessuna forma di controllo da parte sua. La preoccupazione principale deriva dal rapporto di tali dati inferenziali rispetto allo sviluppo di nuove tecnologie, poiché più accelera il processo trasformazione digitale più aumenterà la produzione di dati inferenziali rispetto a quelli coperti dal consenso.

Connesso al fenomeno di dati inferenziali v'è che la trasparenza decisionale è solitamente concepita come trasparenza *ex ante*, nel senso che il titolare del trattamento

[20] M.S. Esposito, Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali, in Diritto dell'Informazione e dell'Informatica, 2019, 1071, sostiene che il «crescente ricorso ai dati ed alla loro elaborazione mediante algoritmi a fini decisionali può tuttavia condurre a conseguenze negative per i diritti e le libertà dei soggetti coinvolti, incidendo sulla libertà di autodeterminazione e sul diritto al rispetto della dignità umana ai medesimi riconosciuti».

[21] Al riguardo N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law, in Law, Innovation and Technology, 10(1), 2018, 40 ss.*

[22] Sull'argomento si veda C.B. Parker, *New Stanford research finds computers are better judges of personality than friends and family*, in *news.stanford.edu,* 12 gennaio 2015. La nuova ricerca di Stanford rileva che i computer giudicano meglio la personalità di amici e familiari.

informa in anticipo l'interessato che utilizzerà i suoi dati per un processo decisionale automatizzato. La mancanza di un'attività di *reporting*, che realizzerebbe una trasparenza post trattamento, conduce alla mancanza di consapevolezza circa le conseguenze effettive del trattamento automatizzato che, in alcuni casi, nemmeno il titolare era in grado di aspettarsi.

A ciò si aggiunga che le persone hanno gradi diversi di comprensione e nell'ambito delle nuove tecnologie è ancor più difficile esercitare l'arte del comprendere, trattandosi spesso di esperienze inedite per l'uomo e soprattutto in continua evoluzione[23]. Per alcune persone potrebbe essere difficile comprendere le logiche utilizzate nei processi decisionali automatizzati, peraltro sempre più complesse ed oscure[24]. Ciò determina l'inadeguatezza dell'adozione, da parte del titolare del trattamento, di un unico livello di trasparenza che possa raggiungere l'obiettivo della conoscenza e della consapevolezza indistintamente per tutti gli interessati.

Se ciò non bastasse, si consideri che spesso i processi automatizzati sono annidati all'interno delle cd *black box*, rispetto alle quali non si è sempre in grado di cogliere con esattezza quale sia il processo seguito dall'algoritmo per produrre il risultato finale. Un ulteriore freno alla conoscenza del processo interno deriva da esigenze di tutela della proprietà intellettuale, necessaria al fine di garantire la segretezza del know-how tecnico di un determinato sistema che verrebbe ingiustamente pregiudicata se l'algoritmo venisse reso accessibile, conoscibile e quindi divulgabile a chiunque.

Per tali ragioni non possiamo considerare *tout court* garantito il controllo dell'interessato sulla propria sfera informazionale e, di conseguenza, non possiamo considerare soddisfatti quei canoni di libertà al cui presidio è posto il principio di trasparenza.

Ma v'è di più. La carenza di un effettivo controllo sulla propria sfera informazionale si manifesta anche sotto altro aspetto, quella di un controllo senza partecipazione dell'interessato, di guisa da impedirgli di essere partecipe della individuazione della "parte disponibile" del proprio patrimonio informativo.

Al riguardo possiamo rilevare che le informative sempre più spesso sono dirette a tutelare il titolare del trattamento, piuttosto che l'interessato[25]. Quest'ultimo, al di là della difficoltà nel leggere e comprenderne il testo, è in una posizione debole non potendo negoziare nessun aspetto del trattamento, né di quali dati personali disporre né in che modalità. A rigori, più che di consenso sarebbe corretto parlare di un assenso al trattamento, inteso quale atto con cui si aderisce, più o meno scientemente, a un'impostazione già perfezionata da altri. In tal senso depone anche l'art. 4, n. 11), del GDPR che

[23] Nelle linee guida del Gruppo di lavoro Articolo 29 si pone in evidenza che «le persone fisiche hanno gradi diversi di comprensione e per alcune potrebbe essere difficile comprendere le complesse tecniche coinvolte nella profilazione e nei processi decisionali automatizzati»: *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018, 10.

[24] La criticità deriva non soltanto dalla diffusione di cd *black box* quanto dalla scarsa diffusione nella società di competenze digitali, settore in cui l'Italia è ancora in una posizione di svantaggio rispetto agli altri paesi avanzati, stando ai risultati del Rapporto Annuale 2020 dell'Istituto Nazionale di Statistica (*Rapporto annuale 2020. La situazione del Paese,* Istat, 3 luglio 2020).

