SECONDA EDIZIONE DEL SEMINARIO INTERNAZIONALE DI DIRITTO COMPARATO
«DIRITTO E NUOVE TECNOLOGIE TRA COMPARAZIONE E INTERDISCIPLINARITÀ»
- IN MEMORIA DEL PROF. PAOLO CARROZZA -

INTELLIGENZA ARTIFICIALE E DISCRIMINAZIONE: QUALI PROSPETTIVE? IL MODELLO INGLESE DEL DATA TRUST

ENRICO MANTOVANI

SOMMARIO: 1. Introduzione. – 2. Intelligenza artificiale e dati. – 3. Intelligenza artificiale e discriminazione. – 4. Criticità degli attuali strumenti di tutela. – 5. Il *Data Trust*. – 6. Conclusioni

1. *Introduzione*

Il presente contributo si inserisce nel dibattito relativo al rapporto tra intelligenza artificiale (*IA*) e protezione dei dati personali occupandosi di indagare le modalità più adeguate a garantire un elevato standard di tutela dei diritti fondamentali, senza per ciò compromettere lo sviluppo delle tecnologie di IA. In particolare, sembra necessario riflettere sulla necessità di assicurare un modello di sviluppo e applicazione di tale tecnologia coerente e rispettoso dei principi costituzionali, con specifico riferimento al principio di uguaglianza e non discriminazione di cui all'art. 3, primo comma, della Costituzione – che trova ampia tutela anche nel diritto dell'Unione Europea[1]. Lo sviluppo dell'IA, costituirà certamente uno degli elementi più dirompenti con cui la scienza

[1] Il riferimento normativo principe è certamente l'art. 21 della Carta dei diritti fondamentali dell'Unione Europea, ma la legislazione secondaria è particolarmente vasta e di enorme rilievo applicativo. In dottrina, con riferimento al diritto comunitario, si veda per tutti M. BELL, *Anti-Discrimination and the European Union*, Oxford University Press, Oxford, 2002 e, per l'Italia, M. BARBERA (a cura di*), Il nuovo diritto antidiscriminatorio*, Milano, 2007.

giuridica dovrà confrontarsi nel prossimo futuro, anche, e forse soprattutto, in relazione alla minaccia posta alla tutela dei diritti individuali: il rapporto tra decisione automatizzata, IA e *privacy* pone sfide su molteplici piani, idonee ad alterare in modo significativo il rapporto tra potere ed individuo, si pensi, ad esempio, al tema della sorveglianza, dell'autodeterminazione individuale, e appunto della discriminazione. Dall'altro lato, le enormi potenzialità insite nello strumento in discorso, come confermato anche nel corso della crisi pandemica, non consentono irrealistiche e riduttive soluzioni volte a impedirne lo sviluppo e la diffusione. È invece necessario individuare strumenti, prima regolatori e poi tecnici, funzionali a garantire uno sviluppo e un'applicazione dell'IA conforme ai valori e ai principi costituzionali, fugando il rischio di un pericoloso predominio da parte dei poteri privati[2] idoneo a consolidare le logiche del «capitalismo della sorveglianza»[3]. Ad oggi, i principali documenti programmatici che interessano la materia dell'IA, con riferimento a quelli adottati dall'Unione Europea[4] e dal Regno Unito[5], opportunamente già stabiliscono come obiettivo primario la realizzazione di un IA conforme a principi etici condivisi, con particolare riferimento alla realizzazione di un'IA sicura, affidabile e capace di generare fiducia tra gli utenti; particolare enfasi è stata dunque posta, specialmente nel diritto comunitario[6], sulla necessità di prevenire discriminazioni arbitrarie e di assicurare la tutela dei dati personali coinvolti. Di particolare interesse dunque appare l'indagine sulla stretta relazione intercorrente tra la tutela dei dati personali e la prevenzione di decisioni discriminatorie da parte dell'IA e, a tal fine, si procederà sinteticamente ad una disamina del rapporto tra dati personali, intelligenza artificiale e discriminazione, alla valutazione dell'adeguatezza degli attuali strumenti normativi, e infine, alla valutazione di alcune proposte avanzate nel Regno Unito sul tema in esame.

[2] M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in *Rivista Gruppo di Pisa*, 2, 2021.

[3] S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss, 2019.

[4] Si pensi alla Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale, relativo alle *Questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale*), all'*Assessment List on Trustworthy Artificial Intelligence* (ALTAI) (17 luglio 2020) predisposto dal Gruppo Indipendente di esperti di Alto Livello sull'IA, istituito dalla Commissione Europea, al Libro Bianco sull'Intelligenza Artificiale della Commissione (19 febbraio 2020), agli Orientamenti etici per un'IA affidabile (9 aprile 2019) e alla la Strategia europea sull'Intelligenza artificiale (aprile 2018). Per l'Italia, il punto di riferimento è il Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino pubblicato dall'Agenzia per l'Italia Digitale (AGID) nel marzo 2018.

[5] Cfr. Rapporto del Comitato della *House of Lords* sull'IA (dicembre 2020), alla risposta ufficiale a tale rapporto da parte del Governo inglese (febbraio 2021) e all'*AI Roadmap* pubblicata dall'*AI Council* (gennaio 2020).

[6] I sette pilastri fondamentali previsti negli Orientamenti etici per un'IA affidabile (del 9 aprile 2019) sono: 1) intervento e sorveglianza umani, 2) robustezza tecnica e sicurezza, 3) riservatezza e governance dei dati, 4) trasparenza, 5) diversità, non discriminazione ed equità, 6) benessere sociale e ambientale e 7) accountability. In generale, per una riflessione sulle implicazioni etiche legate allo sviluppo e all'impiego dell'IA, J. KAPLAN, *Artificial Intelligence. What Everyone Needs to Know*, Oxford University Press, 2016 e per la dottrina italiana, A. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi Giuridica dell'Economia*, 2019, 47 e ss.

