Privacy e Intelligenza Artificiale

Tommaso Maria Ubertazzi

Sommario: 1. L'evoluzione della privacy. – 2. L'intelligenza artificiale e i sistemi di *machine learning*. – 3. Intelligenza artificiale e privacy. – 4. GDPR ed intelligenza artificiale. – 5. Limiti del GDPR. – 6. L'applicazione del modello culturale dell'autodeterminazione ai sistemi di intelligenza artificiale. – 7. Le soluzioni proposte della dottrina per limitare aspetti dell'intelligenza artificiale. – 8. L'*Artificial Intelligence Act*. – 9. Il coordinamento del GDPR e dell'*Artificial Intelligence Act*. – 10. La funzione di incentivare la circolazione dei dati.

1. Come noto il diritto alla privacy ha via via conosciuto una progressiva evoluzione che ne ha modificato la struttura e il contenuto. Nato inizialmente come *right to be left alone* e precisamente come un diritto della persona volto ad escludere qualsiasi ingerenza estranea all'interno delle mura domestiche (*seclusion*)[1]; con l'avvento dei computer a partire dalla metà degli anni Sessanta (in grado di rilevare e registrare i dati personali degli individui) ha via via modificato la sua struttura passando da una concezione statica di *seclusion* ad una dinamica volta al «control over personal information» e tale da verificare come le informazioni di un individuo circolassero nella società[2]. D'altro canto, parallelamente a questa nozione dinamica di controllo sui dati personali un diverso approccio al diritto alla privacy è stato proposto dall'analisi economica del diritto che con una serie di argomentazioni ha via via posto l'attenzione (non solo al diritto del singolo a mantenere riservate le proprie informazioni, ma) anche a quello della collettività a conoscere queste[3]. E tutto ciò ha via via portato la dottrina a rilevare come nel mondo della

[1] S.D. Warren - L.D. Brandeis, *The right to privacy*, in *Harv. L. Rev.*, 4, 1890, p. 193.

[2] A. Westin, *Privacy and freedom*, New York, 1967, p. 7 scrive testualmente che «the claim of individuals, groups, or institution to determine for themselves when, how, and to what extent information about them is communicated to others».

[3] Così R.A. Posner, *The right of privacy*, in *Ga. L. Rev.*, 12, 1978, p. 394; Id., *The economic of justice*, Harvard University Press, Cambridge, 1981, p. 231; Id., *An economic theory of privacy*, in *Philosophical Dimension of privacy*, a cura di F.D. Schoeman, Cambridge University Press, UK, 1984, p. 333; Id., *Blackmail, privacy, and freedom of contract*, in *U. Pa. L. Rev.*, 141, 1993, p. 1817; Id., *Economic analysis of law*, New York, 1998, p. 46; Id., *Orwell versus Huxley, economics, technology, privacy, and satire*, in *John M. Olin Law & Economics Working Papers*, 89, 1999, p. 1.

 ISSN 2037-5662

privacy sussistono tutta una serie di ulteriori interessi tra loro non necessariamente contrapposti: e più precisamente l'interesse del titolare del dato, ma anche quello della banca dati che lo raccoglie e della collettività a conoscerne.

In questo modo si è andata affermando una concezione di una privacy non più incentrata sull'interesse del singolo, ma volta a prevedere e ad un tempo tutelare diversi interessi tra loro anche contrapposti quali quello alla conoscenza dei dati e alla sua raccolta. E parallelamente a ciò si è andata formando una legislazione privacy volta: (i) ad accordare al soggetto interessato non solo rimedi difensivi (come la cancellazione, la rettifica, l'opposizione ecc.), ma anche positivi per consentirgli tutte le diverse forme di benefici che derivano dalla circolazione dei dati (come l'utilizzazione economica, la portabilità dei dati ecc.); e (ii) a tutelare i diversi interessi in campo nel mondo della circolazione dei dati nella consapevolezza che la condivisione e raccolta di essi genera ricchezza per l'intera collettività ed è un fenomeno che non solo non si può arrestare, ma soprattutto sarebbe contrario agli interessi dell'intera collettività[4].

Oggigiorno si assiste tuttavia all'avvento dell'intelligenza artificiale che con le sue tecnologie potrebbe per certi versi rideterminare un nuovo scenario in materia di dati personali. Infatti la capacità di questa tecnologia di raccogliere dati e ad un tempo auto-apprendere la conoscenza di essi mette in crisi i precedenti modelli di circolazione delle informazioni al punto da portare alcuni a ritenere definitivamente morta l'idea di riservatezza di una persona sui propri dati personali. Naturalmente queste preoccupazioni sono certamente suggestive. Tuttavia, non mi sembrano calzanti. Infatti, a me sembra che lo scenario che si sta delineando altro non è che una naturale evoluzione di un mercato delle informazioni che ormai non può più essere ostacolato ed anzi deve essere incentivato in quanto fonte di benessere per l'intera collettività[5].

2. Questo articolo ha come obiettivo quello di analizzare proprio alcuni aspetti dei rapporti tra intelligenza artificiale e privacy[6]. In particolare con

[4] Per un'analisi dei primi studi sul d.lgs. n. 196/2003 v. F. Cardarelli - S. Sica - V. Zeno-Zencovich, *Il codice dei dati personali*, Milano, 2004.

[5] Sul tema del c.d. diritto dell'Internet v. S. Sica - V. Zeno-Zencovich, *Legislazione, giurisprudenza e dottrina nel diritto dell'Internet*, in *Dif. inf.*, 2010, p. 377 ss.