[25] Pure se dettata nell'ambito della responsabilità medica in tema di cure è rilevante, per il suo contenuto assiologico che può esser esteso alla presente indagine, l'osservazione della Cass. Civ., sez. III, 9 febbraio 2010, n. 2847, p.to 3.4, secondo cui non è il consenso ad essere informato ma è l'interessato a dovere essere informato, cioè capace di aver compreso ciò a cui ha dato l'assenso.

definisce il consenso come una manifestazione di volontà libera, specifica, informata e inequivocabile con cui l'interessato «manifesta il proprio assenso» al trattamento deciso - in tutto e per tutto - dal titolare del trattamento: l'unico spazio di decisione che gli residua è rappresentato dalla scelta di non aderire. Uno scenario che non appartiene al paradigma del consenso, caratterizzato sul piano generale del diritto dall'incontro delle volontà di due o più soggetti che si contrappongono da posizioni formali analoghe e giungono a una composizione di interessi. Sul piano più settoriale della tutela dei dati personali, tale paradigma dovrebbe tradursi in un processo che riproduca un dialogo tra titolare e interessato, attraverso cui entrambi possano giungere, grazie all'esercizio di poteri omogenei, alla composizione dei reciproci bisogni.

Dunque, il fenomeno si caratterizza non soltanto per la difficoltà di raggiungere quel grado di consapevolezza indispensabile per esercitare un effettivo controllo sulla propria sfera informazionale, che potremmo definire asimmetria informativa, ma per l'impossibilità dell'interessato di partecipare alla individuazione della "parte disponibile" del patrimonio informativo, che caratterizza una tipica situazione di asimmetria di poteri.

Tali condizioni, non solo portano a compromettere il controllo dell'interessato sulla propria sfera informazionale ma, correlato ad un indiscriminato utilizzo degli stessi da parte di terzi, determinano una ricaduta sul livello di libertà di cui una persona può beneficiare[26], ciò in quanto il controllo sul proprio patrimonio informativo è un mezzo per assicurare all'individuo una protezione a tutela della «persona nella sua interezza»[27].

In effetti, con l'ingresso dell'individuo nell'economia digitale, caratterizzata da una rapidità dell'evoluzione tecnologica e dalla globalizzazione, aumentano significativamente la condivisione e la raccolta di dati personali. Ed ecco che il regolamento, nella prospettiva di assicurare l'effettività delle libertà classiche dell'individuo nel contesto dello sviluppo dell'economia digitale in tutto il mercato interno, enfatizza la stretta alleanza esistente tra la protezione dei dati e gli altri diritti fondamentali, incoraggiando la visione della *data protection* come ausilio delle libertà classiche[28]. In questo senso, la protezione dei dati si colloca a supporto degli altri diritti[29] e, grazie a questi, alla base

[26] Nell'ambito della 41st International Conference of Data Protection and Privacy Commissioners tenutasi a Tirana dal 21 al 24 ottobre 2019, è stata adottata la *International resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights*, per la quale «*the right to privacy as a fundamental right and its role in both informing and serving as a foundation to other inalienable rights*» e si rileva che «*privacy is a precondition for citizens' other freedoms as well as a keystone right for democracy and personal and social development*». Il considerando 4 del regolamento (UE) 2016/679 chiarisce che «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma […] va contemperato con altri diritti fondamentali».

[27] Cfr. C. Colapietro - A. Moretti, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali,* in *BioLaw Journal – Rivista di BioDiritto*, 3, 2020, 379.

[28] Il diritto dell'interessato al controllo delle proprie informazioni è tradizionalmente ricondotto alla libertà e segretezza della corrispondenza e di ogni altro mezzo di comunicazione, espressamente qualificate dall'art. 15 della Costituzione come diritto inviolabile, ed esso attiene, a voler usare la parola della Consulta del 91, «al nucleo essenziale dei valori di personalità» senza i quali la persona «non può esistere e svilupparsi in armonia con i postulati della dignità umana» (Corte Cost., sent. 366/1991).

[29] C. Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy,* Napoli, 2018, 34, secondo cui la privacy «assume il carattere di "garanzia presupposto" dell'esercizio di altri diritti fondamentali, al fine

dello sviluppo e della realizzazione personale[30].
Si comprende allora come un affievolimento del principio di trasparenza, che dovrebbe assicurare quel grado irrinunciabile di autonomia e di libertà di autodeterminazione correlate al proprio patrimonio informativo, si traduce in un indebolimento di una garanzia posta a presidio di tutte le libertà tradizionali[31].

3. Il principio di non esclusività della decisione automatizzata

Corollario del principio di trasparenza è il principio di non esclusività della decisione automatizzata, sancito nell'art. 22 del GDPR, secondo cui «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[32].
Si tratterebbe di un divieto rivolto al titolare del trattamento, nell'ottica della tutela *by default* sancita dal GDPR, senza la necessità che per la sua applicazione l'interessato sia onerato di un qualche comportamento. Almeno sul piano teorico.
Tuttavia, già nella sua formulazione, il principio porta con sé due condizioni "limitanti" che lo costringono a recedere quando: il trattamento automatizzato è accompagnato da un intervento umano; la decisione che ne scaturisce non incide in modo significativo sulla persona. Dunque, non siamo in presenza di un principio di carattere assoluto e l'atteggiarsi in concreto delle sue eccezioni consente di indugiare sulla sua effettiva efficacia applicativa.
Quanto al primo aspetto, quello dell'intervento umano, non è dato intendere come esso possa esser misurato per poterlo comparare all'altro elemento del trattamento automatizzato, al fine di stabilire in quale misura l'uno sia prevalente sull'altro e se, in definitiva, la decisione possa esser considerata lecita, cioè non basata «unicamente» sul trattamento automatizzato.
Senza considerare le difficoltà di valutare quelle ipotesi in cui l'intervento umano assu-

di rendere possibile lo sviluppo della persona, l'esplicazione reale ed effettiva delle sue libertà».