2. *Intelligenza artificiale e dati*

Come anticipato, il tema della regolamentazione dell'IA, si interseca significativamente con la dimensione dei c.d. *Big Data*, e sebbene questa relazione possa essere esplorata sotto diversi profili[7]– ciascuno dei quali fondamentale per addivenire ad un'efficace regolamentazione – in questa sede si approfondiranno quelli legati al rischio di discriminazioni arbitrarie in relazione all'impiego di dati personali degli utenti, tralasciando gli aspetti concernenti i dati non personali[8]. È senz'altro noto che proprio la disponibilità e l'utilizzo di una amplissima quantità di dati rende possibile l'apprendimento automatico e l'elaborazione di meccanismi predittivi efficaci, con la conseguenza che tanto maggiore sarà la mole di dati messa a disposizione per alimentare il sistema di *machine learning*, tanto maggiore risulterà la capacità di apprendimento del sistema, nonché la sua affidabilità e precisone; si parla in proposito di una tecnologia «*Data Intensive*»[9]. A tal proposito, pare opportuno soffermarsi, nonostante l'assenza di un'univoca nozione, sulla definizione di IA avanzata dal Gruppo Indipendente di esperti di Alto Livello nominati dalla Commissione Europea che fa riferimento appunto al processo di acquisizione ed analisi dei dati raccolti quale elemento strutturale della tecnologia in discorso, riferendosi a «*sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulle conoscenze, o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato*»[10]. Invero, pur non potendo ignorare la complessità definitoria diffusamente analizzata da recente dottrina[11], per tutti i sistemi di IA, ma specialmente per i sistemi sub-simbolici[12], non può tralasciarsi l'importanza dell'impatto

[7] Si pensi ai rilevanti risvolti sul piano del diritto della concorrenza, per tutti G. BELLITTI, *Big Data e Abuso di Posizione Dominante*, in *Diritto Antitrust*, A. CATRICALÀ, E. CAZZATO e F. FIMMANÒ (a cura di), 2021, p. 472 e ss. Da ultimo, G. SCHNEIDER, *Data sharing for collaborative research under art. 101 TFEU: lessons from the proposed regulations for data markets* in *European Competition Journal,* 2021.

[8] Per fare un esempio dei primi, si pensi alle informazioni relative alla storia creditizia, alle propensioni di acquisto di un consumatore, oppure alle informazioni relative alla salute o alle preferenze politiche di un lavoratore e, per i secondi, le informazioni relative allo stato funzionale di un veicolo intelligente (chilometri percorsi, anomalie rilevate, strade attraversate, etc.), agli elettrodomestici interconnessi, oppure le informazioni prodotte dal settore pubblico (informazioni catastali, cartografiche, meteorologiche, etc). Cfr. G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza,* in *Politica Del Diritto*, 2019, 199-236.

[9] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1/2019, 102.

[10] High-Level Expert Group On Artificial Intelligence, *Una definizione di IA: principali capacità e discipline*, Bruxelles, 8 aprile 2019, 6.

[11] Per la dottrina italiana, il riferimento sono C. COLAPIETRO, A. MORETTI, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *Rivista di BioDiritto*, 2020, 365 e ss. e C. NARDOCCI, *Intelligenza Artificiale e Discriminazioni*, Relazione al Convegno annuale dell'associazione "Gruppo di Pisa" (Versione provvisoria). Per la dottrina straniera, K. FRANKISH, W. M. RAMSEY (a cura di), *The Cambridge Handbook of Artificial Intelligence*, Cambridge University Press, Cambridge, 2014, 89.

[12] La distinzione tracciata tra sistemi simbolici e sub-simbolici fa riferimento alla logica sottesa al sistema di IA per cui, nel primo caso, esso opera sulla base di regole logiche-deduttive predeterminate dal

che i dati hanno per il loro funzionamento e per le decisioni assunte. Ancora più rilevante, tuttavia, risulta l'incidenza nella fase di apprendimento, per quei sistemi definiti c.d. *learning* (e.g. *deep learning*) già oggi, ad esempio, i principali sistemi di IA vengono continuamente "addestrati" sfruttando l'amplissima quantità di dati prodotti su internet, ovvero *data-sets* più specifici, come nel caso della ricerca medica avviene mediante banche dati informatiche specializzate[13]. Nel dibattito più recente, sono state opportunamente superate le iniziali perplessità relative alla questione della potenzialità discriminatorie insite nelle tecnologie di intelligenza artificiale, venendo rilevata l'inadeguatezza di una costruzione giuridica che muova dalla considerazione di una pretesa neutralità dello strumento tecnico al fine di cogliere la complessità dell'IA: è ormai chiaro che essa ben può produrre risultati inesatti, errati e, talora, appunto, perfino discriminatori[14], come emerso nell'ampia casistica esaminata dalla dottrina[15] e dai recenti casi che in Italia sono stati oggetto di intervento da parte della giurisprudenza di merito[16].

3. *Intelligenza artificiale e discriminazione*

La capacità di un sistema di IA di generare risultati corretti consegue irrimediabilmente a due fasi: (*i*) la fase programmazione e realizzazione del sistema e (*ii*) quella di apprendimento. In ciascuna di queste, possono introdursi, scientemente o inconsapevolmente, elementi tali da ingenerare risultati idonei a escludere o sotto rappresentare specifici gruppi: i pregiudizi del programmatore, la poca varietà – o ricchezza – dei dati considerati dall'algoritmo, sono tutti fattori che potenzialmente posso avere radicali effetti distorsivi. Per quanto riguarda la prima fase, si segnalano in particolare quei meccanismi relativi all'individuazione delle caratteristiche rilevanti per

programmatore, al contrario nel secondo caso, la macchina segue un approccio dal basso – rimanendo priva di regole predeterminate – procedendo all'analisi dei dati sottoposti secondo una logica correlativa. Cfr. C. COLAPIETRO, A. MORETTI, *L'Intelligenza Artificiale*, cit. e EUROPEAN PARLIAMENT, *Artificial intelligence: How does it work, why does it matter, and what can we do about it*?, EPRS-STOA, 2020, 2 ss. Si noti anche si stanno studiando sistemi misti che sfidando anche questa categorizzazione, sul punto, P. TRAVERSO, *Forum AI and Law*, in *Biolaw Journal*, 2020, n. 1, 480.

