mediaLAWS

Rivista di diritto dei media
2/2022 settembre

SEDE
CONTACTS

ACCMS Studio Legale
Via Podgora 13 – 20122 Milano

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

e-mail: submissions@medialaws.eu

ANNO 2022 - CODICE ISSN 2532-9146
Impaginazione a cura di Chiara Pavesi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Indice
Index

Saggi

Note a sentenza

Cronache

Recensioni

Indice
Index

Essays

Case notes

Comments

Book reviews

Sono stati sottoposti a referaggio a doppio cieco i contributi di: Maria Romana Allegri, Andrea Buratti, Ylenia Maria Citino, Caterina Di Costanzo, Federica Giovanella, Angela Mendola, Daniela Messina, Cristina Evanghelia Papadimitriu, Alberto Randazzo.
Su determinazione della direzione, sono inoltre stati sottoposti a referaggio anonimo i contributi di: Filippo Donati, Simone Lonati e Vincenzo Zeno Zencovich.

Cronache

Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato

Maria Grazia Peluso

Sommario

1. Introduzione

La diffusione di applicazioni di Intelligenza Artificiale, in grado di processare ingenti moli di dati, è oggi al centro di un intenso dibattito in merito sia al regime di responsabilità civile applicabile, sia alla compatibilità o meno di queste tecnologie con la normativa sulla *data protection*.

L'esigenza di una maggiore tutela dei diritti degli utilizzatori è particolarmente sentita per tutte quelle applicazioni che vedono l'utilizzo di algoritmi complessi e di cui, spesso, il funzionamento diviene di difficile comprensibilità anche per gli stessi programmatori ("*black box*").

Attenzione meritano quei sistemi che operano una profilazione delle persone, aventi la capacità di inferire dati personali anche da *dataset* di diversa natura, i cui esiti possono rivelarsi discriminatori. Del pari, preoccupazione destano i sistemi destinati a operare decisioni automatizzate. Si pensi a quegli algoritmi utilizzati per la concessione di beni o servizi pubblici o per decidere la concessione di un mutuo; all'utilizzo fatto nelle Corti americane del software COMPAS, o, anche, all'utilizzo che ne può essere fatto in ambito medico.

Sempre più numerosi sono gli ambiti in cui queste tecnologie vengono impiegate, arrivando a parlare di una vera e propria pervasività delle applicazioni Intelligenza Artificiale in tutti i settori socio-economici.

Le prospettive di crescita economica e sviluppo anche sociale che la tecnologia *data driven* veicola hanno permesso una significativa spinta nella diffusione e nell'utilizzo di dette applicazioni; alle promesse di crescita si accompagnano tuttavia anche rischi di esternalità negative e discriminazioni che dovrebbero essere attentamente ponderati.

Se dunque la tecnologia può portare grandi vantaggi, e il progresso appare difficile da arrestare, pare opportuna un'attenta analisi in merito alla tenuta degli istituti attualmente vigenti, in una prospettiva che permetta di individuarne non solamente

le criticità, ma anche i punti di forza, per una regolazione efficiente ed efficace del fenomeno digitale.

2. Quale ruolo giocano i *data* nelle applicazioni di Intelligenza Artificiale

Prima di procedere è necessario chiarire cosa debba intendersi con il termine Intelligenza Artificiale. Come è noto, difatti, la comunità scientifica non appare concorde nella scelta di una definizione che sia in grado di ricomprendere le diverse aree di studio che interessano la materia[1].

Nella consapevolezza che una nozione universalmente condivisa di Intelligenza Artificiale ad oggi non esiste[2], una definizione potrebbe essere quella secondo cui l'AI è una disciplina che studia le modalità di addestramento di algoritmi che siano in grado, secondo diversi gradi di autonomia, di raggiungere un dato obiettivo mediante la ge-

[1] Diversi sono stati i tentativi definitori, non solamente giudici, tra i quali di particolare pregio si mostrano le definizioni elaborate da Russell e Norvig, tra i maggiori studiosi della materia, e dall'High Level Expert Group on AI, che da ultimo ha elaborato una definizione piuttosto articolata. Secondo Russell e Norvig «l'IA è la ricerca del miglior programma agente per una specifica architettura» (S. Russell-P. Norvig, *Intelligenza Artificiale un approccio moderno*, Milano, 2005, vol. 1, 588 ss.). Questa definizione merita una particolare menzione, sebbene appaia particolarmente ampia, questa mostra di cogliere l'essenza della disciplina, prestandosi al contempo a una interpretazione capace di adattarsi ai differenti angoli visuali che caratterizzano un campo di indagine così ampio. L'High-Level Expert Group on AI, abbracciando una concezione volta a sottolineare le razionalità dei sistemi agenti e discostandosi in parte da quanto affermato dalla Commissione Europea, ha recentemente elaborato una definizione avente il dichiarato scopo di rendere maggiormente compresibile l'oggetto della materia. Il Gruppo di Esperti ha così precisato che per AI debbano intendersi: «*software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)*». High Level Expert Group, *Definition of AI. Main capabilities and disciplines*, in *ec.europa.eu*, 8 aprile 2019.

La Commissione europea, nella raccomandazione emanata nel 2018, aveva già elaborato una prima definizione di Intelligenza Artificiale, da cui emerge il riferimento a capacità delle macchine tali da poterle considerare "intelligenti": «*Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)*». Comunicazione della Commissione, *Un'intelligenza artificiale per l'Europa*, COM (2018) 237 final.

[2] Ad oggi l'elemento cardine su cui paiono ruotare le definizioni di Intelligenza Artificiale è la capacità delle macchine di raggiungere un risultato. Cfr. sul punto G. Romano, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in G. Alpa (a cura di), *Diritto e Intelligenza Artificiale*, Pisa, 2020, 108. Secondo l'Autore questa tipologia di definizioni comporterebbe alcune criticità dal punto di vista giuridico, dal momento che pare esservi stata unicamente una sostituzione del termine "intelligenza" con il termine "obiettivo"; portando così l'attenzione degli interpreti su aspetti filosofici di poco ausilio nel campo legislativo.

stione ed elaborazione di dati, indipendentemente dalla implementazione dell'algoritmo in una macchina[3].

Ciò che accomuna le diverse tecniche di Intelligenza Artificiale è difatti proprio la capacità di elaborazione dei dati a queste sottoposte. È noto come non solamente l'aumento della potenza di calcolo degli elaboratori elettronici, ma anche la disponibilità di una grande quantità di *data* ha permesso la diffusione sempre più pervasiva delle applicazioni di AI, e in particolare oggi quelle fondate su tecniche di *machine learning*, tra cui va annoverato anche il *deep learning*. Ne discende evidentemente l'esigenza di un approccio alla materia che sia attento anche alla regolazione dei *data*, dovendosi necessariamente procedere con una regolazione coordinata.

Una particolare riflessione meritano le tecniche di *deep learning* e, nello specifico, le reti neurali, sia in quanto tra le metodologie di AI più complesse e che fanno emergere maggiori criticità, sia in quanto si mostrano al centro dell'attenzione grazie ai sensazionali successi raggiunti negli ultimi anni.

A mero titolo di esempio, si pensi a Deep Blue, l'AI che nel 1997 ha battuto il campione di scacchi Kasparov; a Watson, un software IBM che dopo aver vinto nel 2011 il gioco Jeopary! oggi viene utilizzato per le diagnosi mediche[4], o ancor più di recente ad AlphaGo, che nel 2016 ha battuto Lee Sedol, uno dei più grandi campioni mondiali di Go[5].

Oltre a queste dimostrazioni di abilità nei giochi, si pensi al dibattito in merito alla

[3] E. Giusti, *Intelligenza artificiale e sistema sanitario*, in S. Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, 310; si veda anche G. Romano, ivi, 107-108. Sul punto è stato osservato come non sia il «*corpus mechanicum* a definire e qualificare l'AI bensì un processo totalmente automatizzato basato sull'acquisizione e l'elaborazione di informazioni in grado di fornire un risultato, di correggerlo e implementarlo» C. Trevisi, *La regolamentazione in materia di intelligenza artificiale, robot, automazione: a che punto siamo*, in questa *Rivista*, 2, 2018, 447.