[6] Cfr. G. Olivi, *Big Data, metadati e Intelligenza Artificiale: i confini tra i diversi diritti*, in *Dir. ind.*, 2, 2020, p. 181 ss.; G. Finocchiaro, *Intelligenza artificiale e diritto – Intelligenza artificiale*

 ISSN 2037-5662

il termine Intelligenza Artificiale si intende «the computational part of the ability to achieve goals in the world»[7]: si tratta di «una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali»[8]. Ed in questa «tecnologia» rientrano tutti i sistemi e i programmi che consentono ad un computer di eseguire prestazioni che sono tradizionalmente svolte dall'uomo: e così tra le più recenti applicazioni dei sistemi di intelligenza artificiale vi sono quelle di apprendimento automatico (*machine learning*)[9].

Più precisamente con il termine *machine learning* si intende «an application of Al that trains algorithms to improve on algorithmically programmed decision-making processes, meaning the algorithm may assess the shortcomings in its decision-making process in early iterations and improve upon its analyses and predictions regarding likely outcomes based on the data»[10]. E questi sistemi di *machine learning* sono in grado di ricevere una quantità potenzialmente infinita di dati, analizzare e comprendere il contenuto di questi dati per poi elaborare informazioni finali di risultato. Ma non solo. I sistemi di *machine learning* sono anche capaci di modificare l'algoritmo di funzionamento interno in modo tale da poter migliorare le proprie prestazioni nello svolgimento di un determinato compito nel corso del tempo. E tutto ciò dimostra l'estrema potenzialità di questa tecnologia specialmente in un mondo di circolazione di dati reso sempre più imponente anche con l'affermarsi dei *Big Data*[11].

3 / 2023

e protezione dei dati personali, in *Giur. it.*, 2019, p. 1657; I.A. Filipova - A.R. Akhatov - Z.O. Kuvandikov, *Artificial Intelligence Regulation: Experience of the European Union*, in *Sci. J. Samarkand St. U.*, 4, 2022, p. 169 ss.

[7] R.S. Sutton, *John McCarthy's Definition of Intelligence*, in *J. Artificial General Intelligence*, 11, 2, 2020, p. 66.

[8] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, SWD(2021) 84 final, Brussels, Explanatory Memorandum, April 21, 2021, p. 1.

[9] G. Comandé, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, 1, 2019, p. 169; V. Servings, *Artificial Intelligence. Machine Learning and Data Science in the 21st Century*, Self Publisher, 2019, *passim*.

[10] Così K. Johnson - F. Pasquale - J. Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, in *Fordham L. Rev.*, 88, 2, 2019, p. 499 ss.

[11] In generale sul rapporto tra privacy e i sistemi di *machine learning* v. E. Hesamifard - H. Takabi - M. Ghasemi - R.N. Wright, *Privacy-preserving machine learning as a service*, in *Proc.*

 ISSN 2037-5662

3. In questo quadro è evidente come la tecnologia sottesa all'intelligenza artificiale è in grado di ricevere set di dati di grandi dimensioni e comprenderne il contenuto sino ad auto-modificarsi in base ai dati raccolti. Naturalmente l'applicazione dei sistemi di apprendimento automatico «è estremamente dipendente dalla disponibilità di significative basi di dati, che devono anche essere annotati in modo da consentire alla macchina la piena interpretabilità e utilizzabilità nella fase di apprendimento»[12]. E di conseguenza la disponibilità di ingenti quantità di dati costituisce un elemento essenziale per il funzionamento e lo sviluppo di questa nuova tecnologia[13]. Tuttavia mentre risulta evidente come «l'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, può contribuire al conseguimento di risultati vantaggiosi dal punto di vista sociale e ambientale nonché fornire vantaggi competitivi fondamentali alle imprese e all'economia europea». Altrettanto evidente risulta come questa tecnologia è in grado di determinare dei rischi alla società ed alle persone ed in particolare in questo caso alla loro privacy. Così ad esempio (i) la non suf-

Priv. Enhancing Technol., 2018, p. 123 ss.; J. Shook - R. Smith - A. Antonio, *Transparency and Fairness in Machine Learning Applications*, in *Texas A&M J. Prop. L.*, 4, 5, p. 2018, p. 443 ss.; M. Hildebrandt, *Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning*, in *Theoretical Inquiries in Law*, 20, 1, 2019, p. 83 ss.; S. McJohn - I. McJohn, *Fair Use and Machine Learning*, in *Northeastern U. L. Rev.*, 12, 1, 2020, pp. 99-161; T. Minssen - S. Gerke - M. Aboy - N. Price - G. Cohen, *Regulatory Responses to Medical Machine Learning*, in *J. of L. and the Biosciences*, 7, 1, 2020, p. 1 ss.; W.N. Price - A. Rai, *Clearing Opacity through Machine Learning*, in *Essay Iowa L. Rev.*, 106, 2, 2021, p. 775 ss.; B. Liu - M. Ding - S. Shaham - W. Rahayu - F. Farokhi - Z. Lin, *When machine learning meets privacy: A survey and outlook*, in *ACM Computing Surveys (CSUR)*, 54, 2, 2021, p. 1 ss.

[12] Gruppo di esperti MiSE sull'intelligenza artificiale, *Proposte per una Strategia italiana per l'intelligenza artificiale*, in *mimit.gov.it*, 2020, p. 11.