30 S. Wachter, *Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights*, 2017, 19-21, secondo cui la privacy è la base per lo sviluppo e la realizzazione personale e «*Notwithstanding that other human rights play an important role in our society, it is privacy that is needed to fully exercise many of them*».

31 Sul punto si rinvia a F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, I, Torino, 2016, 9-10, il quale afferma che «nella società digitale e delle comunicazioni elettroniche il diritto fondamentale alla protezione dei dati diventa anche il presidio irrinunciabile di tutte le libertà classiche delle nostre Costituzioni» e che «rinunciare alla protezione dei dati personali da ogni indebita ingerenza, significa rischiare di vanificare ogni forma di libertà e mettere in pericolo tutti i diritti fondamentali»; nonché a L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, 16, che evidenzia come la protezione dei dati personali concorra a realizzare una piena valorizzazione e garanzia sia della dignità umana sia della società democratica: in particolare, «il diritto fondamentale alla protezione dei dati diviene anche presidio irrinunciabile di tutte le altre libertà classiche costituzionalmente garantite, cioè funzionale al loro esercizio e, in ultima analisi, funzionale alla difesa della nostra stessa società democratica».

32 Art. 22, par. 1, del GDPR.

ma le connotazioni di un elemento marginale, se non addirittura fittizio.

Anche l'aspetto incidenza del trattamento sulla persona non è di facile valutazione. Anzitutto, la stessa formulazione del principio di non esclusività non esprime criteri oggettivi attraverso cui valutare quando un trattamento automatizzato sia destinato ad incidere «significativamente» sulla persona dell'interessato[33]. E, in mancanza, si è costretti a ricorrere a criteri soggettivi, cioè ad affidare siffatta valutazione al titolare del trattamento. Ma, la sua valutazione sarà comprensibilmente rivolta ad uno standard di tutela in cui non tutte le persone potrebbero identificarsi, per via dei loro differenti gradi di vulnerabilità e per via del fatto che il concetto di dignità della persona non è comprimibile in standard omogenei, per cui l'interessato si troverebbe costretto a dover eccepire le proprie ragioni opponendosi alla decisione automatizzata. E ciò potrà avvenire soltanto *ex post*, a decisione assunta e sacrificio ormai prodotto.

Per di più, ci sono casi in cui la incisività della decisione automatizzata è celata agli occhi dell'interessato per cui viene a mancare anche quell'ultimo baluardo di garanzia rappresentato dall'autodifesa. Si pensi alla pubblicità mirata che, apparentemente non incisiva dal momento che può essere ignorata, influenza il punto di vista e la libertà di scelta degli utenti. Attraverso messaggi inviati ai singoli individui, e personalizzati grazie a sofisticati modelli predittivi computazionali di *microtargeting*[34], di cui la maggior parte degli utenti ignora l'esistenza e il funzionamento, si creano delle vere e proprie *filter bubbles*[35], ovvero delle bolle in cui l'utente viene rinchiuso ricevendo soltanto informazioni conformi alle proprie opinioni e pregiudizi[36].

Ecco perché sul piano applicativo l'efficacia di tale principio è discutibile, a prescindere dai casi di aggiramento voluto del principio di non esclusività[37]. Per tali ragioni si è fatta

---

[33] Un'indicazione viene fornita nei considerando (71) laddove si cita a titolo esemplificativo «il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani». Anche il Gruppo di lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 24, è intervenuto sull'argomento, enucleando quali situazioni significative quelle che influenzano le condizioni finanziarie di una persona (ammissibilità al credito), ovvero l'accesso ai servizi sanitari, che negano un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio; decisioni che influenzano l'accesso di una persona all'istruzione, ad esempio le ammissioni universitarie.

[34] Il *microtargeting* è una tecnica che analizza i dati personali per prevedere gli interessi di un pubblico specifico: una pratica che costituisce il modello di business fondamentale di diverse grandi piattaforme di social media e che è diventata nota al grande pubblico con lo scandalo Cambridge Analytica del 2016.

[35] E. Pariser, *The filter bubble: What the Internet is hiding from you,* London, 2011, e più di recente K. Shaffer, *Data versus Democracy: How Big Data Algorithms Shape Opinions and Alter the Course of History, Apress*, Colorado, 2019; E. Longo, *Dai big data alle «bolle filtro»: nuovi rischi per i sistemi democratici,* in *Percorsi costituzionali*, 2, 2019, 29 ss.; R. Montaldo, L*e dinamiche della rappresentanza tra nuove tecnologie, populismo, e riforme costituzionali*, in *Quaderni costituzionali,* 4, 2019, 790 ss.