[4] Per un approfondimento in merito al funzionamento di Watson si rimanda a M.A. Boden, *L'intelligenza Artificiale*, Bologna, 2019, 66 ss. Oggi sono diversi gli algoritmi utilizzati per le diagnosi mediche, di recente è stato utilizzato un software in grado di diagnosticare la contrazione dell'infezione da Covid-19 solo analizzando il tono della voce in una conversazione telefonica. Sono in uso software in grado di individuare tumori grazie allo screening di immagini. Si pensi anche alle sperimentazioni in corso dirette ad utilizzare le applicazioni di AI per il riconoscimento dei sintomi di un infarto mediante l'analisi dell'andatura di un gruppo di pazienti, o alla possibilità di diagnosticare un principio di malattia neurodegenerativa dal tremolio del mouse. Per un approfondimento si rimanda a M. Savini Nicci-G. Vetrugno, *Intelligenza artificiale e responsabilità nel settore sanitario*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti e l'etica*, Milano, 2020, 601 e 607 ss.; P. Cappelletti-M. Golato, *Medicina di laboratorio 4.0*, in *Rivista italiana di medicina di laboratorio*, 14, 2018, 194-195; N. Bakkar-T. Kovalik-I. Lorenzini-S. Spangler-A. Lacoste-K. Sponaugle-P. Ferrante-E. Argentinis-R. Sattler-R- Bowser, *Artificial Intelligence in Neurodegenerative Disease Research: Use of IBM Watson to Identify Additional RNA-Binding Proteins Altered in Amyotrophic Lateral Sclerosis,* in *Acta Neuropathologica*, 135, 2018, 227; F. Jiang-Y. Jiang-H. Zhi-Y. Dong-H. Li-S. Ma-Yi. Wang-Q. Dong-H. Shen-Yo. Wang, *Artificial Intelligence in Healthcare: Past, Present and Future*, in *Stroke & Vascular Neurology*, 4, 2017, 2, 240; R.W. White- P.M. Doraiswamy- E. Horvitz, *Detecting Neurodegenerative Disorders from Web Search Signals*, in *Npj Digital Medicine*, 2018, 1 ss.; A.M. Froomkin-I. Kerr-J. Pineau, *When AIs Outperform Doctors: Confronting the Challenges of a Tort-Induced Over-Reliance on Machine Learning*, in *Arizona Law Review*, 1, 2019, 61, 33.

[5] Il software sviluppato da DeepMind, che nel 2016 riuscì a battere uno dei migliori giocatori a livello mondiale, utilizza diverse reti neurali. Proprio l'utilizzo combinato di queste ultime ha permesso ad AlphaGO non solo di apprendere le regole del gioco e le strategie utilizzate dai campioni mondiali, ma anche di elaborane alcune del tutto inedite. All'esito della competizione con Lee Sedol alcuni commentatori hanno ritenuto che AlpahaGo fosse dotata di quello che noi chiamiamo intuito. Si v. D. Heaven (a cura di), *Macchine che pensano*, Bari, 2018, 73 ss.

circolazione delle auto a guida autonoma o all'utilizzo di robot medicali; compiti che fino a pochi anni fa venivano ritenuti troppo complessi per un sistema informatico[6].
Tutti questi software, sempre più abili nel compiere azioni complesse, si basano su sistemi algoritmici che prevedono l'utilizzo di reti neurali artificiali (*Artificial Neural Network*)[7] che permettono alle macchine non solamente di processare numerose variabili[8] ma anche di "imparare" dall'esperienza[9]; da qui il termine "*machine learning*".
I risultati raggiunti dai sistemi algoritmici mostrano una sempre maggiore affidabilità e correttezza degli *output* da questi elaborati, tuttavia una tra le maggiori preoccupazioni in merito all'utilizzo delle ANN discende dalla loro intrinseca opacità di funzionamento. Se infatti da una parte è in astrattamente possibile conoscere i dati di addestramento e gli *output* della macchina, difficile è comprendere la *ratio* a fondamento della decisione presa nel singolo caso concreto. Ciò è dovuto proprio alla complessità del sistema, caratterizzato da una elevata mole di interazioni tra i nodi che compongono i livelli intermedi e "nascosti" in queste reti. Ne discende come sia difficile risalire a quale delle possibili variabili, in una fitta rete di connessioni e interazioni, abbia avuto un peso prevalente nella determinazione della scelta della macchina.
Questa condizione è stata efficacemente definita "*black box*"[10], proprio in ragione della

[6] Le reti neurali, lungi dall'essere utilizzate unicamente nei giochi, hanno trovato applicazione in molti settori socio-economici, dalla finanza alla medicina. La DeepMind di Google ha in corso diversi progetti in ambito medico e, grazie a una collaborazione con il sistema sanitario nazionale del Regno Unito, ha accesso a grandi quantità di dati sui pazienti. Sul punto si rimanda ivi, 124.

[7] Il funzionamento delle reti neurali artificiali si ispira al cervello umano. Queste vengono programmate con diversi livelli di neuroni artificiali, o nodi, tra loro collegati e aventi ognuno un "peso". Le reti oggi maggiormente utilizzate sono quelle multilivello, dove cioè sono presenti oltre all'*input* e all'*output* anche dei livelli "nascosti", composti da nodi che processano i dati raccolti. Ogni livello (*layer*) di neuroni indaga a un diverso livello di astrazione e trasmette l'informazione al livello successivo a cui esso è collegato, fino all'ultimo che corrisponde all'*output* del sistema. Per arrivare ad una AI affidabile è necessario un lungo periodo di addestramento, che viene compiuto sottoponendo agli algoritmi una grande quantità di dati che possono essere o meno catalogati. Per un approfondimento tecnico in merito al funzionamento delle diverse tipologie di reti neurali si rimanda a S. Russell-P. Norvig, *Intelligenza Artificiale*, cit., vol. 2, 423 ss. e a I. Goodfellow-Y. Bengio-A. Courville, *Deep Learning*, Cambridge, 2016, 489 ss. È possibile vedere le modalità di funzionamento di una rete neurale all'indirizzo *playground.tensorflow.org*.

[8] Tra le diverse tipologie di addestramento, quelle maggiormente utilizzare consistono nell'apprendimento per rinforzo, nell'apprendimento supervisionato e in quello non supervisionato. Per un approfondimento in merito alle tecniche di addestramento si rimanda a I. Goodfellow-Y. Bengio-A. Courville, ivi, 105 ss.; L. Deng-D. Yu, *Deep Learning: Methods and Applications*, in *Foundations and Trends in Signal Processing*, 3-4, 2013, 197 ss.; Y. LeCun-Y. Bengio-G. Hinton, *Deep Learning*, in *Nature*, 521, 2015, 436 ss.

[9] Una volta restituito un risultato, un algoritmo di *back-propagation* solitamente confronta il risultato ottenuto dal sistema neurale e modifica di conseguenza i singoli pesi dati ai nodi, così da rinforzare alcuni collegamenti e indebolirne altri; ciò al fine di giungere in maniera ottimale e più velocemente possibile al risultato corretto. In questo senso è possibile dire che l'algoritmo è autonomo e che "impara"; in quanto non è il programmatore del software a modificare i singoli pesi dei neuroni appartenenti alla rete. In ragione della sempre maggiore complessità data dall'estensione della rete è un altro algoritmo che compie quest'ultimo passaggio, a partire dei risultati ottenuti dal sistema. I. Goodfellow-Y. Bengio-A. Courville, *Deep Learning*, cit., 18 e 203 ss.; L. Deng-D. Yu, *Deep Learning*, cit., 203 ss.; Y. LeCun-Y. Bengio-G. Hinton, *Deep Learning*, cit., 436 ss.; Y. Bengio, *Learning Deep Architectures for AI,* in *Foundations and Trends® in Machine Learning*, 2(1), 2009, 10 ss.; C. Lexcellent, *Artificial intelligence versus human intelligence: are humans going to be hacked?*, Berlino, 2019, 10 ss.