[13] Cfr. R. Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, in *SSRN* 2017, p. 16 secondo cui «the acceleration of artificial intelligence […] is intimately tied to the availability of data»; G. Sanseverino, *IA e diritto dei brevetti*, in *AIDA*, 2020, p. 32 secondo cui «maggiori dati verranno forniti alla macchina maggiore sarà l'efficacia del funionamento e dei risultati dell'algoritmo di apprendimento»; C. Giorgini, *Intelligenza artificiale e Internet of Things: privacy e responsabilità civile*, in *Ciberspazio e diritto*, 23, 70, 2022, p. 4 secondo cui «l'applicazione delle tecniche di *machine learning* implica la disponibilità di grandi quantità di basi di dati […] quanto più accurati e adeguatamente annotati sono i dati su cui i sistemi di IA si basano, tanto più gli stessi risulteranno efficaci. Pertanto, il funzionamento dei sistemi di IA, tra cui quelli di *machine learning*, dipende in larga misura dai set di dati utilizzati per addestrarli ed è fondamentale che i dati "di addestramento" siano sufficientemente ampi, ricomprendendo il più vasto numero di scenari possibili».

 ISSN 2037-5662

ficiente trasparenza dei sistemi di intelligenza artificiale, perché l'interessato, i cui dati sono oggetto di analisi da parte del sistema di intelligenza artificiale, non riceve un'adeguata spiegazione sui meccanismi di funzionamento del sistema, sugli specifici dati utilizzati e sulle possibili limitazioni dei suoi interessi personali[14]; (ii) la capacità di queste tecnologie di dedurre dati personali a partire da dati anonimizzati, anonimi o non personali, infatti i sistemi di *machine learning* sono capaci di elaborare nuove informazioni (anche di carattere personale) a partire dal set di dati ricevuti[15]; (iii) l'inefficacia del principio di non esclusività[16] perché ove l'interessato veda leso il suo diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, difficilmente sarebbe in grado di dimostrare che la decisione lesiva sia stata presa unicamente sulla base dell'algoritmo[17]; e (iv) la difficoltà

[14] G.V. Gizem, *A Case Study on the Interaction between the General Data Protection Regulation and Artificial Intelligence Technologies*, in *Pro Futuro: A Jovo Nemzedekek Joga*, 4, 2020, p. 45 ss. secondo cui «technical complexity and the black-box nature of the algorithmic assessments may hinder the transparency and explainability principles which are relevant to data repurposing, unforeseeable system functionality, and finally, complex data controller relationships, which may prevent data subjects from exercising effective consent implementations, if not making it impossible to give informed and unambiguous consent»; G. De Gregorio - F. Paolucci, *Dati e intelligenza artificiale all'intersezione tra mercato e democrazia*, in *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, a cura di E. Cremona - F. Laviola - V. Pagnanelli, Torino, 2022, p. 117 secondo cui «il dibattito sul nesso tra dati e IA si è, difatti, molto concentrato sul tema dell'*explainability*, vale a dire il diritto dell'individuo ad ottenere il disvelamento della ratio decisionale del sistema automatizzato a seguito di un'analisi effettuata sui propri dati (personali)»; F. Lazzini, *Etica digitale e Intelligenza Artificiale. I rischi per la protezione dei dati*, Torino, 2022, p. 30 ss. secondo cui «nel caso in cui una decisione che produce effetti giuridici oppure che ha un impatto significativo sulla vita di un individuo sia stata riferita o presa da un sistema di IA, spetta il diritto ad una spiegazione significativa di come funzioni tale sistema, quale logica di ottimizzazione segua, che tipo di dati utilizzi e, come influisca sugli interessi individuali».

[15] Cfr. F. Lazzini, *Etica digitale e Intelligenza Artificiale*, cit., 2022, p. 30 ss. secondo cui «la protezione dei dati e il diritto alla privacy possono essere messe a repentaglio dai sistemi di IA anche qualora tali sistemi di IA non siano progettati per elaborare dati personali, e si basino invece, su dati anonimizzati, anonimi o non personali. In effetti, i sistemi di apprendimento automatico possono dedurre da tali dati informazioni personali, compresi i dati sensibili».

[16] Sul principio di non esclusività v. 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 *Int'l Data Privacy L.*, 2, 7, 2016, p. 76 ss.

[17] A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *Rivista di BioDiritto*, 1, 2019, p. 63 ss. secondo cui «in base al principio di non esclusività sarebbero vietate le decisioni basate "*unicamente*" su trattamenti automatizzati dei dati. […] In realtà, questo principio – codificato nella normativa europeo-nazionale – è del tutto inefficace di fronte a quella che potremmo definire la travolgente forza pratica dell'algoritmo».

 ISSN 2037-5662

tecnica di garantire la cancellazione dei dati, in quanto i sistemi di intelligenza artificiale sono capaci di modificare i propri algoritmi di funzionamento interno sulla base dei dati ricevuti e quindi i dati, diventando parte dell'algoritmo, non possono essere più identificati e cancellati[18].