[13] P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, in *Consulta Online*, 16 marzo 2020.

[14] Per ampi riferimenti al tema e, in special modo, ai profili relativi all'applicazione delle normativa antidiscriminazione, si veda C. NARDOCCI, *Intelligenza Artificiale e Discriminazioni*, cit. Ulteriori riferimenti, più generali, in P. ZUDDAS *Intelligenza artificiale e discriminazioni,* Cit.; L. GIACOMELLI, *Big brother is «gendering» you. Il diritto antidiscriminatorio alla prova dell'intelligenza artificiale: quale tutela per il corpo digitale?*, in *BioLaw Journal*, 2019, 2, 269 ss.; M. FAVARETTO, E. DE CLERCQ, B. SIMONE ELGER, *Big data and discrimination: perils, promises and solutions. A systematic review*, in *Journal of Big Data*, 2019, 1 e ss.

[15] Cfr. A. HOFFMANN, *Where fairness fails: data, algorithms, and the limits of antidiscrimination discourse, Information*, in *Communication & Society*, 2019; J. GERARDS, R. XENIDIS, *Algorithmic discrimination in Europe : Challenges and opportunities for gender equality and non-discrimination law*, Publications Office of the European Union, 2020.

[16] Tribunale di Bologna, ordinanza del 31 dicembre 2020 (caso «Deliveroo»), su cui, per tutti, si rimanda a M. PERUZZI, *Il diritto antidiscriminatorio al test di intelligenza artificiale*, in *Labour & Law Issues*, 7(1), 2021, I.48-I.76 e Tribunale di Torino, sentenza n. 778 del 7 maggio 2018 (caso «Foodora»), su cui si veda, C. SALAZAR, *Diritti e algoritmi: la gig economy e il "caso Foodora", tra giudici e legislatore,* in *Consulta Online*, 2019, 143 e ss.

il sistema, dunque oggetto dell'indagine compiuta dalla macchina (*target variable*, *feature selection*) per la successiva associazione con una determinata categoria (*class label*). In questi casi, la questione è resa particolarmente complessa dalla possibile valutazione di elementi che solo indirettamente possono generare effetti discriminatori, si pensi ad esempio alle c.d. *proxy discriminations*, con la conseguenza che previsioni volte a vietare la considerazione di caratteristiche tradizionalmente legate a scelte discriminatorie (*e.g*. razza, sesso, orientamento sessuale) – come tra l'altro espressamente previsto dall'art. 22.4 del Regolamento (UE) 2016/679 (*GDPR*) – non sempre sono idonee a prevenire la costruzione di sistemi di IA portatori di risultati *biased*, data la possibile considerazione di elementi diversi da quelli vietati ma comunque idonei a discriminare specifici gruppi. Ancora più rilevante per i nostri fini risultano tuttavia i rischi insiti nella seconda fase, quella di apprendimento, in cui la macchina operando in modo, più o meno, autonomo si discosta dal modello iniziale e produce soluzioni al problema sottoposto, sulla base dell'analisi svolta. La logica correlativa di un sistema di IA potrebbe dunque procedere a identificare tra i dati analizzati correlazioni ritenute rilevanti, traendo dalla vastità delle interrelazioni presenti decisioni idonee a produrre esiti discriminatori. In particolare, straordinariamente complessi da affrontare sono le questioni legate alle decisioni discriminatorie generate all'interno della "*black box*" quindi autonomamente prodotte dal sistema di IA, al di fuori del controllo del soggetto programmatore e frutto di una logica non comprensibile da parte dell'uomo. Il rischio che tali sistemi individuino caratteristiche idonee a distinguere specifici gruppi, nonostante espressi divieti imposti in tal senso, secondo logiche che ripropongono schemi incorporati nei *data set* analizzati, può condurre nella riproduzione e spesso produzione di disparità economiche e sociali nella decisione algoritmica[17], senza che tale logica decisionale possa essere agevolmente ricostruita *ex post.* Il rischio è la possibile disparità nell'accesso a beni e servizi essenziali per certi gruppi svantaggiati e la contribuzione alla «creazione di invisibili», talora realizzando nuove forme di discriminazione impreviste ed imprevedibili[18], essendo di fatto il *proprium* dell'IA quello di discernere e distinguere (con il conseguente dovere per il giurista di interrogarsi su cosa costituisca una discriminazione illegittima[19]). In altri termini, risultati discriminatori possono conseguire, sia nel caso in cui i dati impiegati non siano adeguatamente rappresentavi della ricchezza del tessuto sociale analizzato – conducendo dunque ad una distorta e parziale comprensione della realtà – sia nel caso in cui si riproducano disparità effettivamente esistenti, con il rischio di una «invisibile produzione di invisibili».

L'analisi di dati parziali o compromessi, nella misura in cui favorisce la produzione o interiorizzazione di logiche discriminatorie, difficilmente può essere corretta efficacemente *ex post*, ad esempio mediante l'introduzione di correttivi; per questo è particolarmente importante identificare e rimuovere i potenziali *bias* già nella fase della

[17] R. XENIDIS, *Turning EU Equality Law to algorithmic discrimination: three pathways to resilience*, in *Maastricht Journal of European and Comparative Law*, 6, 2020.

[18] M. MANN, T. MATZNER, *Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination*, in *Big Data & Society*, 6, 2019.

[19] *Ibidem*. Si veda anche L. ALEXANDER, *What makes wrongful discrimination wrong? Biases, preferences, stereotypes, and proxies,* in *University of Pennsylvania Law Review*, 191, 1992.

raccolta dei dati, e dunque procedere all'acquisizione di un panorama informativo il più possibile ampio e completo, come ha ricordato da ultimo anche il gruppo di esperti nominato dalla Commissione Europea sull'IA[20]. La dottrina ha efficacemente parlato di una logica del *garbage in – garbage out*, per cui «*dati incongrui, inesatti o non aggiornati non possono che produrre risultati decisionali inaffidabili*»[21] con l'ulteriore precisazione che, con specifico riferimento ai sistemi di IA, l'introduzione di *Bad Data* nella fase di apprendimento non solo compromette l'esito del processo decisionale ma ne pregiudica lo strumento e dunque la sua capacità di apprendere, trasformando l'errore occasionale in errore sistematico[22].