[10] Questa espressione è stata coniata da F. Pasquale, *The Black Box Society: The Secret Algorithms That*

sua complessità e opacità anche agli occhi degli stessi programmatori.
Finché i risultati ottenuti sono corretti *nulla quaestio*. Tuttavia qualora il sistema sbagli, o mostri risultati discriminatori, la difficoltà di arrivare a una spiegazione che sia intellegibile comporta l'emergere di preoccupazioni in merito all'utilizzo sempre più esteso che viene fatto e, soprattutto, in ragione all'individuazione di chi debba essere ritenuto responsabile dei danni che dall'uso di questi applicativi può discendere[11].

3. La qualità dei dati come requisito necessario per AI affidabili

Da quanto brevemente richiamato in merito al funzionamento delle applicazioni di AI, emerge con evidenza come una tra le maggiori criticità risieda nella considerazione per cui il volume e l'eterogeneità dei dati generati e raccolti renda difficoltosa la verifica in merito alla qualità degli stessi, sia in termini di esattezza dei *data*, che di rimozione di possibili *bias*.
Il problema si avverte in modo particolare proprio perché i dati raccolti fungono da dataset per l'addestramento degli algoritmi, e su questi si fondano gli *output* del sistema; la capacità delle applicazioni *data driven* di trovare collegamenti e ricorrenze statistiche potrebbe difatti portare a risultati di scarsa qualità, secondo un effetto di c.d. *garbage in-garbage out*[12].
Sul punto è necessario evidenziare come i possibili *output* discriminatori generati delle macchine non siano *tout court* legati ad una "informazione" errata processata dal sistema, ma possano essere dovuti anche ad una sotto rappresentazione di determinate categorie di soggetti; problema che potrebbe acuirsi in considerazione del divario tecnologico, che pare oggi essere in forte crescita[13].

Control Money and Information, Cambridge, 2015.

[11] La necessità sempre più sentita in merito alla trasparenza di funzionamento degli algoritmi, alla luce del rischio di possibili violazioni dei diritti degli interessati, vede come contraltare l'utilizzo di tecnologie di AI quali mezzi idonei a migliorare e rendere più efficiente la stessa società. Sul punto interessanti le considerazioni critiche di Messinetti in merito all'utilizzo degli algoritmi, che verrebbe presentato quale "rassicurante". Le modalità stesse di funzionamento, mediante correlazioni statistiche, permetterebbero di affrancarsi dalla necessità di ricostruzione delle cause degli eventi; così facendo sarebbe possibile governare meglio la complessità, definita "liquida", della società moderna e ciò grazie a previsioni generalizzanti, in quanto calcolate matematicamente. Le tecnologie di AI consentirebbero dunque il raggiungimento di alcuni obiettivi ritenuti decisivi dalla società: la sicurezza, la velocità e l'economicità. R. Messinetti, *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contratto e impresa*, 3, 2019, 863 ss.

[12] Appare chiaro come le possibili esternalità negative, legate a una cattiva rappresentazione dei dati in ingresso, abbiano portato a istanze di regolazione e valutazione della loro qualità. Prendendo dati sporchi e imprecisi o di cattiva qualità in ingresso, le AI producono modelli sbagliati e quindi poco rispondenti allo scopo per cui i dati sono stati raccolti. Cfr. G.F. Italiano, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Analisi giuridica dell'economia*, 1, 2019, 13.

[13] Si parla di un vero e proprio *digital divide*, con tale espressione intendendosi il divario tra chi ha accesso alle tecnologie dell'informazione e invece chi ne è escluso. Le disuguaglianze e la disomogeneità di accesso agli strumenti tecnologici mostrano altresì un divario culturale, richiedendo interventi mirati anche sul piano dell'educazione e dell'aggiornamento costante, al fine di garantire effettivamente pari

A ciò deve aggiungersi come spesso venga incoraggiato l'utilizzo delle tecnologie di Intelligenza Artificiale sull'assunto per cui i risultati da esse generati siano "neutrali". Detta affermazione appare però frutto di un fraintendimento.

Si crede che le scelte operate dagli algoritmi siano neutrali perché essi non sono condizionati da costrutti valoriali o da esperienze personali, come invece sarebbero gli operatori umani chiamati a decidere nelle medesime situazioni. Questa considerazione tuttavia non è del tutto corretta.

Gli *output* della macchina sono generati processando i dati raccolti nella società e di questa quindi ne sono espressione. Difficilmente i dataset verranno creati con dati volutamente discriminatori, ma proprio la capacità di analisi dei sistemi *data driven* può portare alla luce discriminazioni latenti e intrise nel tessuto sociale[14]. È qui che emerge come gli *output* delle macchine non siano neutrali, e ciò semplicemente perché non lo sono i dati su cui esse operano. Nemmeno neutrale risulta essere la scelta operata dal programmatore sia in merito alla scelta dei dataset di addestramento, che alla stessa creazione dell'algoritmo di AI[15].

Al fine di mitigare possibili esternalità negative allora appare necessaria *in primis* una attenta verifica della qualità dei dati raccolti, operazione che dovrebbe vedere coinvolti anche gli stessi programmatori delle AI[16].

Difatti, dal momento che il concetto di qualità non ha un'interpretazione univoca,

---

opportunità di accesso alla tecnologia. Cfr. sul punto L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Roma, 2020, 26 ss. Interessante anche la panoramica offerta da S. Rodotà, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014. Le stesse Istituzioni europee si sono mostrate consapevoli dell'urgenza di rendere la tecnologia accessibile paritariamente proponendo nell'agenda digitale lo stanziamento di fondi a ciò specificamente destinati. Sul punto si rimanda alle comunicazioni consultabili all'indirizzo *europarl.europa.eu*. Per un approfondimento sul tema si rimanda a R.K. Jorgensen (a cura di), *Human rights in the global information society*, Cambridge, 2019.

[14] S. Scalzini, *Alcune questioni a proposito di algoritmi, dati, etica e ricerca*, in *Rivista italiana di medicina legale (e del Diritto in campo sanitario)*, 1, 2019, 172 ss.; E. Pellecchia, *Profilazione e decisioni automatizzate al tempo della Black Box Society: quale leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Nuove leggi civili commentate*, 5, 2018, 1210 ss. V. sul punto F. Corona-A. Del Pizzo, *IA: l'approccio europeo è basato sull'eccellenza e la fiducia*, in *dirittodiinternet.it*, 5 giugno 2020.

[15] Andando ancora più a ritroso nemmeno il dato considerato singolarmente può essere considerato neutrale; esso difatti essendo espressione del reale ne è una necessaria semplificazione, frutto della scelta operata da coloro che hanno determinato gli *script* – i comandi – idonei a rendere computabile il fenomeno. Interessante anche la posizione di Amato Mangiameli, il quale sottolinea come la non neutralità degli algoritmi sia legata ad alcuni fattori tra cui: l'asimmetria informativa tra una società che offre un servizio e l'utente; l'assenza di trasparenza relativa al funzionamento dell'algoritmo e la creazione di una *filter bubble* che mostrerebbe all'utente solamente le informazioni che l'algoritmo ha calcolato possano interessargli. Da ciò ne discende – chiarisce l'Autore – come non vi siano algoritmi neutrali, questi non si limiterebbero a riflettere la realtà, ma ne proporrebbero una loro versione «fatta di formule classificanti, dal peso attribuito ai singoli parametri inseriti, dalle procedure che determinano il risultato». A.C. Amato Mangiameli, *Algoritmi e "big data". Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1, 2019, 109.