[36] Sulla questione si è pronunciato anche il garante della protezione dei dati dell'UE (GEPD) sulle proposte della Commissione europea per il *Digital Services Act* (DSA) e il *Digital Markets Act* (DMA), per il quale «Data la moltitudine di rischi associati alla pubblicità mirata online, il GEPD esorta i colegislatori a prendere in considerazione norme aggiuntive che vadano oltre la trasparenza».

[37] La Commissione europea, nella *Communication "Building Trust in Human-Centric Artificial Intelligence*", COM(2019)168 final, 8 aprile 2019, 4, al fine di circoscrivere uno spazio di intervento dell'uomo ha individuato almeno tre diverse intensità: "*Human-in-the-loop*" l'intervento umano in ogni ciclo decisionale del sistema; "*Human-on-the-loop*" l'intervento umano a monte del design del sistema e durante il suo funzionamento; "*Human-in-command*" l'intervento capace di decidere come e quando usare l'IA in una situazione particolare. V. anche D. Amoroso – G. Tamburrini, *I sistemi robotici ad autonomia crescente tra etica*

strada una interpretazione sostanziale del principio di non esclusività, nel senso di considerare soddisfatto il principio laddove l'intervento dell'essere umano non è solamente formale ma esprime una vera e propria valutazione attiva[38]. Nello stesso senso si è mosso anche il Parlamento Europeo che nella Risoluzione sugli aspetti etici dell'IA (20 ottobre 2020) evidenziano che nei casi in cui siano in gioco le libertà fondamentali gli Stati membri dovrebbero ricorrere a tali tecnologie soltanto «quando sono possibili o sistematici un intervento e una verifica sostanziali da parte dell'uomo». Analoga stretta si rintraccia nella giurisprudenza più recente del TAR Lazio, il quale ha relegato l'uso di decisione completamente automatizzare nell'ambito dell'istruttoria amministrativa ad un «ruolo strumentale e meramente ausiliario in seno al procedimento amministrativo e giammai dominante o surrogatorio dell'attività dell'uomo»[39].

La consapevolezza che si tratta di una previsione di difficile interpretazione ha reso l'interprete consapevole che nella pratica possano rinvenirsi situazioni di non facile qualificazione. Per tale ragione il Gruppo di lavoro Articolo 29 ha identificato almeno due elementi da considerarsi rappresentativi di un intervento umano: vale a dire che il coinvolgimento umano sia opera di «una persona che dispone dell'autorità e della competenza per modificare la decisione» e che «tale persona dovrebbe prendere in considerazione tutti i dati pertinenti»[40]. Resta, tuttavia, il dubbio di come una persona, per quanto autorevole e competente, possa «prendere in considerazione tutti i dati pertinenti» che soltanto sofisticati sistemi di IA sono in grado di analizzare ed elaborare.

Sebbene venga prestata notevole attenzione affinché i trattamenti automatizzati non siano affidati soltanto all'algoritmo ma contemplino anche un effettivo coinvolgimento umano e nonostante gli sforzi interpretativi a ciò dedicati, l'effettività del principio stesso resta nel dubbio, complice anche la «travolgente forza pratica dell'algoritmo»[41], quella capacità dell'algoritmo di indurre la persona coinvolta ad affidarsi e a delegare per intero l'attività valutativa e decisionale assegnatale.

Per arginare il rischio di vanificare l'effettività del principio, il Parlamento Europeo si è mosso nella direzione di ritagliare alle decisioni automatizzate un ruolo di supporto o

e diritto: quale ruolo per il controllo umano?, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 33 ss., 51.

[38] L.A. Bygrave, *Automated Profiling: Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, in *Computer Law & Security Review*, 17, 2001, 20; G. Malgieri - G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law,* 7(4), 2017, 251.

[39] Vedi Tar Lazio, sez. III-bis, 10 settembre 2018, n. 9227, in cui si stabilisce che «le procedure informatiche, finanche ove pervengano al loro maggior grado di precisione e addirittura alla perfezione, non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere». Sul rapporto tra PA e IA, D.U. Galetta - J.G. Corvalán, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019. Sia consentito infine richiamare G. Fasano, *L'intelligenza artificiale nella cura dell'interesse generale*, in *Giornale di Diritto Amministrativo,* 6, 2020, 715 ss.

[40] Gruppo di lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, cit., 23.

[41] A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 81, che puntualizza come tale forza non dipenda da ragioni di valore scientifico, di accuratezza predittiva o di affidabilità tecnica dell'automatismo, ma – appunto – da mera convenienza pratica.

strumentale alla decisione presa dall'agente umano, almeno in ambiti particolarmente delicati come quello medico. In effetti, nel campo dell'assistenza sanitaria l'intelligenza artificiale svolge un ruolo sempre più cruciale, si pensi agli algoritmi di supporto alla diagnosi, la chirurgia robotica, le protesi intelligenti e i robot sociali per l'assistenza agli anziani la cui diffusione potrebbe inficiare la parità di trattamento dei pazienti in termini di accesso alle cure e alterare il rapporto tra paziente e medico. Nella Risoluzione del 20 gennaio 2021 il Parlamento ha voluto stigmatizzare la responsabilità del professionista evidenziando come egli deve aver sempre presente la possibilità di discostarsi dalla soluzione proposta dall'IA[42]. La questione viene così affrontata dal punto di vista della responsabilità, quasi a monito di un utilizzo spesso ossequioso e conformativo alle risultanze del sistema automatizzato.