4. Certo viene da chiedersi se questi rischi siano regolati e contemplati dalla legislazione attuale in materia di privacy[19]. E qui si potrebbe in prima battuta dare una risposta positiva considerando che il legislatore europeo con il regolamento UE n. 2016/679 (di seguito: GDPR)[20]ritiene lecito il trattamento «solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del

[18] B.W. Jackson, *Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense*, in *Minnesota J. L. Sci. and Tech.*, 21, 1, 2019, p. 192 secondo cui «another key feature of the GDPR relates to erasing data the "right to be forgotten" […] this can create significant challenges for Al. The utility of algorithms trained on machine learning processes stems from the training data. If data is subsequently removed, this can disrupt the algorithm's future behavior and create inaccurate or unreliable results. Although companies could train algorithms on updated datasets, this may create additional risk and liabilities given the volatility and uncertainty if significant portions of training data can be so easily removed. In the context of cybersecurity, this could prove disastrous. For example, if a large dataset of IP addresses was removed from a training model, then the baseline for the network defense system may be altered and no longer be reliable in detecting anomalies»; K. Karaboue, *Intelligenza artificiale nell'ambito del sistema sanitario. Implicazioni in termini di privacy alla luce del nuovo GDPR*, in *Riv. trim. dir. amm.*, 1, 2023, p. 370 secondo cui «nel contesto dell'IA, una specificità del deep learning è che l'algoritmo utilizzato per ottenere un risultato è creato automaticamente sulla base di dati che sono stati introdotti in precedenza. Questi dati diventano, quindi, parte dell'algoritmo e diventa impossibile identificare ed estrarre dati specifici per cancellarli».

[19] In generale sul tema della privacy nell'era dei *Big Data* v. A. Ottolia, *Big Data e innovazione computazionale*, in *Quaderni di AIDA n. 28*, Torino, 2017; R. D'Orazio - V. Cuffaro - V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019.

[20] Più precisamente Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

 ISSN 2037-5662

trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore» (così l'art. 6). E reciprocamente ove l'intelligenza artificiale procedesse ad un trattamento non lecito l'interessato sarebbe comunque fornito di tutta una serie di rimedi quali l'accesso dell'interessato al fine di ottenere «dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano» (così l'art. 15, par. 1)[21]; la rettifica dei dati personali per «ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa» (così l'art. 16, par. 1)[22]; la revoca del «proprio consenso» per il trattamento prestato (così l'art. 7, par. 3)[23]; la cancellazione «dei

3 / 2023

[21] Sul diritto di accesso dell'interessato v. S. Wachter - B. Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Col. Bus. L. Rev.*, 2, 2019, p. 494 ss.; S. Mihail - T. Wisman, *The Right to Privacy with Respect to the Processing of Personal Data in the Context of Controlling Tax Fraud*, in *EDPL*, 3, 2, 2017, p. 267; A. Sobolciakova, *Right of Access under GDPR and Copyright*, in *Masaryk U. J. L. Tech.*, 12, 2, 2018, p. 221 ss.

[22] Sul diritto di rettifica dei dati personali v. E. Barraco - A. Sitzia - S. Iacobucci, *Privacy: diritti degli interessati*, in *Dir. prat. lav.*, 43, 2018, p. 2557 ss.; L. Spataru - Negura - C. Lazar, *Lifting the veil of the GDPR to data subjects*, in *Challenges of the Knowledge Society*, 2018, p. 658 ss.; A. Ausley, *The Prospective Impact of the Global Data Protection Regulation on Entrepreneurship: A Roboadvisor Case Study*, in *ISJLP*, 15, 2019, p. 85 ss.; N. Palmieri, *Data Protection in an Increasingly Globalized World*, in *Indiana L .J.*, 94, 1, 2019, p. 297 ss.; E. Tosi, *La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR) (prima parte)*, in *Studium Iuris*, 7-8, 2020, p. 840 ss.

[23] Sul diritto alla revoca del consenso v. T.M. Ubertazzi, *Dubbi sulla revocabilità del consenso all'utilizzazione dell'immagine*, in *Foro it.*, 2009, 1, p. 2731; E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 1, 2018, p. 106 ss.; A. Metzger - Z. Efroni - L. Mischau - J. Metzger, *Data-Related Aspects of the Digital Content Directive*, in *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 9, 1, 2018, p. 90 ss.; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, p. 187; K.A. Houser - W. Voss, *GDPR: The End of Google and Facebook Or New Paradigm in Data Privacy*, in *Richmond J. L. & Tech.*, 25, 1, 2018, pp. 1-109; F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, p. 44; C. Irti, *Persona minore di età e libertà di autodeterminazione*, in *Giust. civ.*, 3, 2019, p. 617 ss.; A.

 ISSN 2037-5662

dati personali che lo riguardano» (così l'art. 17, par. 1)[24]; la «limitazione del trattamento» (così l'art. 18, par. 1)[25]; la «portabilità dei dati» (così l'art. 20)[26]; e l'opposizione «per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano» (così l'art. 21, par. 1)[27]. Analogamente si potrebbe dare una risposta positiva anche sulla base della consi-

De Franceschi, *Il pagamento mediante dati personali*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro - R. D'Orazio - V. Ricciuto, cit., p. 1406 ss.; J. Erbguth, *Five Ways to GDPR-Compliant Use of Blockchains*, in *EDPL*, 5, 3, 2019, pp. 427-433; E. Murati - M. Henkoja, *Location Data Privacy on MAAS under GDPR*, in *EJPLT*, 2, 2019, p. 131; A. Addante, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, in *Giust. civ.*, 4, 1, 2020, p. 889 ss.; M. Schmidt - Kessel, *Right to Withdraw Consent to Data Processin. The Effect on the Contract*, in *Data as Counter-Performance - Contract Law 2.0?*, a cura di S. Lohsse - R. Schulze - D. Staudenmayer, Baden-Baden, 2020, p. 129 ss.; C. Angiolini, *A proposito del caso Orange Romania deciso dalla Corte di Giustizia dell'UE: il rapporto tra contratto e consenso al trattamento dei dati personali*, in *Contratto e impresa*, 2, 2021, p. 602 ss.; T.M. Ubertazzi, *Rethinking the withdrawal of consent in the functional perspective of privacy*, in *Quaderni di AIDA* n. 32, Torino, 2022, *passim*.