4. *Criticità degli attuali strumenti di tutela*

Agli albori della rivoluzione digitale, era radicata l'idea per cui la promessa di libertà di internet potesse essere frustrata da tentativi di regolazione che ne minassero la natura spontanea, orizzontale e policentrica; si invocava – al contrario – l'avvento per autopoiesi di un'autoregolamentazione fondata, almeno nelle impostazioni iniziali, su regole puramente tecniche che fossero immuni dall'intervento statale[23]. Ad oggi, analoghi interrogativi si sono posti in merito all'opportunità di un intervento di regolazione in materia di IA, frapponendosi posizioni favorevoli ad un minimo intervento da parte dei soggetti pubblici, in favore dell'affermazione di un «*diritto spontaneo*»[24] in linea con la nota nozione di *lex informatica* avanzata da Lessig[25] avente natura di *co-regulation* con lo Stato – od altri attori pubblici – e di *self-regulation* dal basso o ancora di «costituzioni civili» secondo l'impostazione di Gunther Teubner[26], e opposte posizioni che evidenziano il rischio che un simile approccio di *de-regulation* possa rafforzare ulteriormente centri di potere privati la cui natura organizzata, opaca ed oligopolista, non sembra compatibile con i principi cardine del costituzionalismo e con la sua tradizionale missione di «*limitare il potere, pubblico o privato che sia*»[27].

Se dunque la necessità di un «*costituzionalismo digitale*»[28] si impone, le possibili modalità di attuazione sono numerose e complesse, così come l'individuazione del livello

[20] High-Level Expert Group on Artificial Intelligence*, The Assessment List for Trustworthy Artificial Intelligence*, 2020.

[21] G. RESTA, *Governare l'innovazione tecnologica*, cit.

[22] F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, 2018, 288.

[23] Per approfondimento si rinvia a M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, cit. e G. DE MINICO, *Fundamental Rights, European Digital Regulation and Algorithmic Challenge,* in *Media Laws,* 1/2021.

[24] T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Diritto dell'informatica*, 2020, 483.

[25] L. LESSIG, *Code*, Basic Books, 2006.

[26] G. TEUBNER, *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, Roma, Armando, 2005; G. TEUBNER, A. FEBBRAJO, *State, Law and Economy as autopoietic system. Regulation and autonomy in a new perspective*, Milano, 1992.

[27] T. GROPPI, *Alle frontiere dello Stato Costituzionale, Innovazione tecnologica e Intelligenza Artificiale*, in *Consulta Online*, 3, 2020, 681.

[28] Da ultimo, si veda la recente ricostruzione di G. DE GREGORIO, *The rise of digital constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 19/1, 2020, 41-70.

più adeguato di regolazione e dei soggetti istituzionali deputati ad intervenire. A tal proposito, si rileva come l'Unione Europea abbia opportunamente deciso di agire e, nelle more dell'adozione di uno strumento di compiuta regolazione dell'IA[29], le principali disposizioni sulla materia si rinvengono nel GDPR, a testimonianza della stretta connessione tra *privacy* ed IA. Senza alcuna pretesa di completezza, si nota che, come rilevato anche da larga parte della dottrina[30], le tutele garantite all'individuo soggetto a decisioni automatizzate da tali disposizioni, ed in particolare, dagli artt. 15 e 22 del GDPR, non sembrano ancora sufficienti ad assicurare un adeguato livello di garanzia. In particolare, pur ammettendo il riconoscimento di un vero e proprio «diritto alla spiegazione dell'algoritmo», in luogo di un più limitato diritto di accesso alle informazioni relative al funzionamento dello stesso, esso sembra di difficile conciliazione, sia con le già segnalate difficoltà in termini di spiegabilità e comprensibilità della logica algoritmica, sia con l'elevata complessità tecnica della materia. In altri termini, sembra ragionevole dubitare che i meccanismi informativi così disegnati siano idonei a consentire all'individuo di "aprire la black-box*"* o di comprendere cosa vi sia all'interno. Allo stesso tempo, il divieto di essere sottoposti a decisioni esclusivamente automatizzate, si scontra con la possibilità di aggirare la previsione – introducendo *a human-in-the-loop* – e con le numerose eccezioni a cui il divieto è soggetto, tra cui l'avvenuta prestazione del consenso dell'interessato[31]. Il tema del rischio di discriminazione è poi solo marginalmente trattato dal GDPR (al Considerando 71) in una disposizione assolutamente generica e di dubbia efficacia[32]. In sintesi, il GDPR, nonostante il significativo progresso rispetto alla Direttiva 95/46/CE[33], stabilisce un sistema di garanzie ancora inadeguato a reagire alle complessità dell'IA anche in ragione di una tutela di natura eminentemente individuale che sembra ormai inadeguata a salvaguardare anche quella dimensione istituzionale che appare quanto mai

[29] Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) COM/2021/206 del 21 aprile 2021.

[30] Cfr. L. EDWARDS, M. VEALE, *Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for*, in *Duke Law & Technology Review*, 16, 2017; S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*, in *International Data Privacy Law,* 2/2017; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, 79 e ss.

[31] Sono notissime le critiche mosse all'effettività del consenso prestato per servizi resi su internet, ambito in cui le informative sono lunghe decine di pagine e raramente sono oggetto di grande attenzione da parte dell'utente, tuttavia, ancora più rilevante, sembra essere la scarsità di opzioni a disposizione del soggetto che, davanti alle richieste di consenso, spesso ha una sola alternativa, accettare o non usufruire del servizio offerto. Muovendo proprio da questa valutazione l'Autorità tedesca garante per la concorrenza (Bundeskartellamt, 2019) ha ritenuto che Facebook avesse commesso un abuso di posizione dominante nella misura in cui subordinava l'accesso ai suoi prodotti all'accettazione da parte dell'utente di penetranti meccanismi di raccolta dati e profilazione, sottolineando che: "*There is no effective consent to the users' information being collected if their consent is a prerequisite for using the Facebook service in the first place*". Cfr.E. BIETTI, *The Discourse of Consent and Control over Data in EU Data Protection Law and Beyond*, in *Aegis Paper Series*, 2020.