[16] In argomento si v. A. Moretti, *Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679*, in *Diritto dell'informazione e dell'informatica*, 4-5, 2018, 815 ss. L'Autore, dopo aver sottolineato l'inscindibilità tra algoritmi e dati, e dunque la necessità che questi ultimi siano di qualità affinché il procedimento matematico possa condurre a un risultato apprezzabile, pone l'attenzione sul ruolo dei *data scientist*. Essi sono, infatti, i soggetti preposti alla creazione dell'architettura del sistema, determinano gli obiettivi e le logiche seguite; si reputa allora opportuno un intervento che disciplini e vigili sul loro operato. L'Autore ipotizza l'adozione di codici di condotta che fissino regole condivise e omogenee.

dovendo essere parametrato agli scopi ai quali i dati sono diretti, al fine di miticare le difficoltà di verifica e misurazione della qualità dei dataset potrebbero essere predisposti dagli operatori che programmano i sistemi *data driven* codici di condotta e standard tecnici che siano condivisi dalla comunità scientifica.

Il legislatore europeo aveva già considerato la predisposizione di standard legati alla interoperabilità dei dati, nella prospettiva di renderne più agevole la circolazione e permettere un completo sviluppo del mercato unico europeo. Del pari anche gli standard qualitativi ricoprirebbero allora un importate ruolo nella strategia di sviluppo del mercato, comportando una maggiore sicurezza dei sistemi e un rafforzamento dell'affidamento degli utenti; obiettivo anch'esso perseguito nella strategia europea sui dati.

Sul punto, le normative della serie ISO/IEC 25000, dedicate proprio alla certificazione della qualità dei dati e dei software, potrebbero fornire alcuni spunti interessanti[17].

Lo standard ISO-25012 individua 15 caratteristiche[18], alcune delle quali inerenti gli stessi dati e altre dipendenti dal sistema a cui sono destinati, lasciando tuttavia ai singoli settori, in ragione del contesto d'uso, la definizione di soglie di accettabilità secondo cui verificare la rispondenza o meno ai requisiti di qualità richiesti.

Successivamente, nel 2014, è stato emanato un nuovo standard (ISO/IEC 25024) diretto ad estendere il campo delle misurazioni, definendo ben 63 caratteristiche identificative di qualità[19]. Elemento di particolare rilevanza è la presenza di caratteristiche quali la comprensibilità, la disponibilità, la portabilità, la sicurezza (in termini di privacy) e l'accessibilità, che se implementanti all'interno delle applicazioni di Intelligenza Artificiale permetterebbero la diffusione di sistemi maggiormente interoperabili e sicuri, potendo questi ultimi operare su dati controllati e condivisi.

Una maggiore qualità favorirebbe non solamente un miglior governo dei *big data*, ma anche l'incremento di dati riusabili, il miglioramento dei processi che causano dati errati, la stima dei costi di prodotti di non qualità, etc.[20]. Evidentemente una diffusione di una prassi condivisa tra gli operatori comporterebbe altresì una maggiore possibilità di diffusione di *open data*[21], particolarmente importanti per esempio nel settore medicale, ove lo sviluppo di soluzioni di Intelligenza Artificiale necessita di una sempre

---

[17] Si tratta dello standard ISO/IEC 25012 che definisce le caratteristiche di qualità dei dati, pubblicato nel 2008 e successivamente esteso con lo standard ISO/IEC 25024. Complementare è il modello di qualità dei software compreso nello standard ISO/IEC 25010.

[18] Le caratteristiche elencate dallo standard ISO/IEC 25012/2008 sono: accuratezza, completezza, coerenza, credibilità, attualità, accessibilità, conformità, riservatezza, efficienza, precisione, tracciabilità, comprensibilità, disponibilità, portabilità e ripristinabilità. Come si nota le ultime tre sono direttamente dipendenti dalle caratteristiche del sistema in cui i dati sono utilizzati.

[19] Per un approfondimento in merito alle caratteristiche di qualità dei dati e un confronto con lo standard ISO/IEC 9126-3, sulla qualità dei software, si rimanda a M.F. Pinzon-J.S. Sanabria, *Aplicación del estándar ISO/IEC 9126-3 en el modelo de datos conceptual entidad-relación*, in *Revista Facultad de Ingeniería*, 35, 2013, 35, 113 ss.; D. Natale, *Orientamenti sul modello di qualità dell'Intelligenza Artificiale*, in *intelligenzartificiale.unisal.it,* 22 aprile 2020.

[20] Si v. il comunicato stampa dell'AGID in merito alla misurazione della qualità dei dati, che accompagna la pubblicazione dello standard ISO nella versione in lingua italiana. Consultabile all'indirizzo *agid.gov.it*.

[21] V. F. Faini, *Dati, algoritmi e Regolamento europeo 2016/679*, in M. Mantelero-D. Poletti (a cura di), *Regolare la tecnologia: il Reg. UE n. 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 344. ss. In argomento si rimanda anche a M. Maretti-V. Russo-E. Gobbo, *Open data governance: civic hacking movement, topics and opinions in digital space*, in *Quality & Quantity*, 3, 2021, 1133 ss.

maggiore condivisione al fine di risolvere i problemi di replicabilità dei risultati; ciò al fine di permettere una sicura diffusione degli applicativi *data driven* all'interno della comunità scientifica.

4. Il principio di esattezza in una visione d'insieme

La necessità di una maggiore attenzione alla qualità, lungi dall'essere una esigenza sentita solo dagli esperti della materia è avvertita anche dalle stesse istituzioni europee[22].
La Commissione, in un comunicato stampa di accompagnamento alla pubblicazione delle linee guida etiche, dopo aver ripreso i principi di *privacy by design* e di *data protection*[23] già previsti nel Regolamento 2016/679 UE, fa un'importante precisazione: sottolinea in modo chiaro come la necessità di elaborare sistemi di AI di elevata qualità non possa prescindere dalla qualità degli stessi dati di addestramento.
Detto riferimento è particolarmente significativo. Per la prima volta in modo esplicito viene dato rilievo allo stretto legame funzionale tre le due materie, così dimostrando che solo una visione coordinata e unitaria del fenomeno tecnologico ne permette la comprensione e dunque una regolazione efficace.
Compreso il ruolo centrale che l'analisi dei dati riveste nelle applicazioni di Intelligenza Artificiale si comprende la preoccupazione mostrata non solamente dalle Istituzioni europee, ma anche dai maggiori esperti della materia, in merito all'utilizzo di dati di qualità.
Da più parti sono infatti state avanzate istanze di maggiore attenzione al rispetto dei principi introdotti dal GDPR anche nello sviluppo delle tecnologie *data driven*.
Sul punto si pensi alle linee guida in materia di Intelligenza Artificiale emanate dal comitato consultivo della Convenzione 108 e indirizzate ai *policy maker* e agli sviluppatori degli algoritmi[24].
Dopo aver evidenziato come le applicazioni di Intelligenza Artificiale rappresentino uno strumento utile, specialmente nel supportare politiche inclusive, viene fatta luce sulle possibili ripercussioni negative che un uso non regolato della tecnologia può comportare sia per gli individui che per l'intera società. Proprio in relazione alla necessità di evitare possibili pregiudizi una particolare attenzione viene posta anche alla verifica circa la qualità dei dati, secondo una declinazione atta a ricomprendere la natura, l'origine e la quantità, per tutte le fasi di funzionamento degli algoritmi.
Di fronte a esternalità negative sotto certi versi inevitabili, in quanto connaturate al funzionamento di ogni sistema discreto, ivi compresi i sistemi di AI, così come teoriz-

[22] Da ultimo un rimando alla necessaria attenzione a dati di alta qualità viene fatto anche nella recentissima proposta di regolamento "Data Act" emanata dalla Commissione il 23 febbraio 2022. Nel testo si fa espresso riferimento alla qualità dei dati quale requisito in grado di incrementare la competitività e l'innovazione, assicurando al contempo una crescita sostenibile. Si rimanda al testo della Commissione, *Proposal for a Regulation of the European parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, 23.2.2022, COM(2022) 68 final.

[23] Comunicato stampa consultabile all'indirizzo *ec.europa.eu*.

[24] Comitato Consultivo Convezione 108, *Linee guida in materia di intelligenza artificiale e protezione dei dati*, 2019, T-PD (2019) 01.

zato da Gödel[25], appare infatti necessario un approccio avente natura precauzionale e volto a diminuirne l'incidenza.