[24] Sul diritto alla cancellazione dei dati personali v. J. Bovenberg - M. Kattenberg-B. Baselmans-M. Sinke-R. Hoekstra - D.I. Boomsma - G. Willemsen, *Enhancing Biobank Participants' Rights from Paper to Portal*, in *SCRIPTed*, 13, 1, 2016, pp. 70-82; S. Sica - V. D'Antonio, *La procedura di de-indicizzazione*, in *La nuova disciplina europea della privacy*, a cura di S. Sica - V. D'Antonio - G.M. Riccio, Milanofiori Assago, 2016, p. 154; J. Ausloos, *Ctrl+Z: The Right to Be Forgotten*, in *EDPL*, 3, 1, 2017, pp. 138-142; Z. Li, *Confronting Algorithm Bias Risks: Will Blockchain Provide New Opportunities or Challenges for Data Protection Law?*, in *Dublin L. & Pol'y Rev.*, 2, 2021, pp. 43-67.

[25] Sulla limitazione al trattamento v. N. Zorzi Galgano, *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, *passim*; G. De Gregorio - R. Torino, *Privacy, protezione dei dati personali e Big Data*, in *Privacy digitale*, a cura di E. Tosi, cit., p. 447 ss.; L. Califano, *I diritti e le garanzie degli interessati nel regolamento europeo 2016/679*, in *Cultura giuridica e diritto vivente*, 10, 2022, p. 1 ss.

[26] Sul diritto alla portabilità dei dati v. L. Scudiero, *Bringing Your Data Everywhere: A Legal Reading of the Right to Portability*, in *EDPL*, 3, 1, 2017, p. 119 ss.; R. Janal, *Data Portability - A Tale of Two Concepts*, in *Journal of Intellectual Property, Info. Tech. & Elec. Comm. L.*, 8, 1, 2017, p. 59; I. Graef - M. Husovec - N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, in *German L.J.*, 19, 6, 2018, p. 1359 ss.; S. Hondagneu - Messner, *Data Portability: Guide and Roadmap*, in *Rutgers Computer & Tech. L. J.*, 47, 2, 2021, p. 240 ss.

[27] Sul diritto di opposizione al trattamento v. A. de Hingh, *Some Reflections on Dignity as an Alternative Legal Concept in Data Protection Regulation*, in *German L.J.*, 19, 5, 2018, p. 1269 ss.; M.G. Porcedda, *On Boundaries – Finding the Essence of the Right to the Protection of Personal Data*, in *Data Protection and Privacy. The Internet of Bodies*, a cura di P. De Hert - R. Leenes - R. Van Brakel - S. Gutwirth, Bloomsbury Publishing, 2018, p. 305; C. Etteldorf, *Data Protection Authorities Give Guidance on Direct Marketing under GDPR*, in *EDPL*, 5, 1, 2019, p. 85 ss.

 ISSN 2037-5662

derazione il GDPR ha previsto, tra le condizioni di legittimità del consenso, i principi di limitazione delle finalità e di minimizzazione dei dati: e dunque in base al primo principio i dati personali devono infatti essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali» (così art. 5, par. 1 b)); in base al secondo principio i dati personali devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» (così art. 5, par. 1 c)). In questo modo questi principi rafforzano ulteriormente l'idea che i dati personali possono essere trattati solo nei limiti di quanto risulti indispensabile in vista delle finalità perseguite con quello specifico trattamento[28]. E tutto ciò legittimerebbe allora ad escludere trattamenti di dati con l'intelligenza artificiale contrari a questi principi.

Ed infine si potrebbe dare una risposta positiva anche sulla base della considerazione che l'art. 22, par. 1, GDPR ha enunciato il c.d. principio di non esclusività prevendendo che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»; ed il considerando n. 71 ha previsto che l'interessato deve «avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani». E tutto ciò dovrebbe allora escludere comportamenti dei fornitori di intelligenza artificiale contrari a questi principi.

5. Certo è che queste tutele non sono da sole sufficienti. Anzitutto perché alcune di esse non si applicano proprio in caso di acquisizione del consenso dell'interessato[29]. Così si è visto ad esempio che l'art. 22, par. 1, GDPR ha

[28] Così A. Alongi - F. Pompei, *Diritto della privacy e protezione dei dati personali. Il GDPR alla prova della data driven economy*, Roma, 2021, p. 133.

[29] Sul principio di non esclusività v. S. Wachter - B. Mittelstadt - L. Floridi, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation*,

 ISSN 2037-5662

enunciato il c.d. principio di non esclusività prevedendo che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Ma lo stesso art. 22 al par. 2 specifica che questa limitazione non si applica «nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al par. 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione». E la dottrina ha giustamente sottolineato che è «evidente che la portata di queste eccezioni è nei fatti amplissima, tanto che viene da chiedersi quando, in realtà, si possa applicare la regola»[30].