[32] C. NARDOCCI, *Intelligenza Artificiale e Discriminazioni*, cit., 62.

[33] Si pensi al nuovo rilievo attribuito all'*accountability* del titolare del trattamento, alle previsioni sulla valutazione di impatto (art. 35) e l'importante disposizione sul principio della *privacy by design* (art.25).

opportuno riconoscere al diritto all'autodeterminazione informativa[34]; riconoscendo quindi tale diritto non solamente nella sua dimensione negativa volta a salvaguardare l'interesse di uno specifico individuo ma quale uno dei valori fondamentale per l'intera società digitale. Non solo il rischio di una discriminazione sistemica, di cui *supra*, investe potenzialmente l'intero gruppo sociale oggetto di discriminazione, ma la stessa tutela degli interessati al trattamento dei dati oggetto della fase di *learning* non può limitarsi – anche in ragione dell'evidente squilibrio nei rapporti di forza con i potenti attori privati che dominano il settore – ad un rapporto bilaterale con l'operatore che opera il trattamento. È quindi opportuno muovere dal riconoscimento di una sfera di tutela collettiva[35], correlata a meccanismi di tutela istituzionalizzata, tra cui, naturalmente, *in primis*, il Garante per la protezione dei dati personali, tali da offrire efficaci strumenti per incidere sulla costruzione di macchine conformi ai valori di trasparenza, rispetto della *privacy*, dignità umana e non discriminazione, intervenendo sia nella loro fase genetica di programmazione che in quella successiva di raccolta dei dati necessari per il loro funzionamento.

5. *Il Data Trust*

Al fine di elaborare strumenti di tutela dei diritti efficaci, ed idonei a prevenire il rischio che *bias* acquisiti nel corso della fase di apprendimento possano indurre un'IA ad assumere autonomamente decisioni discriminatorie, occorre dunque identificare un soggetto quale responsabile più idoneo ad assicurare una raccolta dei dati – funzionale ai processi di *machine learning* – in linea con i requisiti di qualità e diversificazione necessari. Se l'inadeguatezza del ricorso all'autoregolamentazione dei produttori di sistemi di intelligenza artificiale è già stata sottolineata, occorre evidenziare anche l'inopportunità di attribuire a tali soggetti la responsabilità di provvedere ad una raccolta dei dati «etica», finanche temperata da una vigilanza pubblica (e.g. mediante codici di condotta, certificazioni, etc.). A ragioni di carattere pratico, relative all'evidente conflitto di interesse in cui verserebbe un soggetto chiamato a controllare se stesso, si sommano considerazioni di carattere teorico legate all'opportunità di riconoscere anche in una fase preliminare, e forse specialmente in questa – in considerazione di quanto si è argomentato sopra – un ruolo all'individuo-utente, il quale oltre ad essere l'interessato del trattamento dei dati personali potrebbe essere anche oggetto dalle future decisioni della macchina. La rilevata esigenza di assicurare un efficace strumento di tutela collettiva e la necessità di ispirare una diffusa fiducia (*trust*) nei sistemi di IA hanno condizionato l'elaborazione di alcuni istituti nell'ordinamento inglese che, sebbene ad una prima analisi appaiano per

[34] Nello stesso senso, G. DE MINICO, *Fundamental Rights, European Digital Regulation And Algorithmic Challenge*, cit., 29.

[35] Cfr. B. CARAVITA, *Principi costituzionali e intelligenza artificiale*, in U. RUFFOLO (a cura di), *Intelligenza artificiale*, cit., 451 ss; A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma,* cit; G. RESTA, *Governare l'innovazione tecnologica*, cit; C. COLAPIETRO, A. MORETTI., *L'Intelligenza Artificiale nel dettato costituzionale,* cit.. Si è parlato anche di *privacy* collettiva o di gruppo, cfr. M. LOI, M. CHRISTEN, *Two Concepts of Group Privacy*, in *Philosophy & Technology*, 33/2020, 207–224.

certi versi lontani dalla prospettiva assiologica e culturale italiana dell'Unione Europea, possono offrire un'importante occasione di comparazione. Sebbene la proposta britannica in materia di IA sia ancora in fase di elaborazione, sono già disponibili diversi documenti preparatori e programmatici tra cui, recentemente, una comunicazione del Governo Inglese all'*House of Lords Select Committee on Artificial Intelligence*[36], da cui emerge l'attenzione riservata all'innovativo istituto dei *data trusts*, la cui importanza è confermata anche dal gruppo di esperti (*Report Hall-Pesenti*)[37] che nel 2017 ha posto le basi per l'elaborazione della strategia inglese, identificando i *data trusts* come la più importante tra le misure da implementare[38].

Tale istituto è funzionale ad assicurare la realizzazione, sin dalla fase di sviluppo e apprendimento dell'IA, di sistemi in linea con principi etici condivisi così da assicurare un elevato livello di tutela dei diritti fondamentali a partire da quello della protezione dei dati personali e di tutela da possibili risultati discriminatori[39]. Il Regno Unito dunque è orientato a raggiungere tali obiettivi, che nei loro tratti principali sono sovrapponibili a quelli stabiliti a livello europeo[40], focalizzando l'attenzione sui temi della *data governance* in relazione ai processi di IA: particolare attenzione è dunque posta alle modalità di gestione e selezione dei dati impiegati nelle fasi di *machine learning*, ricorrendo ad innovativi istituti – di chiara matrice privatistica e fondati su una concezione patrimoniale del rapporto individuo e dato personale – quali appunto i *data trusts*, i contratti e le *data cooperatives*[41]. L'istituto del *data trust*[42]– che riproduce, sebbene con diverse differenze rispetto all'istituto tradizionale, lo schema del *trust* di diritto inglese – comporta la costituzione di un soggetto giuridico da parte di un gruppo di utenti che mette a disposizione i propri dati personali, assumendo le vesti sia di disponente del *trust* che di beneficiario degli obblighi fiduciari[43] verso gli amministratori, i quali saranno chiamati a gestire i dati personali conferiti, ed esercitare i diritti

[36] *Government Response to the House of Lords Select Committee on Artificial Intelligence*, Febbraio 2021, disponibile al sito.