In argomento il regolamento (UE) 679/2016 (GDPR) riveste un ruolo di rilievo. Questo, pur non occupandosi direttamente di Intelligenza Artificiale, prevede infatti alcuni strumenti che ben potrebbero – se potenziati – essere utilizzati proprio al fine di rendere i sistemi in parola più sicuri, affidabili e di qualità.

Per l'argomento che qui ci occupa, una particolare importanza non può che rivestire il principio di esattezza dei dati[26].

Si tratta di un principio diretto a evitare distorsioni nella rappresentazione dei *data*, che dunque costituisce un presupposto necessario all'effettività del diritto all'autodeterminazione informativa.

Il principio di esattezza mostra tutta la sua centralità proprio nei trattamenti articolati su filiere complesse, quali quelli operati mediante metodologie di AI. Come visto, dette tecniche sono influenzate dalla qualità dei dati in ingresso[27], infatti queste permettono la "creazione" di dati e di informazioni, spesso partendo *raw data*, mediante la combinazione e la ricerca di ricorrenze statistiche. Il principio in parola acquista allora una rilevanza fondamentale, legandosi a una necessaria affidabilità, non solamente dei dati, ma anche delle modalità di raccolta e di analisi degli stessi.

È infatti indispensabile per avere *dataset* di qualità che le capacità degli analisti di verificare se i dati siano utilizzabili o meno per il successivo trattamento siano affidabili. Del pari devono essere affidabili le modalità di analisi probabilistica utilizzate allo scopo di trarre nuovi dati da quelli raccolti in origine[28].

---

[25] Il lavoro di Gödel, pur riguardando le proposizioni cosiddette indecidibili, ha portata generale e può essere esteso a tutti i sistemi formali (cioè sistemi finiti, quali sono ad oggi quelli informatici). Gödel dimostrò che è sempre possibile aggiungere assiomi all'interno di un sistema formale al fine di poter verificare la verità di una proposizione indecidibile. Tuttavia in questo sistema, arricchito dai nuovi assiomi aggiunti, esisterebbero comunque nuove proposizioni indecidibili. Il risultato raggiunto dal logico austriaco è generale, dunque è possibile affermare che per qualsiasi programma (sistema formale) esistono sempre affermazioni false che verranno interpretate come vere. Dunque ogni programma avrà sempre e inevitabilmente infinite istruzioni che non ne permettono il corretto funzionamento. Il teorema trova particolare espressione anche nell'ambito della sicurezza dei sistemi digitali; quando un programma riceve in ingresso delle informazioni non decidibili non è possibile prevedere il risultato dell'elaborazione, rendendo il sistema vulnerabile, in quanto soggetto a ogni tipo di potenziale incidente di sicurezza. In argomento si rimanda a G. D'Acquisto-M. Naldi, *Big Data e Privacy by Design*, Torino, 2017, 180 ss.

[26] «[I dati personali devono essere, ndr] esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati», art. 5, lett. *d*), GDPR.

[27] La stessa varietà di dati resi disponibili agli algoritmi per l'analisi comporta in una certa misura una inevitabile incertezza in merito alla loro accuratezza. De Gregorio e Torino sul punto richiamano le parole di Boyd e Crawford secondo cui sarebbe direttamente proporzionale il rapporto che lega l'incremento delle fonti di provenienza dei dati e l'aumento del rischio di dati inaccurati. Si v. G. De Gregorio-R. Torino, *Privacy, tutela dei dati personali e Big Data*, in E. Tosi (a cura di), *Privacy digitale, Riservatezza e protezione dei dati e nuovo Codice Privacy*, Milano, 2019, 465.

[28] Di catena di affidabilità parla F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, *Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 260-261. L'Autore richiama inoltre la necessità che il concetto di esattezza venga parametrato anche alla dimensione "tempo", ciò in quanto la realtà è in continua evoluzione, comportando così l'inevitabile "invecchiamento" dei dati e la loro perdita di esattezza, intesa come "corrispondenza alla porzione di realtà".

Procedendo con l'analisi del principio in parola, il legislatore europeo introduce nel testo del Regolamento un obbligo per il titolare particolarmente impegnativo, anche in relazione alla sua estensione[29]. Viene prevista la verifica circa l'esattezza e l'aggiornamento dei dati rispetto alle finalità per le quali sono trattati, secondo quello che è stato definito uno specifico onere di "fedeltà contenutistica"[30].

Possiamo dunque notare innanzitutto come la nozione di esattezza del dato sia un concetto eminentemente relazionale, da valutare in correlazione al fine e all'utilizzo stesso che ne dovrà essere fatto. Appare infatti chiaramente che la correttezza e adeguatezza dei dati debba essere valutata in relazione agli scopi perseguiti. Come sottolinea autorevole dottrina, per esempio, non tutti i dati debbono essere costantemente aggiornati, ben potendo dati anche molto risalenti nel tempo rispondere adeguatamente agli scopi del trattamento[31].

Dalla lettura del testo emergere dunque per certi versi un divieto di utilizzo e raccolta indiscriminato dei dati, c.d. pesca a strascico[32], senza cioè aver definito gli scopi perseguiti e senza una verifica circa la loro utilità e correttezza. Previsione questa che sembra essere diretta proprio a regolare quei trattamenti che si fondano sull'uso di tecnologie *data driven*, e in particolare le AI, il cui funzionamento ad oggi si fonda per la maggior parte su di un uso indiscriminato di un numero considerevole di dati, senza alcuna selezione né quantitativa né qualitativa.

Il legislatore europeo pare allora essere consapevole che se non pare attualmente operabile una selezione nella quantità dei dati raccolti, dal momento che il valore delle tecniche di *data mining* risiede proprio nell'estrarre informazioni – e così ricchezza – da un numero considerevole di variabili, è allora necessario prestare una concreta attenzione alla qualità del dato, così da poter limitare i rischi di *output* distorti.

Alla luce di quanto fin qui esposto, nell'attuale assetto normativo il principio di esattezza meriterebbe forse un potenziamento, mostrandosi particolarmente rilevante nella regolazione del fenomeno digitale; questo ad oggi viene tuttavia declinato nella previsione di una prerogativa dell'interessato, il quale ha il diritto di chiedere la rettifica o l'integrazione dei propri dati personali[33]. L'interessato è chiamato a farsi parte attiva,

---

[29] Il titolare è chiamato a comunicare a tutti coloro a cui egli abbia trasmesso i dati le eventuali rettifiche, cancellazioni o richieste di limitazione di trattamento. È tuttavia previsto un limite a questo obbligo, che altrimenti avrebbe potuto comportare un eccessivo aggravio degli oneri del titolare, prevedendo che questo non sussista nel caso in cui si riveli impossibile, a fronte della natura del trattamento, o implichi uno sforzo sproporzionato. Si v. art. 34, par. 3, GDPR.

[30] M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 210. Sul punto Di Resta, facendo uno specifico richiamo all'ambito giornalistico, parla di introduzione di uno "standard di diligenza" che verrebbe così a gravare sul titolare del trattamento nella gestione dei dati raccolti. Si v. F. Di Resta, *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino, 2018, 46.

[31] Si v. F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in Id., *Intelligenza Artificiale, protezione dei dati personali e regolazione,* Torino, 2018, 44 ss., spec. 60-61; F. Resta, *Sub* art. 5, in G.M. Riccio-G. Scorza-E. Belisario (a cura di), *Commentario GDPR e normativa privacy*, Milano, 2018, 58-59.

[32] F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 61.