Inoltre, perché alcune tutele previste nel GDPR possono di fatto essere «aggirate» proprio con l'intelligenza artificiale. A questo proposito è infatti vero che il GDPR non autorizza il trattamento sulla base di un semplice consenso, ma richiede che questo deve essere (i) «liberamente fornito, specifico, informato e inequivocabile» (così art. 4, par. 1, n. 11, GDPR); (ii) espresso «mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale» (così considerando n. 32 del GDPR); e (iii) tale per cui i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità» (così art. 5, par. 1

op. cit., p. 76 ss.; A. Simoncini, *L'algoritmo incostituzionale*, *op. cit.*, p. 63 ss.; A. Simoncini - S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 8, 1, 2019, p. 87 ss.; M. Iaselli - F. Corona, *Manuale di diritto di Internet. Le principali ed innovative tematiche dell'informatica giuridica: l'ambito civile, penale, amministrativo e le tecnologie emergenti*, Roma, 2021, *passim*; D. Morana - T. Balduzzi - F. Morganti, *La salute «intelligente": eHealth, consenso informato e principio di non-discriminazione*, in *Federalismi.it*, 2022, p. 127 ss.; F. Lazzini, *Etica digitale e Intelligenza Artificiale*, cit., p. 52.

[30] V. A. Simoncini, *L'algoritmo incostituzionale*, *op. cit.*, p. 17.

 ISSN 2037-5662

b), GDPR). Ma è altrettanto vero che l'intelligenza artificiale proprio grazie alla sua capacità di auto-apprendere (e quindi elaborare nuove informazioni a partire dal set di dati con cui è stata programmata) potrebbe arrivare a bypassare il consenso e trattare i dati personali per finalità ulteriori rispetto a quelle predeterminate dal titolare del dato raccogliendo i dati di una persona in forma anonima da altre fonti per poi rielaborarli e ricondurli all'interessato[31]. D'altro canto, l'intelligenza artificiale pone delle criticità anche all'applicazione del principio di minimizzazione dei dati perché i sistemi automatizzati di questa tecnologia sono in grado di analizzare i dati ricevuti per poi generare ulteriori informazioni rispetto a quelle fornite con il consenso dell'interessato. E proprio per questo «la capacità di prendere decisioni e metterle in atto nel mondo esterno»[32] che caratterizza l'intelligenza artificiale rende di difficile applicazione i principi ora detti[33].

Ed infine perché le tutele esistenti difficilmente permettono all'interessato di interrompere il trattamento effettuato con queste tecnologie una volta prestato il consenso e ciò a prescindere che si adotti o meno una visione restrittiva dei rimedi che il GDPR fornisce a quest'ultimo (come la revoca del consenso, il diritto di opposizione o di cancellazione etc.). Infatti, i dati utilizzati dall'intelligenza artificiale possono diventare parte stessa dell'algoritmo della macchina con la conseguenza che non potrebbero più essere identificati e cancellati. E tutto ciò dimostra come questi rimedi dell'inte-

3/2023

31 Così S. Jain - S.A. Jain, *Artificial Intelligence: A Threat to Privacy*, in *Nirma U. L. J.*, 8, 2, 2019, p. 33 secondo cui «if the personal data is anonymised and once it becomes a part of a large data set, an AI can de-anonymize this data based on inference from other devices». V. anche M. Bartlett, *Beyond Privacy: Protecting Data Interests in the Age of Artificial Intelligence*, in *L. Tech. and Humans*, 3, 1, 2021, p. 96 ss.; F. Lazzini, *Etica digitale e Intelligenza Artificiale*, cit., p. 30 ss.

32 Considerando AA della Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

33 Sulle implicazioni dell'intelligenza artificiale sui principi di limitazione delle finalità e di minimizzazione dei dati v. G. Clavell - M.M. Zamorano - C. Castillo - O. Smith - A. Matic, *Auditing algorithms: On lessons learned and the risks of data minimization*, in *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 2020, p. 265 ss.; A. Goldsteen - G. Ezov - R. Shmelkin - M. Moffie - A. Farkash, *Data minimization for GDPR compliance in machine learning models*, in *AI and Ethics*, 2021, p. 1 ss.; A. Astone, *Autodeterminazione nei dati e sistemi di A.I.*, in *Contr. impr.*, 2, 4, 2022, p. 429 ss.; A. Brauneck - L. Schmalhorst - M.M. Kazemi Majdabadi - M. Bakhtiari - U. Völker - J. Baumbach - L. Baumbach - G. Buchholtz, *Federated machine learning, privacy-enhancing technologies, and data protection laws in medical research: Scoping review*, in *J. Med. Internet Res.*, 25, 2023, *passim*.

 ISSN 2037-5662

ressato da soli si rivelerebbero una semplice arma spuntata verso i sistemi di intelligenza artificiale.