In esito a questa breve analisi, pare evidente che il principio di non esclusività, inestricabilmente connesso a quello della trasparenza, si presti ad esser poco efficace come garanzia dei diritti e libertà fondamentali, e non soltanto per via dei suoi connaturati limiti strutturali ma anche a causa della presenza di numerose cause derogatorie che ne indeboliscono la portata effettiva, prima tra tutte, l'eccezione del consenso.

4. Le eccezioni al principio di non esclusività: il consenso

Come anticipato, il GDPR prevede delle eccezioni al divieto di decisioni completamente automatizzate, quali la loro necessità per la conclusione o l'esecuzione di un contratto, l'autorizzazione da parte del diritto dell'UE o dello Stato membro[43], oppure il consenso esplicito dell'interessato. La presenza di tali e tante eccezioni, molto frequenti nella pratica, rende il principio di non esclusività, di fatto, un principio debole.

Tra queste eccezioni il consenso del soggetto destinatario della decisione automatizzata presenta la principale criticità, imponendo di riflettere sulla sua efficacia di fronte alla forza di questi meccanismi[44].

Per un verso, occorre riconoscere che il principio del consenso, nell'ecosistema introdotto dal GDPR, rappresenta uno dei pilastri su cui si fonda l'intera disciplina europea sulla protezione dei dati: oltre ad esser annoverato quale prima condizione di liceità del trattamento (art. 6), viene rappresentato come momento di manifestazione di una «intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano» (considerando 32)[45].

[42] Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale, par 65. In tal senso si veda anche l'art. 11 della Loi n° 2021-1017 cit.

[43] I. Mendoza - L. A. Byg Rave, *The Right Not to be Subject to Automated Decisions Based on Profiling*, in T. Synodinou - P. Jougleux - C. Markou - T. Prastitou (eds.), *EU Internet Law. Regulation and Enforcement*, London, 2017, 95, osservano che la possibilità per la legislazione nazionale di legalizzare specifici trattamenti interamente automatizzati incide sull'obiettivo del regolamento (UE) 2016/679 di favorire una maggiore armonizzazione della disciplina tra gli Stati membri.

[44] Si rileva come la deroga del consenso esplicito dell'interessato, riconosciuta all'art. 22, par. 2, lett. c) del regolamento (UE) 2016/679, non era prevista in precedenza all'interno dell'abrogato art. 15 della direttiva 95/46/CE riguardante le "Decisioni individuali automatizzate".

[45] La centralità del ruolo del consenso ha tradizionalmente ispirato gli stessi padri della privacy, S. D. Warren - L. Brandeis, *The Right to Privacy*, in *Harvard Law Review,* 4(5), 1890, 193 ss. Stefano Rodotà

Nell'ambito dei sistemi decisionali automatizzati, inoltre, il consenso dell'interessato acquisisce una differente e maggiore portata: il principio del trattamento trasparente comporta una dilatazione degli oneri informativi, per cui non è sufficiente che l'interessato riceva informazioni sull'esistenza del trattamento e sulle sue finalità, egli deve esser destinatario di «informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato» (art. 13, par 2, lett. f) e art. 14, par 2, lett. g)). Ecco che la trasparenza, e dunque il consenso che sulla base di essa viene espresso, involve aspetti inediti ampliando la portata della manifestazione di volontà, in vista della realizzazione piena dell'autodeterminazione informativa. Tuttavia, tale scopo rischia di cedere a fronte di meccanismi altamente sofisticati in cui le decisioni automatizzate non lasciano comprendere la loro rilevanza in termini di compressione delle libertà fondamentali.

Ciò accade per una serie di ragioni. *In primis*, la finalità del trattamento e l'uso che potenzialmente potrebbe esser fatto dei dati rischiano di non essere determinabili al momento iniziale di espressione del consenso alla raccolta, o comunque a priori, vincolando il consenso ad una prospettazione infedele delle finalità e dell'utilizzo dei dati. In tale condizione non potrebbe esprimersi un consenso consapevole. Si pensi ai sistemi di machine learning, i quali generano essi stesi nuovi dati, rispetto ai quali non può esservi spazio per alcun consenso, visto che al momento della raccolta, momento in cui va espresso un consenso consapevole, quei dati non esistono.

La valutazione circa «l'importanza e le conseguenze» del trattamento automatizzato non può esser frutto dell'analisi solitaria effettuata da una sola parte e, peraltro, in chiave meramente prospettica. Il principio dell'autodeterminazione è declinato, ancora una volta, come assenso ad un'attività valutativa - foriera della decisione finale - rimessa ad esclusivo appannaggio del titolare del trattamento dati. Ma, senza la partecipazione attiva dell'interessato, con la sua unicità, con le sue vulnerabilità, con la sua identità dignitaria[46], non può giungersi ad una prospettazione verosimile circa l'importanza e le conseguenze del trattamento automatizzato. Sulla base della quale, questa volta sì, si può esprimere un consenso informato.