[33] Interessante la considerazione di Dell'Utri secondo cui dai principi di esattezza e minimizzazione deriverebbe la necessità di un confronto tra gli interessati e il titolare del trattamento. Dal confronto

instaurando così un confronto dialettico tra diritti e interessi in parte confliggenti.
Si auspica, tuttavia, che proprio alla luce dei rischi nascenti dall'utilizzo di tecnologie di AI, le quali possono avere un impatto nei confronti di qualunque persona fisica e – in definitiva – dell'intera società nel suo complesso[34], dunque non solamente nei confronti dei singoli interessati, il principio venga declinato quale obbligo maggiormente specifico anche nei confronti dei titolari[35].
Il principio di esattezza potrebbe difatti essere implementato nella fase iniziale di raccolta, mediante specifici obblighi per i titolari del trattamento di verifica a monte circa la presenza di caratteristiche intrinseche dei dati che ne definiscono la qualità. Tra queste potrebbero per esempio essere fatte rientrare, mutuando quanto previsto negli standard ISO/IEC sopra richiamati: la descrizione in modo accurato della realtà che i dati intendono rappresentare; l'attualità e dunque l'aggiornamento dei dati; la loro non contraddittorietà e, infine, la completezza, cioè la presenza di un numero di attributi sufficiente a rappresentare correttamente il fenomeno analizzato[36].

5. Le tecnologia quale alleato nella filiera di dati di qualità

Se dunque una particolare attenzione dovrebbe essere posta alla verifica circa la qualità dei dati, secondo una declinazione atta a ricomprendere la natura, l'origine e la quantità, per tutte le fasi di funzionamento degli algoritmi, non appare tuttavia a prima vista immediato il rispetto di requisiti così parametrati.
Per raggiungere detto obiettivo, oltre alle necessarie previsioni normative fin qui richiamate, spazio potrebbero trovare anche le stesse applicazioni di Intelligenza Artificiale, tra cui, in particolare la tecnologia *blockchain* e i cc.dd. dati sintetici.
Da un lato la tecnologia *blockchain* potrebbe difatti rispondere all'obiettivo di creare *dataset* di comprovata qualità, dal momento che permetterebbe di collazionare all'interno della "catena" unicamente quei dati rispondenti a predeterminate caratteristiche e standard definiti a monte, il cui rispetto verrebbe così certificato.

troverebbe composizione l'eventuale scontro tra la «dimensione oggettiva della funzionalità minima del trattamento (così come della rispondenza oggettiva del contenuto dei dati alla realtà da essi rispecchiata), al valore soggettivamente attribuito, dai rispettivi titolari, così come a quelli che, per converso, invocano un profilo specifico dell'esattezza della rappresentazione, nella sua idoneità a rispettare le forme o i modi attraverso i quali ciascuno percepisce riflessivamente i termini della propria identità personale partecipata al contesto di relazione», M. Dell'Utri, *Principi generali e condizioni di liceità*, cit., 210.

[34] Nella valutazione circa la natura del principio di esattezza Pizzetti evidenza come, a differenza degli altri principi elencati nell'art. 5, questo abbia un evidente spessore di carattere collettivo. Il principio in parola impegnerebbe «il titolare a una ancor più approfondita valutazione di rischio, soprattutto rispetto all'orizzonte degli effetti dei trattamenti. Il titolare, infatti, deve avere come punto di riferimento non solo l'interessato ma la tutela delle libertà e dei diritti delle persone fisiche che possono essere coinvolte e, in sostanza, della società come tale», V. F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 62.

[35] Ad oggi un espresso riferimento in tal senso si rinviene unicamente nel considerando 71 del GDPR.

[36] A. Travaglia, Big data e Regolamento europeo sulla protezione dei dati personali, in *academia.edu*, 2017, 5.

Ciò sarebbe possibile poiché la *blockchain* si basa su di un registro distribuito[37]: le informazioni presenti nel sistema vengono infatti replicate in una serie di terminali, chiamati nodi, tra loro in posizione di parità.

Entrando più nello specifico, le transazioni eseguite vengono ordinate cronologicamente (grazie a delle marcature temporali o *timestamps*) e divise in blocchi[38]. I blocchi sono dotati di un *header*, utilizzato per organizzare il database distribuito, al cui interno è contenuto: un codice *hash* univoco (che si compone di una striscia alfanumerica)[39] di tutte le transazioni registrate nel blocco; la marcatura temporale e il codice *hash* del blocco precedente. Si forma così una vera e propria catena di blocchi, da qui il termine "*blockchain*"[40].

È evidente come questa tecnologia mostri una particolare resistenza agli attacchi esterni, dal momento che qualora si forzasse il sistema ciò comporterebbe una modifica del codice *hash*, "spezzando" così la catena. Inoltre essendo un registro distribuito, in cui i nodi sono protetti da una crittografia asimmetrica[41], sarebbe difficile per un soggetto esterno individuare e modificare tutte le copie conservate nei nodi, rivelando così il tentativo di manomissione.

Una volta validati, dunque inseriti all'interno della *blockchain*, i dati sarebbero difficilmente modificabili, e ciò permetterebbe evidentemente una maggiore sicurezza circa

---

[37] Detta tecnologia fa, infatti, parte della categoria delle *Distributed Ledger Technology* (DLT). Questo sistema si pone in contrapposizione con il classico modello centralizzato, ove le informazioni sono raccolte tutte in un server e si diramano mediante il download dei *clients*.

[38] Per poter essere aggiunto alla catena, ciascun blocco deve essere validato. Solitamente questo compito viene affidato a nodi a ciò incaricati sulla base di regole prestabilite dal protocollo informatico e condivise dai partecipanti alla *blockchain*. La modalità di validazione più conosciuta è la c.d. *proof of work* – la stessa utilizzata per i Bitcoin – che consiste in una competizione tra validatori (*miners*), ove il primo che risolve un complesso problema matematico è legittimato a inserire un nuovo blocco e a ricevere una ricompensa per il lavoro svolto. Questa non è l'unica modalità di aggiunta di nuovi blocchi alla catena, la scelta varia tendenzialmente in ragione della tipologia di *blockchain* scelta. Cfr. sul punto A.M. Gambino-C. Bomprezzi, *Blockchain e protezione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 3, 2019, 622 ss.; F. Sarzana di S. Ippolito-M. Nicotra, *Diritto della Blockchain, intelligenza artificiale e IoT*, Milano, 2018, 26 ss.; F. Bellini-D. Martinescu-L. Vassalli, *Digital Ledger Technologies*, in F. Bellini-F. D'Ascenzo (a cura di), *Digital transformation and data management*, Pisa, 2020, 133; P. Cuccuru, *Blockchain ed automazione contrattuale. Riflessioni sugli smart contract*, in *Nuova giurisprudenza civile commentata*, 1, II, 2017, 108 s.; S. Capaccioli, *La blockchain*, in G. Ziccardi-P. Perri (a cura di), *Tecnologia e Diritto*, vol. 2, Milano, 2019, 374 ss.

[39] La funzione di *hash* permette di comprimere i dati in un formato composto da una sequenza, avente lunghezza determinata, di cifre e lettere, assegnate mediante un algoritmo di calcolo. Per un approfondimento si rimanda a M. Giuliano, *La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio*, in *Diritto dell'informazione e dell'informatica*, 6, 2018, 999 ss.; G. D'Acquisto-M. Naldi, *Big Data e Privacy by Design*, cit., 136 ss.

[40] Cfr. F. Bellini-D. Martinescu-L. Vassalli, *Digital Ledger Technologies*, cit., 127 ss.; E. Terolli, *Blockchain e compliance (Regtech)*, in G. Alpa (a cura di), *Diritto e Intelligenza Artificiale*, Pisa, 2020, 378 ss.; F. Sarzana di S. Ippolito-M. Nicotra, *Diritto della Blockchain*, cit., 11 ss.; A.M. Gambino-C. Bomprezzi, *Blockchain e protezione dei dati personali,* cit., 620 ss.; A. Fiorelli-A.R. Cassano, *La rivoluzione tecnologica della blockchain*, in G. Cassano-S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Milano, 2020, 253 ss.; S. Capaccioli, *La blockchain*, cit., 371 ss.