[37] D. W. HALL, J. PESENTI, *Growing the artificial intelligence industry in the UK,* 2017. Si veda poi, il Working group ADA Lovelance Institute, *Final Report* on *Exploring legal mechanisms for data stewardship*, marzo 2021, disponibile al seguente link: https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/

[38] UK House of Lords, *AI in the UK: No Room for Complacency*, 2020, 13; secondo cui "*The Hall-Pesenti Review made 18 recommendations on how to make the UK the best place in the world for businesses developing AI. Professor Hall told us that they "made data trusts the first recommendation in our review*."

[39] In questo senso, si veda, Working group ADA Lovelance Institute*, Final Report* on *Exploring legal mechanisms for data stewardship,* 32.

[40] *Una Strategia europea per i dati,* COM (2020) 66 FINAL, 19.02.2020.

[41] In questa sede non si approfondiranno tali due ultimi istituiti, basti solo considerare che i primi sono contratti standardizzati per la cessione di dati e i secondi sono associazioni di utenti funzionali ad un esercizio collettivo dei diritti spettanti agli interessati.

[42] Sulla tematica del *data trust*, J. LAU, J. PENNER, B. WONG, *The Basics of Private And Public Data Trusts*, in *NUS Law Working Paper Series*, 19, 2019. BPE Solicitors, Pinsent Masons & Chris Reed, *Data trusts: legal and governance considerations*, Open Data Institute, 2019, disponible online al link: https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf; S. DELACROIX, N. LAWRENCE, *Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance*, in *International Data Privacy Law*, 2019, 9-4.

[43] Per una compiuta ricostruzione della disciplina dei Trusts nel diritto inglese, il riferimento per la dottrina italiana è M. LUPOI, *Trusts*, 2001.

corrispondenti, secondo la diligenza che ispira tradizionalmente l'istituto, con il fine di curare gli interessi degli utenti nei confronti dei fornitori o produttori di sistemi di IA a cui i dati raccolti potranno essere ceduti, eventualmente dietro corrispettivo. Al di là dell'esatta corrispondenza del modello proposto con lo schema tradizionale del *trust* inglese, stante l'assenza di un vincolo di irrevocabilità, che invece caratterizza il modello tradizionale, e la mancanza di una netta indipendenza degli amministratori rispetto ai disponenti, l'elemento centrale della proposta è la decisione di interporre tra i fornitori di dati personali e i gestori di sistemi di IA, dei soggetti giuridici nuovi, preposti alla cura dei diritti e degli interessi dei primi, sulla base di solidi vincoli fiduciari che, nell'ordinamento inglese, sono considerati più efficaci di un modello di responsabilità extracontrattuale o contrattuale. L'elaborazione dell'istituto in commento risale alla metà del 2015[44], per poi venire ripreso dal Report Hall-Pesenti nel 2017, dalle proposte di regolazione del Governo inglese e dal report del 2021 dell'*Ada Lovelace Institute* (*Report ADA 2021*), tuttavia anche in precedenza si rintracciano diversi contributi da parte della dottrina anglosassone interessata a verificare la possibilità di costruire forme aggregate di gestione e tutela collettiva dei dati personali[45]. Più precisamente, l'utilizzo del termine *trust* avveniva spesso in modo atecnico riferendosi talvolta alla nomina di un rappresentante comune degli interessi degli utenti vincolato da obblighi fiduciari (c.d. *data stewardship*), lo stesso Report Hall-Pesenti fa riferimento alla nozione di *data trust* come "*not a legal entity or institution, but rather a set of relationships underpinned by a repeatable framework, compliant with parties' obligations, to share data in a fair, safe and equitable way*[46]". In particolare, uno dei punti controversi più rilevanti circa l'ammissibilità di un *data trust*[47] verteva sulla effettiva possibilità di ammettere la sussistenza di un vero e proprio diritto di proprietà da parte dell'interessato sui dati personali che, in ossequio allo schema tradizionale, avrebbero dovuto costituire l'oggetto del conferimento, formando dunque, come sopra si è provato ad illustrare, il patrimonio comune che i *trustee* sarebbero poi chiamati ad amministrare[48]. Nonostante l'ampiezza del dibattito, dalle radici molto profonde, le più recenti proposte ricostruttive hanno superato la questione della sussistenza o meno di un diritto di proprietà da parte dell'interessato sui dati ceduti, ipotizzando il conferimento[49] dei diritti soggettivi vantati

[44] J. LAU, J. PENNER, B. WONG, *The Basics Of Private And Public Data Trusts*, in *NUS Law Working Paper Series,* cit. e S. DELACROIX, N. LAWRENCE, *Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance,* cit., con riferimento ad una pubblicazione di N. LAWRENCE, *Data trusts could allay our privacy fears*, in *The Guardian Media & Tech Network*, 2016 disponibile al link, https://www.theguardian.com/media-network/ 2016/jun/03/data-trusts-privacy-fears-feudalism-democracy.

[45] Per tutti, L. EDWARDS, *The Problem with privacy*, in *International Review of Law Computers & Technology,* 18, 2004.

[46] D. W. HALL, J. PESENTI, *Growing the artificial intelligence industry in the UK,* 46.

[47] Tale rilievo è contenuto, a titolo esemplificativo, nel Report dell'Open Data Institute, *Data trusts: legal and governance considerations* del 2019.

[48] Per un'efficace sintesi del dibattito si rinvia a B. MCFARLANE, *Data Trusts and Defining property*, disponibile al seguente link: tps://www.law.ox.ac.uk/research-and-subject-groups/property-law/blog/2019/10/data-trusts-and-defining-property.