La stessa complessità dei sistemi di IA non è d'aiuto in termini di esercizio dell'autodeterminazione, considerata la difficoltà di comprendere le conseguenze di un trattamento quando i dati sono destinati ad essere processati con sistemi di IA di cui si ignorano le logiche di funzionamento interno. Si parla di *black box* per indicare quei processi automatizzati che impediscono di comprendere il funzionamento, rendendo le decisioni imperscrutabili e indecifrabili – non solo - per il destinatario. In ragione di ciò, l'interessato finisce per ricevere informazioni generiche sulle modalità di elaborazione dei propri dati ovvero indicazioni talmente tecniche da risultare incomprensibili. E la mancata comprensione si traduce in un mancato controllo su tali sistemi.

La complessità si manifesta anche per effetto dei livelli di sofisticatezza raggiunti da

considerava il consenso la massima espressione del controllo da parte dell'individuo sulle proprie informazioni, S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione,* Bari, 2004.

[46] A. Oddenino, *Decisioni algoritmiche e prospettive internazionali di valorizzazione dell'intervento umano*, in *DPCE online*, 2020, 1, 213, il quale identifica «la dignità umana come elemento fondativo dello stesso concetto di privacy».

alcuni sistemi, si pensi alle tecniche di profilazione e di predizione che da dati apparentemente neutrali possono ricavare dati sensibili. Recenti studi hanno dimostrato come, grazie alle tecniche di correlazione statistica, analizzando i semplici *like* di Facebook è possibile desumere con una ragionevole certezza informazioni sulla personalità dei singoli individui[47], cioè a dire orientamento sessuale, politico e religioso.

In tali circostanze l'asimmetria informativa non è tanto un condizionamento nell'esercizio di un potere, quello sottostante il consenso, bensì un vero e proprio stato di soggezione in cui sono relegati gli interessati al trattamento dei dati[48].

A tentare di porre rimedi a tali criticità è intervenuto anche il Gruppo di lavoro Articolo 29[49] ma, ancora una volta, la soluzione è stata individuata attorno all'istituto del consenso onerando il titolare del trattamento, che voglia basare la profilazione sul consenso, di un obbligo specifico, quello di «dimostrare che gli interessati comprendono esattamente a cosa stanno acconsentendo».

Resta evidente la difficoltà operativa di tale misura, in primis, poiché non vi sono elementi oggettivi di misurazione del grado di consapevolezza e, inoltre, perché qualora il titolare non riesca a fornir prova della consapevolezza raggiunta dagli interessati le conseguenze nocive di un trattamento automatizzato rimarrebbero in piedi, riversandosi sulla parte debole del rapporto e determinando una lacuna nella tutela effettiva degli interessati. Consapevole di ciò, lo stesso Gruppo di lavoro rammenta che «il consenso non è sempre una base appropriata per il trattamento», con ciò riconoscendo i suoi limiti intrinseci sul piano delle tutele effettive.

La preoccupazione che il principio del consenso possa non bastare come tutela nell'ambito delle decisioni automatizzate è stata presente anche nel legislatore unionale. Per tale ragione viene ampliato il novero degli obblighi assegnati al titolare del trattamento. In effetti, la prescrizione unionale impone a questi l'adozione di «misure appropriate» ulteriori rispetto al consenso per tutelare i diritti, le libertà e i legittimi interessi dell'interessato qualora si proceda al trattamento automatizzato, specificando che il corredo minimo di tali garanzie sia costituito dal «diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione».

Tradurre tali «misure appropriate» sul piano concreto non è affatto scontato. A partire dalla garanzia circa l'intervento umano, che se dovesse esprimersi sempre e comunque non consentirebbe di raggiungere i vantaggi connessi all'automazione delle decisioni, e senza contare quei processi automatizzati che non consentono, per loro natura, di

---

47 M. Kosinski - D. Stillwell - T. Graepel, *Private traits and attributes are predictable from digital records of human behavior,* in *PNAS*, 110, 15, 2013, 5802 ss. Secondo questi studi condotti dall'Università di Cambridge, sono sufficienti meno di 70 *like* di Facebook per determinare il colore della pelle dell'utente (con il 95% di precisione), l'orientamento sessuale (con l'88% di precisione), l'afferenza al partito politico (con il 95% di precisione). Ma a partire da queste rilevazioni sarebbe possibile anche risalire al credo religioso, al consumo di alcolici, sigarette o droghe, sino alla circostanza che i genitori abbiano convissuto o meno fino a che l'interessato abbia raggiunto i 21 anni.

48 L. Mitrou, *Data Protection, Artificial Intelligence and Cognitive Services. Is the General Data Protection Regulation (GDPR) "Artificial Intelligence-Proof"?,* in *SSRN*, aprile 2019, 41.

49 Gruppo di lavoro Articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679,* cit., 14.

comprendere le logiche di funzionamento interno (*black box*)[50].

Nel settore della sanità pubblica, ad esempio, il presidio dell'intervento umano viene garantito attraverso una responsabilizzazione di *default* del medico. Questi, qualora faccia ricorso a sistemi di IA nello svolgimento delle proprie attività, viene considerato responsabile di qualsiasi decisione fondata su sistemi decisionali automatizzati, salva comunque la «possibilità di discostarsi dalla soluzione proposta dall'IA»[51]. Non potendo consentire l'intervento diretto dell'uomo nella elaborazione della decisione automatizzata, irrealizzabile in presenza di analisi e studio dei cd *big data*, la tutela dell'intervento umano viene realizzata imputando all'uomo la responsabilità della decisione automatizzata.