[41] La cifratura a chiavi asimmetriche si compone di una chiave pubblica, conosciuta nel *network*, e di una privata che invece è conosciuta solamente dall'utente. Questa tecnica permette di assicurare la paternità di un messaggio e la sua integrità. V. F. Bellini-D. Martinescu-L. Vassalli, *Digital Ledger Technologies*, cit., 136-137.

la rispondenza ai requisiti di qualità da questi soddisfatti.
Detta tecnologia, potrebbe inoltre permettere una maggiore consapevolezza da parte degli interessati, i quali potrebbero verificare tutte le transazioni eseguite. Inoltre, la crittografia asimmetrica permetterebbe di limitare l'accesso da parte dei titolari ai soli dati per cui gli utenti abbiano effettivamente dato il consenso, così inverando il principio di minimizzazione previsto all'art. 5 del GDPR[42].
La *blockchain* potrebbe essere inoltre utilizzata per contrastare l'accentramento delle capacità computazionali e l'eccessiva specializzazione degli algoritmi[43]. A questo è diretto, per esempio, il progetto *singularity.net* che si propone di creare un *marketplace* di Intelligenza Artificiale[44].
Grazie alla *blockchain* sarebbe dunque in astratto possibile eliminare posizioni dominanti sul mercato, mediante la predisposizione di registri distribuiti, non solamente di algoritmi di AI, ma anche di dati di addestramento, potendo verificare in ogni momento le transazioni eseguite e la provenienza degli stessi[45].
Nonostante questi indubitabili pregi, la *blockchain* presenta anche alcuni profili di criticità, sia giuridici che di natura tecnica, i quali meritano un'attenta riflessione in un'ottica di ponderare rischi e benefici. In particolare l'uso di questa tecnologia presuppone alti costi di mantenimento, legati alla potenza di calcolo necessaria per far funzionare la catena stessa. Oltre alla fattibilità tecnica, tensioni nascono in relazione alla compatibilità con la normativa sulla *data protection*. Una prima tensione emerge, infatti, nell'individuazione di un soggetto che possa dirsi effettivamente titolare del trattamento, sebbene esistano diverse tipologie di *blockchain* tra cui quelle *permissioned*, in cui dunque è possibile individuare un soggetto titolare dei trattamenti.
Maggiori criticità emergono invece con il principio di limitazione della conservazione dei dati, poiché questi potrebbero astrattamente essere sempre conservati; con il c.d. diritto all'oblio degli interessati e, infine, con il diritto di chiedere la rettifica o l'aggiornamento da parte degli interessati, dal momento che i dati in linea di massima si mostrano immodificabili una volta immessi nella catena[46].

---

[42] Questa caratteristica potrebbe rivelarsi particolarmente utile per rispondere ad alcune criticità legate agli *Internet of Things* (IoT). Queste applicazioni raccolgono costantemente una grande mole di dati degli utenti, spesso senza che questi ne siano pienamente consapevoli. Una limitazione, consistente nella selezione dei soli dati per i quali gli interessati abbiano espresso il consenso, permetterebbe di rendere tecnicamente implementabile anche in dette applicazioni il principio di minimizzazione. Inoltre, ad oggi, gli IoT sono necessariamente collegati a *cloud server* per la raccolta e la conservazione dei dati; così facendo essi sono più soggetti a rischi di attacchi esterni alla sicurezza, essendo i server centralizzati, a differenza di quanto invece accadrebbe se venisse implementata una blockchain.

[43] Si v. F. Sarzana di S. Ippolito-M. Nicotra, *Diritto della Blockchain*, cit., 119.

[44] Sarebbe possibile per i produttori di AI attestare su un nodo della blockchain il proprio sistema di *machine learning*, o il proprio algoritmo, così consentendo ai partecipati al network di utilizzarlo, a fronte del versamento di un corrispettivo. Per un approfondimento in merito al progetto SingularityNET e alle applicazioni ad oggi sviluppate, si rimanda all'indirizzo *singularitynet.io*.

[45] Si v.. F. Sarzana di S. Ippolito-M. Nicotra, *Diritto della Blockchain*, cit., 120-121; J. Rodriguez, *Why Decentralized AI Matters Part I: Economics and Enablers*, in *medium.com*, 2018.

[46] Si rimanda a H. Chang, *Blockchain: Disrupting data protection?*, in *Privacy Laws & Business International Report*, 41, 2017, 2; A.M. Gambino-C. Bomprezzi, *Blockchain e protezione dei dati personali*, cit., 632 ss.; M. Giuliano, *La blockchain e gli smart contracts*, *cit.*, 1010 ss.; M. Finck, *Blockchain and data Protection in the european union,* in *European data protection law review*, 1, 2018, 27; J. Moser, *The Application & Impact of the*

6. (segue) i dati sintetici

Tra le possibili soluzioni atte a regolare i dati di addestramento si potrebbe annoverare anche l'uso dei cc.dd. dati sintetici[47], indicati anche dalle linee guida emanate dal comitato consultivo della Convenzione 108 sopra richiamato[48]. L'espressione viene utilizzata per definire quei dati generati mediante tecniche di AI e aventi l'obiettivo di essere "rappresentativi" di quelli originali.

L'utilizzo di questi potrebbe essere una possibile soluzione atta a minimizzare la quantità dei *Data* di addestramento, così implementando nei sistemi algoritmici anche il principio di minimizzazione.

Inoltre, l'impiego di dati "creati" da una AI premetterebbe di tutelare maggiormente gli interessati a cui ineriscono i dati personali originari; difatti questa tecnica permetterebbe una pseudonimizzazione dei dati, che dunque non sarebbero più direttamente espressivi di informazioni personali e permetterebbe così al contempo una maggiore sicurezza anche negli usi secondari che vengono fatti dei dati raccolti.

Accanto agli indubitabili pregi, è bene fin da subito evidenziare come l'utilizzo di questa tipologia di dati possa comportare altresì alcune criticità. Difatti, se questi non rispecchiassero fedelmente i dati originali ciò potrebbe portare ad *output* errati o nuovamente discriminatori, finendo dunque per essere inutili allo scopo. Si pensi per esempio al settore medico, dove evidentemente è necessario l'utilizzo di dati che siano espressione, e "fedele" riproduzione, di attributi determinati. La manipolazione di dati reali mediante tecniche di AI potrebbe comportare il concreto rischio di perdita di alcuni attributi indispensabili all'indagine medica, rendendo i *data* così "creati" non più idonei allo scopo per cui sono stati inizialmente raccolti, e comportando di conseguenza risultati errati di quelle AI su di questi addestrate.

A fronte della molteplicità degli scopi di utilizzo, come si è già avuto modo di evidenziare, è allora necessaria una attenta determinazione di specifici attributi che permettano di raccogliere dati che siano al contempo di qualità e utili allo scopo per cui dovranno essere utilizzati.

La predisposizione di criteri unitari a tutti i settori mal si concilierebbe con le singole specifiche esigenze; si pensi per esempio all'utilizzo di informazioni per finalità statistiche legate a un determinato fenomeno in un arco temporale definito, se fosse previsto un generale obbligo di aggiornamento ciò comporterebbe la perdita di utilità per quei trattamenti storico-statistici.

European General Data Protection Regulation on Blockchains, in *R3 Reports*, 2017, 10.

[47] . Una definizione è presente nel documento emanato dall'OCSE nel 2007, "Glossario dei termini statistici", ove si precisa come il termine sia espressivo di un approccio «*to confidentiality where instead of disseminating real data, synthetic data that have been generated from one or more population models are released*», OECD, *Glossary Of Statistical Terms*, 2007, 768. Per un approfondimento tecnico sulla creazione e l'utilizzo di dati sintetici si rimanda a S.I. Nikolenko, *Synthetic Data for Deep Learning*, Berlino, 2021, 139 ss. e 269 ss.

[48] Cfr. *supra*, nota 25.