[49] Naturalmente, le modalità di conferimento non possono non considerare i vincoli attualmente imposti dal GDPR, e in particolare dall'art. 80, e dall'analoga legge inglese (il c.d. *UK Data Protection Act* del 2018) in tema di trasferibilità dei diritti ivi riconosciuti. Per riferimenti in questo senso, e sulle proposte avanzate per utilizzare le specificità dell'istituto del *trust* per aggirare tali limitazioni,si rimanda alla relativa

dagli interessati sui propri dati ad una organizzazione, il *trust*, che li eserciti in loro nome e per loro conto[50].

Il Report ADA 2021 affronta diffusamente le possibili forme e modalità di costituzione dei *trusts*, ammettendo l'instaurazione di forme di collaborazione con soggetti dotati di particolare competenza tecnica e indipendenza (e.g. associazioni, centri di ricerca, imprese, etc.) e ipotizzando la formazione di un mercato competitivo, in cui l'utente possa scegliere tra i diversi *trusts* quello più adeguato alle proprie esigenze, mantenendo sempre la facoltà di recedere dal rapporto così instaurato. Sarebbero dunque questi soggetti giuridici a occuparsi della raccolta, selezione, anonimizzazione, pseudonomizzazione dei dati degli aderenti/beneficiari, nonché a intrattenere rapporti con i terzi interessati alla acquisizione di tali dati, ad esempio per il funzionamento di sistemi di IA, sfruttando la "forza negoziale" aggregata delle molteplici posizioni individuali di cui sono portatori. Il *trust* sarebbe dunque responsabile che la raccolta dei dati, avvenuta su base volontaria secondo il meccanismo del conferimento al *trust*, comporti trattamenti dei dati personali in linea con le volontà degli utenti, e costituisca un *set* di dati affidabile per lo specifico trattamento a cui dovranno essere devoluti, facendosi dunque garante della correttezza, completezza e varietà dei dati raccolti, senza per questo esimere da responsabilità l'IA, i cui produttori saranno comunque tenuti ad adottare tutte le misure necessarie per evitare esiti discriminatori. Questo aspetto dell'istituto costituisce un importante risposta al problema della discriminazione, esso infatti – in linea con la nota fragilità della garanzia del consenso dell'interessato nel mondo digitale[51]– e in antitesi con gli attuali meccanismi di raccolta e gestione dei dati fondati generalmente su rapporti contrattuali tra singoli individui e operatori privati, consente di rivalutare l'importante apporto degli individui nella circolazione dei dati, riconoscendo loro un ruolo attivo in termini di partecipazione alla costruzione di una *data economy* più equa e giusta per tutti.

A tal proposito, di particolare importanza sono gli aspetti relativi alla *governance* del *trust* e agli strumenti di partecipazione degli utenti che potrebbero prestabilire le specifiche finalità del trattamento, limitando la raccolta dei dati, ad esempio ad uno specifico settore di ricerca, nonché prevedere periodiche forme di consultazione dal basso (*bottom-up*), salva naturalmente la possibilità, in caso di controversie, di ricorrere alla tutela giurisdizionale nelle Corti di *equity*. Analogamente, nel Report ADA 2021, vengono illustrate diverse forme di finanziamento per i *data trusts*, elemento davvero centrale per la stessa qualificazione dell'istituto, tra cui vengono citate autonome fonti di remunerazione provenienti dallo scambio dei dati raccolti presso gli utenti, la contribuzione da parte degli utenti stessi, le sponsorizzazioni di imprese private e finanziamenti o sussidi pubblici, ovvero combinazione di una o più tra queste modalità.

---

sezione del Report ADA 2021, pag. 27 e ss.. In dottrina, S. DELACROIX, N. LAWRENCE, *Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance,* Cit., 27.

[50] Secondo la definizione contenuta nel Report ADA 2021, "*A data trust is a proposed mechanism for individuals to take the data rights that are set out in law (or the beneficial interest in those rights) and pool these into an organisation – a trust – in which trustees would exercise the data rights conferred by the law on behalf of the trust's beneficiaries*." Working group ADA Lovelance Institute*, Final Report* on *Exploring legal mechanisms for data stewardship,* 34.

[51] Su cui si rimanda, *supra*, a n. 31.

In questa sede non è possibile compiere una completa disamina dei profili segnalati, tuttavia si osserva che tale ultimo aspetto è senz'altro centrale, in particolare con riferimento alle due opposte alternative di realizzare *trust*s fondati sulla cessione dietro corrispettivo dei dati degli utenti[52] – i cui profitti potrebbero essere ridistribuiti tra questi, nella doppia veste di disponenti e beneficiari – ovvero, *trusts* caratterizzati dall'assenza di ogni forma di lucro. La differente natura assunta dall'istituto, e la conseguente necessità di prevedere una adeguata regolamentazione, non può non avere significative ripercussioni operative incidendo sul numero e diffusione di questi soggetti nonché sull'attrattività degli stessi per gli utenti che, stante la limitata consapevolezza o interesse che viene registrato sui temi della tutela dei dati personali, potrebbero essere poco inclini ad aderirvi spontaneamente in assenza di forma di incentivazione. Diversi punti rimangono quindi ancora aperti e sarà necessario attendere la formalizzazione di proposte più puntuali per compiere una valutazione[53]. Tuttavia, sembra opportuno monitorarne attentamente gli sviluppi dell'istituto in discorso, in quanto esso potrebbe costituire un innovativo ed efficace meccanismo di tutela collettiva degli utenti, specialmente se accompagnato da una forte partecipazione o controllo dello Stato (c.d. *Public Data Trust*). Al contrario, sembrerebbe problematico ammettere la proliferazione di molteplici *trusts* privi di una legittimazione e controllo da parte degli utenti, ma costituiti direttamente dai poteri privati al fine di legittimare le proprie attività[54].

6. *Conclusioni*

Se dunque il *data trust* costituisce un rilevante strumento di garanzia dei diritti nell'era dell'IA, nella misura in cui potrebbe contribuire alla realizzazione di una *governace* dei dati "dal basso" – in antitesi a quella governata da potenti forze economiche private – e alla costruzione di sistemi IA affidabili e non discriminatori, esso risulta nondimeno funzionale a favorire lo scambio di dati su larga scala, in linea con i

[52] Per una riflessione sul valore di scambio dei dati personali, ed in particolare sulla natura non rivale e non escludibile del bene in discorso, da cui discende la possibilità di una cessione a più soggetti contemporaneamente, si veda A. STAZI, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Il diritto dell'informazione e dell'informatica,* no. 2/2019.