Lo stesso approccio viene utilizzato nel settore delle armi automatizzate prevedendo che «i sistemi basati sull'IA devono consentire alla leadership militare di assumere la piena responsabilità e rendicontabilità per ... azioni letali o distruttive su larga scala mediante tali sistemi»[52]. Pur non rilevando tali prescrizioni in tema di dati personali, ciò che rileva in questa sede è individuare la tendenza dei regolatori a realizzare la garanzia dell'intervento umano spostando l'asse sulla responsabilità della persona che utilizza siffatti sistemi decisionali, a causa della difficoltà concreta di consentire l'intervento umano nella elaborazione della decisione automatizzata[53].

Il rimedio della responsabilizzazione, però, lascia aperto il tema della democraticità di tali sistemi, soprattutto laddove i meccanismi di *machine learning* riducono, se non eliminano del tutto, la contendibilità delle loro decisioni, intesa come la «*lack of an obvious means to challenge them when they produce unexpected, damaging, unfair or discriminatory results*»[54].

La non facile formulazione della norma (art. 22) e la delicatezza del tema trattato ha originato anche un dibattito tra chi sostiene che il GDPR riconosce soltanto un diritto di accesso e informazione[55], seppur ampliato per effetto della maggior trasparenza

---

[50] Come riferito nella *Communication "Building Trust in Human-Centric Artificial Intelligence"*, COM(2019) 168 final, 8 aprile 2019, 4, "*Human-in-the-loop*" si riferisce all'intervento umano in ogni ciclo decisionale del sistema, che in certi casi può non essere desiderabile; "Human-on-the-loop" si riferisce alla possibilità che l'intervento umano avvenga durante il design del sistema e come monitoraggio durante il suo funzionamento; "*Human-in-command*" si riferisce invece alla possibilità di vigilare sull'attività complessiva del sistema di IA (compreso il più ampio impatto economico, sociale, etico e legale) e alla capacità di decidere come e quando usare il sistema in una situazione particolare. Sul punto riassuntivamente B. Mittelstadt - P. Allo - M. Taddeo - S. Wachter - L. Floridi, *The ethics of algorithms: Mapping the debate,* in *Big Data & Society,* 3, 2016, 1 ss.

[51] Risoluzione del parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale, par. 65.

[52] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)).

[53] L'attenzione verso l'intervento umano è particolarmente sentita in tema di sorveglianza umana tant'è che in tale ambito l'High-Level Expert Group on Al selezionato dalla Comunità europea, nelle *Ethics Guidelines for trusthworty AI,* par. 65, indica di predisporre «meccanismi di governance che consentano un approccio con intervento umano (*human in the loop*), con supervisione umana (*human on the loop*) o con controllo umano (*human in command*)»

[54] L. Edwards - M. Veale, *Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking For*, in *Duke Law and Tech Review*, 16, 2017, 18 ss. Sempre in tema di contestabilità della decisione algoritmica M. Hildebrandt, *The new imbroglio. Living with machine algorithms,* in L. Janssens (hg.), *The Art of Ethics in the Information Society,* Amsterdam, 2016, 55 ss.

[55] S. Wachter - B. Mittelstadt - L. Floridi, *Why a right to explanation of automated decision making does not exist*

richiesta in tali casi, e chi sostiene invece l'esistenza di un vero e proprio diritto alla spiegazione[56]. Questi ultimi attribuiscono natura vincolante al considerando 71 per il quale il trattamento automatizzato «dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione».

Al di là delle difficoltà ermeneutiche derivanti dal quadro formale, e in disparte il rischio che il consenso venga reso come un automatismo[57], perché spesso gli utenti non sono portati a leggere con attenzione l'informativa sul consenso per poi esprimere una «intenzione libera, specifica, informata» sul trattamento[58], nell'ambito delle decisioni automatizzate si palesa evidente la debolezza della costruzione giuridica del consenso. Proprio laddove il consenso abbisogna di elementi di rinforzo esogeni per poter mantenere la centralità del ruolo costruito dal regolatore europeo, attraverso l'adozione di «misure appropriate» complementari che possano raggiungere l'obiettivo della tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, esso finisce per restar solo a operare non come momento di consapevolezza nell'esercizio della libertà di autodeterminazione ma, piuttosto, quale rinuncia inconsapevole alla tutela dei propri diritti.

5. Conclusioni

La regolamentazione sulla trasparenza e sui processi decisionali automatizzati mostra come il legislatore europeo si sia mosso con le migliori intenzioni, ponendosi l'obiettivo della tutela dei dati personali quale strumento per tutelare la persona nella sua interezza. Tale strategia è basata sulla riduzione del dato personale a "bene", da destinare alla libera circolazione in un mercato digitale senza confini: l'interessato viene tutelato per esser parte fondamentale del mercato digitale, unitamente all'imprenditore, in un mercato inteso come luogo nel quale si realizza la persona grazie al bilanciamento degli interessi e dei valori coinvolti.