6. Le considerazioni sino ad ora espresse portano allora a chiedersi se l'attuale disciplina prevista nel GDPR sia adeguata ove applicata ai trattamenti dei dati effettuati mediante sistemi di intelligenza artificiale[34]. In particolare, viene da chiedersi se lo schema del GDPR che riconoscendo diversi interessi sottesi alla circolazione dei dati considera il consenso dell'interessato uno dei fulcri della circolazione di essi non possa via via essere superato o quantomeno stemperato da questo strumento di tecnologia. E qui sembra proprio possibile dare una risposta affermativa. L'intelligenza artificiale dimostra infatti come l'interessato non può da solo interrompere l'utilizzo da parte di questa tecnologia dei dati di una persona. Ma non solo. L'intelligenza artificiale dimostra che una volta prestato il consenso anche più circostanziato con le sue tecnologie è in grado di auto-apprendere i dati forniti anche in forma anonima e individuare esattamente il profilo di una persona. E proprio per questo, infatti una dottrina ha osservato che il modello culturale su cui si basa il GDPR, che è quello dell'autodeterminazione, non può essere applicato a sistemi di intelligenza artificiale basati su ingenti quantità di dati e precisamente «il consenso, astrattamente il miglior modello possibile, si rivela spesso non adeguato nel fornire una tutela effettiva ed efficace. Ciò tanto più se ci si confronta con applicazioni di intelligenza artificiale basate sui Big data, nelle quali la determinabilità a priori dei processi di elaborazione non è scontata e nelle quali la finalità del trattamento sovente non è chiara»[35]. Qui

[34] V. G. Olivi, *Big Data, metadati e Intelligenza Artificiale*, *op. cit.*, p. 181 secondo cui «i sistemi di Intelligenza Artificiale permettono la raccolta, oltre che l'elaborazione di grandi volumi di dati, in tempi molto ridotti: è così, che i Big Data possono diventare al contempo presupposto e conseguenza dei sistemi di Intelligenza Artificiale. E se attività come l'analisi, il trattamento e l'elaborazione di Big Data sono alla base del funzionamento di ogni sistema governato dall'Intelligenza Artificiale e/o riconducibile all'Internet delle Cose, è evidente come debbano essere oggetto di particolare attenzione le problematiche che i sistemi di Intelligenza Artificiale sollevano in materia di tutela dei dati personali. Molte di queste problematiche sono connesse alla capacità del Reg. EU 679/2016 (GDPR) di garantire la protezione dei dati personali delle persone fisiche anche, e soprattutto, nel settore digitale e delle comunicazioni elettroniche. Già le stesse modalità di raccolta di dati personali da parte dei sistemi di Intelligenza Artificiale hanno sollevato alcuni dubbi di compatibilità con le categorie normative previste dal GDPR».

[35] Così G. Finocchiaro, *Intelligenza artificiale e diritto*, *op. cit.*, p. 1662. Ma v. anche Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Report on Artificial Intelligence and Data*

 ISSN 2037-5662

infatti pare chiaro che il focus deve essere rivolto a regolare non tanto quello che può consentire o meno l'interessato con il suo consenso, quanto quello che può fare o non fare il fornitore del servizio di intelligenza artificiale

7. Ne deriva allora la necessità di una regolamentazione apposita dell'intelligenza artificiale che si applichi anche ed a prescindere dal consenso dato dell'interessato. E proprio per questo la dottrina ha proposto via via diverse forme di intervento. Così una prima forma di intervento molto radicale è quella di limitare o bloccare l'intelligenza artificiale ed il trattamento dei dati: cosa che tra l'altro è avvenuta recentemente a seguito del provvedimento del Garante per la Protezione dei Dati Personali volto a bloccare «ChatGPT» (acronimo di *Conversational Generative Pre-Training Transformer*)[36]. In questo caso il Garante per la Protezione dei Dati Personali ha infatti ritenuto che questa piattaforma, sviluppata e gestita dalla società statunitense OpenAI[37], stesse trattando i dati personali degli utenti (anche minorenni) in violazione delle disposizioni del GDPR e precisamente degli artt. 5, 6, 8, 13 e 25 del GDPR.

Protection: Challenges and Possible Remedies, p. 7 secondo cui «long and technical data processing notices, social and technical lock-ins, obscure interface design, and a lack of awareness on the part of the data subject are some of the reasons for this weakness. […] AI-based profiling and hidden nudging practices challenge both the idea of freedom of choice based on contractual agreement and the notion of data subjects' control over their information. Finally, the frequent complexity and obscurity of AI algorithms hamper the chances of obtaining real informed consent».

[36] Così Provvedimento del Garante per la Protezione dei Dati Personali, 30 marzo 2023, n. 112.

[37] ChatGPT è una *chatbot* basata sull'intelligenza artificiale in grado di generare nuovi testi sulla base di modelli appresi a partire dal set di dati di addestramento. Sul tema v. E. Falletti, *Esiste una differenza tra il diritto all'oblio e il presunto diritto alla fuga dai motori di ricerca?*, in *Danno resp.*, 3, 2023, p. 280; L. Megale, *Il Garante della privacy contro ChatGPT: quale ruolo per le autorità pubbliche nel bilanciare sostegno all'innovazione e tutela dei diritti?*, in *Giornale dir. amm.*, 3, 2023, p. 403 ss.; K.L. Fidler, *ChatGPT - The Blurst of Times*, in *Australian L. Libr.*, 31, 1, 2023, p. 19 ss.; T.P. Oltz, *ChatGPT, Professor of Law*, in *Tech. & Pol'y*, 1, 2023, p. 207 ss.; J. Eiseman - N. Ortiz, *Generative AI & Machine Learning in Law Libraries: The Benefits, Risks, and Ethical Issues Surrounding These Potentially Transformative New Tools*, in *AALL Spectrum*, 27, 5, 2023, p. 14 ss.; N. Lucchi, *ChatGPT: A Case Study on Copyright Challenges for Generative AI Systems*, in *SSRN*, 2023, p. 5 secondo cui «ChatGPT is an AI language model developed by OpenAI, which uses Natural Language Processing (NLP) to generate human-like text in response to various inputs. It is essentially an auto-generating chatbot that extracts data from various sources, processes it, and produces grammatically correct and contextually appropriate responses. ChatGPT can be used for a variety of applications, including customer service, chatbots, and virtual assistants. It has been trained on a massive amount of text data and is constantly learning and improving».