[53] Per una analisi, in senso critico, delle varie proposte che sono state avanzate sul tema in discorso, con particolare riferimento al tema della governance e del finanziamento, si veda il Report dell'Open Data Institue, BPE Solicitors, Pinsent Masons & Chris Reed, *Data trusts: legal and governance considerations*, cit.

[54] Uno dei più noti esempi di *Data trust* è quello proposto nel 2018 da *Sidewalk Labs*, una società del gruppo Google, da istituirsi in un quartiere della città di Toronto (Canada) al fine di gestire i dati personali e non che sarebbero stati raccolti nell'ambito di una nuova *smart city*. Si trattava quindi di realizzare un «*urban data trust»* che rappresentasse gli interessi dei cittadini con riferimento alla massiccia raccolta di dati derivante dall'impiego di forme di monitoraggio che si intendeva porre in essere per il miglioramento di diverse funzioni locali e servizi pubblici, dalla gestione del traffico, alla qualità dell'aria, al sistema di telecamere. Nelle dichiarazioni dei promotori, il progetto era funzionale a tutelare il diritto alla *privacy* degli utenti e alla realizzazione di un sistema di condivisione etico di dati personali. In seguito alle perplessità del Garante Canadese, e della cittadinanza, il progetto è stato sospeso. Cfr. D. LIE, L. AUSTIN, *Data Trusts and the Governance of Smart Environments: Lessons from the Failure of Sidewalk Labs' Urban Data Trust*, in *Surveillance & society*, 2021.

più recenti orientamenti espressi anche all'interno dell'Unione Europea[55]. Sebbene dunque, l'istituto in commento appaia molto lontano dalla dimensione teorica propria dell'ordinamento europeo, e in particolare di quella radicata nell'ordinamento Italiano, con riferimento al tradizionale ancoraggio della tutela dei dati personali alle categorie dei diritti indisponibili della personalità e alla stretta connessione di questi con la dignità umana[56], esso sembra essere in linea con alcune recenti proposte di regolazione avanzate dalla Commissione UE, coerentemente con la sempre maggiore valorizzazione della dimensione patrimoniale dei dati personali[57]. Si pensi che la recente proposta di Regolamento relativo alla governance europea dei dati[58] è volta a realizzare uno «spazio unico europeo dei dati» nel quale dati personali, e non, possano circolare tra enti ed istituzioni pubbliche e imprese private – per favorire lo sviluppo – anche e forse specialmente mediante l'applicazione dell'IA – di diversi settori economici (sanità, finanza, energia agricoltura etc.) secondo i principi di riutilizzo e condivisione dei dati per motivi «altruistici»[59]. In aggiunta, tra i molteplici profili di interesse della proposta di Regolamento – che non possono essere affrontati in questa sede[60] – si segnala l'introduzione della centrale figura dei «soggetti intermediari dei dati» che, con riferimento ai dati personali e in analogia con l'istituto del *data trust* elaborato nell'ordinamento inglese, si occuperebbero di «*rafforzare la capacità di agire e il controllo dei singoli individui in merito ai dati che li riguardano*»[61] agendo «*da intermediari tra i singoli individui, quali i titolari dei dati, e le persone giuridiche,* [avendo inoltre] *l'obbligo fiduciario nei confronti dei singoli individui di garantire che agiscono nel migliore interesse dei titolari dei dati*»[62]. In conclusione, l'analisi delle proposte maturate nell'ordinamento inglese, e in particolare dell'istituto del *data trusts* – oltre che di notevole interesse sotto una prospettiva teorica, intersecandosi con le tematiche della natura giuridica del dato personale, della dimensione collettiva o sociale della tutela della *privacy* e del rapporto di questa con il rischio di discriminazione

[55] La crisi pandemica sembra aver accerlerato questa tendeza, come confermato da alcuni documenti della Commissione: "*The Covid-19 crisis has shown the essential role of data use for crisis management and for informed decision-making by governments. Data has a key role in achieving the objectives of the European Green Deal and in the EU Recovery Plan, given its potential for innovation and job creation, as well as its contribution to the efficiency and international competitiveness of industries across all sectors*." Questa è la premessa contenuta nel "Inception Impact Assessments" del maggio 2021 per l'avvio della fase di consultazione per un ulteriore proposta legislativa relativa alla *governace* dei dati, il *Data Act*.

[56] Per tutti, G. ALPA, G. RESTA, *Le persone fisiche e i diritti della personalità*, Utet giuridica, 2006, 632.

[57] Per tutti, V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Diritto dell'Informazione e dell'Informatica*, 2, 4, 689.

[58] Proposta di regolamento COM/2020/767 (2020) relativo alla governance europea dei dati (Atto sulla governance dei dati) del 25 novembre 2020 ("*proposta di Regolamento*").

[59] Cfr. F. CALOPRISCO, *Data Governance Act. Condivisione e "altrusimo" dei dati*, in *Focus "Servizi e piattaforme digitali" AISDUE*, n. 3, 2021.

[60] Per tutti, si pensi al difficile rapporto con la normativa in materia di dati personali che è stato puntualmente rilevato nel parere congiunto del Comitato europeo per la protezione dei dati (EDPB) e del Garante europeo della protezione dei dati (EDPS) e in successivo comunicato (EDPB-EDPS Joint Opinion 03/2021; EDPB Statement 5/2021), in cui il Garante europeo ha ribadito che il dato personale non può essere considerato come una "*tradeable commodity*".

[61] Considerando 23 della proposta di Regolamento.

[62] Considerando 26, *ibidem*.

nell'ambito dell'IA – si appalesa come un importante oggetto di studio comparativo ai fini di comprendere, ed attuare, gli analoghi istituti in via di definizione nell'ambito del diritto comunitario, nell'ottica di elaborare meccanismi di tutela efficaci che mantengano al centro l'individuo, in nome di un costituzionalismo digitale in via di definizione.