7. Considerazioni conclusive

Le applicazioni di intelligenza artificiale aprono a grandi sfide non solamente per gli scienziati intenti a potenziare la tecnologia, nell'intento di semplificare e migliorare la quotidianità così da arrivare a nuove soluzioni che promettono grandi prospettive economiche e di inclusione sociale. Anche i giuristi sono chiamati a rispondere alle criticità che inevitabilmente la diffusione delle tecnologie *disruptive* portano con sé.
Come visto accanto agli indubitabili vantaggi, l'opacità dei sistemi di AI fa emergere la necessità di un approccio rivolto a limitare *ab origine* le possibili esternalità negative che potrebbero comportare la diffusione di danni nei confronti di un numero potenzialmente molto esteso di utenti.
Se il progresso tecnologico appare difficile da arrestare, allora una particolare attenzione dovrebbe porsi alla progettazione e all'addestramento dei sistemi, seguendo così un principio di precauzione.
Tra le possibili soluzioni dirette a rendere le applicazioni di AI sicure ed affidabili un ruolo di rilievo assume l'utilizzo di dati di qualità. Come visto, difatti, dette tecnologie sono fortemente influenzate dai dati, trattandosi di applicazioni cc.dd. *data driven*, che dunque si "nutrono" di *data*, processandoli e facendo emergere ricorrenze statistiche alla base dei propri *output* decisori.
Ne discende il concreto rischio che le decisioni algoritmiche possano rivelarsi errate o discriminatorie, potendo queste essere espressione di *bias* che emergono da dataset, quali quelli oggi utilizzati, su cui non viene compiuta alcuna limitazione né in termini di quantità che di qualità dei dati raccolti. Pertanto se i dati raccolti e trattati sono "esatti", nell'accezione di corretti e aggiornati, e la stessa filiera di trattamento fin dalla fase di progettazione risulta affidabile, ne discende con tutta evidenza come ciò possa limitare in concreto il rischio *output* errati o discriminatori.
In questo dunque la previsione di un principio di esattezza che debba necessariamente informare ogni attività di raccolta e trattamento fin dall'origine mostra tutta la sua centralità, pur dovendo questo essere implementato mediante indicazioni operative maggiormente specifiche; potendo dunque trovare spazio codici di condotta o standard che permettano di uniformare e guidare coloro che operano nella filiera dei dati verso una possibile implementazione *by design* dei principi individuati dalla normativa europea.
Oltre ai necessari interventi normativi, di cui il principio di esattezza previsto dal GDPR rappresenta una tra le più importanti espressioni, un ruolo di rilievo dovrebbero rivestire standard tecnici, oltre che le stesse tecnologie di AI; mostrando in questo la loro anima duale. Le difficoltà legate alla quantità e alla varietà dei dati da controllere potrebbero, infatti, essere superate proprio grazie all'utilizzo delle tecnologie di Intelligenza Artificiale in grado di compiere in tempi ristretti un controllo e una verifica delle informazioni secondo criteri definiti[49].
A fronte di una realtà in continua evoluzione proprio la tecnica e la ricerca scientifica potrebbero rivelarsi strumenti preziosi nell'implementazione dei principi giuridici a tutela degli individui. Una regolazione efficace del fenomeno digitale oggi non può

[49] L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale*, cit., 40 ss.

dunque prescindere dalla considerazione per cui accanto al ruolo necessariamente centrale che deve continuare a rivestire la normazione primaria la tecnologia è chiamata a divenire essa stessa uno strumento elettivo a sostegno del legislatore nella tutela dei diritti.

Elenco autori

Maria Romana Allegri
professoressa associata di istituzioni di diritto pubblico, Sapienza - Università di Roma
Andrea Buratti
professore ordinario di diritto pubblico comparato, Università degli Studi di Roma "Tor Vergata"
Liliana Ciliberti
esperta di copyright e di regolamentazione dei media e delle comunicazioni elettroniche
Ylenia Maria Citino
assegnista di ricerca di istituzioni di diritto pubblico, LUISS Guido Carli
Caterina Di Costanzo
assegnista di ricerca di diritto costituzionale, Università degli Studi di Firenze
Filippo Donati
professore ordinario di diritto costituzionale, Università degli Studi di Firenze
Andrea Fedi
avvocato in Roma
Filippo Luigi Giambrone
ricercatore di diritto tributario, Università degli Studi del Sannio
Federica Giovanella
professoressa associata di diritto privato comparato, Università degli Studi di Udine
Carloalberto Giusti
professore ordinario di diritto privato comparato, Link University
Ottavio Grandinetti
avvocato in Roma
Simone Lonati
professore associato di diritto processuale penale, Università Bocconi
Valerio Lubello
avvocato in Milano
Angela Mendola
docente a contratto di diritto privato, Università degli studi di Salerno
Daniela Messina
docente a contratto di diritto dell'informazione e dell'informatica, Università degli Studi di Napoli "Parthenope"
Matteo Monti
assegnista di ricerca di diritto pubblico comparato, LUISS Guido Carli
Cristina Evanghelia Papadimitriu
ricercatrice di diritto dell'economia, Università degli Studi di Messina
Maria Pia Peluso
dottoranda di ricerca, Università degli Studi di Roma "Tor Vergata"
Ludovica Paseri
assegnista di ricerca di diritto amministrativo, Università degli Studi di Torino
Cesare Pinelli
professore ordinario di istituzioni di diritto pubblico, Sapienza - Università di Roma
Alberto Randazzo
professore associato di istituzioni di diritto pubblico, Università degli Studi di Messina
Marco Ventoruzzo
professore ordinario di diritto commerciale, Università Bocconi
Vincenzo Zeno Zencovich
professore ordinario di diritto privato comparato, Università degli Studi Roma Tre

CODICE ETICO

La **Rivista di diritto dei media** intende garantire la qualità dei contributi scientifici ivi pubblicati. A questo scopo, la direzione, il Comitato degli esperti per la valutazione e gli autori devono agire nel rispetto degli standard internazionali editoriali di carattere etico.

Autori: in sede di invio di un contributo, gli autori sono tenuti a fornire ogni informazione richiesta in base alla policy relativa alle submissions. Fornire informazioni fraudolente o dolosamente false o inesatte costituisce un comportamento contrario a etica. Gli autori garantiscono che i contributi costituiscono interamente opere originali, dando adeguatamente conto dei casi in cui il lavoro o i lavori di terzi sia/siano stati utilizzati. Qualsiasi forma di plagio deve ritenersi inaccettabile. Costituisce parimenti una condotta contraria a etica, oltre che una violazione della policy relativa alle submission, l'invio concomitante dello stesso manoscritto ad altre riviste. Eventuali co-autori devono essere al corrente della submission e approvare la versione finale del contributo prima della sua pubblicazione. Le rassegne di dottrina e giurisprudenza devono dare esaustivamente e accuratamente conto dello stato dell'arte.

Direzione: la direzione (ivi compresi direttori e vice-direttori) si impegna a effettuare la selezione dei contributi esclusivamente in base al relativo valore scientifico. I membri della direzione (ivi compresi direttori e vice-direttori) non potranno fare uso di alcuna delle informazioni acquisite per effetto del loro ruolo in assenza di un'esplicita autorizzazione da parte dell'autore o degli autori. La direzione è tenuta ad attivarsi prontamente nel caso qualsiasi questione etica sia portata alla sua attenzione o emerga in relazione a un contributo inviato per la valutazione ovvero pubblicato.

Comitato degli esperti della valutazione: i contributi sottoposti a valutazione costituiscono documentazione a carattere confidenziale per l'intera durata del processo. Le informazioni o idee acquisite confidenzialmente dai valutatori per effetto del processo di revisione non possono pertanto essere utilizzate per conseguire un vantaggio personale. Le valutazioni devono essere effettuate con profondità di analisi, fornendo commenti e suggerimenti che consentano agli autori di migliorare la qualità delle loro ricerche e dei rispettivi contributi. I revisori dovranno astenersi dal prendere in carico la valutazione di contributi relativi ad argomenti o questioni con i quali sono privi di familiarità e dovranno rispettare la tempistica del processo di valutazione. I revisori dovranno informare la direzione ed evitare di procedere alla valutazione nel caso di conflitto di interessi, derivante per esempio dall'esistenza di perduranti rapporti professionali con l'autore o la relativa istituzione accademica di affiliazione.

mediaLAWS

ANNO 2022 - CODICE ISSN 2532-9146