Ma, il dato-bene non è rappresentativo della realtà personale, è frutto di una rappresentazione ideologicamente orientata e predeterminata da progettisti e sviluppatori, mentre la riduzione *tout court* della persona ai suoi dati è orientata da una scelta di convenienza, di guisa che la costruzione giuridica del consenso, attorno al quale ruota il sistema di legalità della *data protection,* non sempre è garanzia di autodeterminazione individuale. Inoltre, attraverso l'immissione continua dei dati personali nel mondo digitale si acconsente a che lo sviluppo della stessa personalità dell'individuo avvenga lì, nel

in the general data protection regulation, in *International Data Privacy Law*, 7(2), 2017, 76 ss.

[56] A. D. Selbst - J. Powles, *Meaningful information and the right to explanation*, in *International Data Privacy Law*, 7, 2017, 233.

[57] M.L. Jones - E. Kaufman - E. Edenberg, *AI and the Ethics of Automating Consent*, in *IEEE Security & Privacy*, 16, 3, 2018, 64 ss.

[58] E. Carolan, *The continuing problems with online consent under the EU's emerging data protection principles*, in *Computer Law & Security Review,* 32(3), 2016, 462 ss.; M. Butterworth, *The ICO and artificial intelligence: The role of fairness in the GDPR framework*, in *Computer Law and Security Review*, 34, 2018, 262.

mondo snervato e artefatto del digitale, che poi ha la forza di riverberarsi nel mondo materico potendo determinare forti condizionamenti dei comportamenti: gli algoritmi non solo predicono le azioni ma le producono[59]. Nel processo di formazione di tale personalità assume fondamentale rilievo la scelta dei dati che le danno forma, scelta che non è affidata all'individuo bensì al "titolare del trattamento", colui che ne decide scopi e finalità[60].

A fronte di tale scenario occorre sviluppare una riflessione di sistema sul significato che deve assumere il principio di trasparenza, sempre più cruciale per soddisfare l'esigenza, ormai largamente condivisa, della *trustworthy AI*[61]. È necessario indugiare sui profili critici emergenti nonché su possibili soluzioni tecnico-giuridiche, in una prospettiva *de jure condendo*. Non che questo tipo di riflessione possa dirsi agevole da percorrere: la sfida più difficile per i regolatori consiste nel riuscire a sviluppare modelli normativi dinamici, che possano metter le regole del sistema al riparo da un'obsolescenza scaturente da un incalzante processo tecnologico.

E così, il principio di trasparenza deve esser ancorato alle vulnerabilità delle singole persone, ciascuna con un proprio portato di competenze e conoscenze che deve condizionare l'assolvimento degli obblighi informativi da parte del titolare. Non una, ma tante trasparenze quanti sono i profili di rischio degli interessati, assecondando le esigenze di tutela delle vulnerabilità dei singoli, perché la vulnerabilità delle persone è l'unica chiave per mostrar loro quella lealtà fondamentale che può fondare una *trustworthy AI*.

Ancora, attraverso una trasparenza post trattamento, che indichi le conseguenze effettive del trattamento automatizzato, la trasparenza decisionale non sarebbe più un punto statico per l'ancoraggio del consenso ma consentirebbe all'individuo di poter costruire nel tempo, arricchendolo con la conoscenza ad esempio dei dati inferenziali, il proprio punto di vista, le proprie scelte in piena libertà.

La persona deve esser partecipe non tanto della logica imperscrutabile di sofisticati meccanismi che governano i sistemi decisionali automatizzati, quanto dello scopo dell'intero processo di automazione e delle sue conseguenze, prodotte sugli individui, sulla società e sull'ambiente.

Ecco che, messa in chiaro questa base informativa, si potrà costruire un consenso non soltanto libero e informato ma, soprattutto, partecipato, reintegrando l'individuo nel potere di definire quella parte del proprio patrimonio informativo da rendere disponibile nel mondo digitale, così da restituire alla persona umana la decisione sugli aspetti

[59] Ciò varrebbe a confermare l'intuizione di Stefano Rodotà, il quale sosteneva una accezione del diritto alla privacy più estesa che nel passato, di pretesa da parte dell'interessato di stabilire in piena autonomia le «*modalità di costruzione della propria sfera privata*» *S. Rodotà, Tecnologie e diritti, cit., 1995, 122.*

[60] Sul tema dei poteri privati che potrebbero incidere sullo sviluppo della personalità umana, segnatamente della libertà di espressione, si veda M. Bassini, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione, in questa Rivista, 2, 2021, 76. L'autore parla «claim normativo» e muove dalla constatazione che la sospensione della possibilità di accesso ai social network, sulla scorta di regole di ingaggio predisposte unilateralmente dal regolatore privato, può determinare «un vero e proprio impedimento, a seconda dei casi» nell'esercizio della libertà di espressione.*

[61] La strategia per trasformare l'Europa in un hub globale ruota attorno al fulcro della fiducia, vale a dire che per consentire lo sviluppo dei sistemi di intelligenza artificiale (IA) è indispensabile lavorare sulla loro affidabilità. V. l'High-Level Expert Group on Al, *Ethics Guidelines for trustworthy AI,* cit.

più significativi legati alla propria intima vita.