 ISSN 2037-5662

Una seconda forma di intervento proposta è quella di «imporre alle società produttrici ed, in particolare, a quelle che trattano dati altamente contestualizzati, come quelli presenti nell'ecosistema domestico, di ricorrere a certificazioni o a sigilli e marchi, di cui all'art. 42 del GDPR, che attestino il rispetto di determinati parametri, finalizzati ad assicurare un'adeguata protezione dei dati»[38].

Una terza forma di intervento vuole rendere l'*Age Appropriate Design Code*[39], elaborato per i dispositivi destinati ai minori (come giochi, app, programmi e siti web), un modello generale per tutte le tecnologie di automazione domestica. Infatti «it seems that companies are not recognizing the privacy implications involved in children's daily interactions with home automation technologies that are not designed for or targeted at them. […] There is no acknowledgement so far of the complexity of home life data, and much of the privacy debates seem to be evolving around personal (individual) data. It is for this reason that we need to find new measures and solutions to safeguard children and to make sure that age appropriate design code is included within home automation technologies»[40]. Ne deriva che secondo questa impostazione sarebbe necessario applicare le tutele previste dall'*Age Appropriate Design* ogniqualvolta i dati appartenenti a minori siano raccolti (non solo dai dispositivi rivolti ai minori, ma) da tutte le tecnologie di automazione domestica[41]. Una quarta, infine, forma di intervento proposta è quella di introdurre un *right to reasonable inferences* applicabile mediante l'implementazione di meccanismi di tutela precedenti e successivi al

[38] Così A. Astone, *Autodeterminazione nei dati e sistemi di A.I.*, *op. cit.*, 429 ss.

[39] ICO's Age Appropriate Design Code 2020. Sul tema si v. J. Cao, *Safeguarding children's privacy: study of regulation and practice in the United Kingdom and the United States*, in *IJLET*, 1, 2023, p. 56 ss.

[40] Così V. Barassi, *Home life data' and children's privacy*, in *Child Data Citizen*, 2018, p. 18.

[41] Sul tema v. anche V. Barassi, *Datafied Citizens in the Age of Coerced Digital Participation*, in *Soc. Res. Online*, 24, 3, 2019, p. 414 ss. secondo cui «I submitted a report titled "Home Life Data and Children's Privacy Report" (Barassi, 2018) to the Information Commissioner's Office in the UK, which was used as evidence for the importance of the development of age-appropriate design code. In the report, I argue that firms currently fail to recognize the privacy implications of children's daily interactions with home automation technologies that are not designed or targeted at them. I also argue that the data of children that are being collected from home automation technologies are not only personal (individual) data but are "home life data", a mix of family data, household data, and highly contextual data. The problem with current terms and conditions is that they always refer to personal data, and there is little scrutiny or understanding of what happens to the data generated by the aggregation of adult and children profiles».

 ISSN 2037-5662

trattamento. Più precisamente il titolare del trattamento dovrebbe spiegare *ex ante*: (i) perché da determinate informazioni è possibile dedurre ulteriori dati personali; (ii) perché le informazioni dedotte sono compatibili con le finalità del trattamento o il tipo di decisione automatizzata prescelta; e (iii) se i metodi utilizzati per dedurre i dati sono affidabili. Inoltre dovrebbe essere conferito all'interessato un diritto *ex post* di contestare i dati dedotti da queste tecnologie ad esempio perché inesatti o irragionevoli[42].

8. Naturalmente queste soluzioni proposte dalla dottrina tutte evidenziano come al momento sia ormai diventato necessario un intervento legislativo che regoli l'operare dei fornitori di intelligenza artificiale. Proprio l'esigenza di istituire un quadro giuridico in materia di intelligenza artificiale uniforme e ad un tempo conforme ai valori dell'UE nei quali naturalmente vi è anche il rispetto della privacy è stata intercettata dalla Commissione UE che il 21 aprile 2021 ha pubblicato una proposta di regolamento sull'intelligenza artificiale (di seguito: *Artificial Intelligence Act* o proposta di regolamento)[43].

[42] Cfr. S. Wachter - B. Mittelstadt, *Right to reasonable inference*, *op. cit.*, p. 494 ss. secondo cui «data controllers would need to explain (1) why certain data are a normatively acceptable basis to draw inferences; (2) why these inferences are normatively acceptable and relevant for the chosen processing purpose or type of automated decision; and (3) whether the data and methods used to draw the inferences are accurate and statistically reliable […] to complement ex-ante notification requirements, the second half of a 'right to reasonable inferences' should provide an effective ex-post accountability mechanism for the data subject. The ex-ante justification is bolstered by an additional ex-post mechanism enabling unreasonable inferences to be challenged. This right would allow data subjects to contest inferences themselves (e.g., credit score), which complements the existing right to contest automated decisions found in Article 22(3)».

[43] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, SWD(2021) 84 final, Brussels, April 21, 2021. Sul tema v. T. Madiega, *Artificial intelligence act*, in *Eur. Parliamentary Res. Serv.*, 2021, *passim*; O. Posykaliuk, *Proposal for artificial intelligence act and its influence on private law*, in *Law Ukr.: Legal J.*, 12, 2021, p. 242 ss.; P. Hacker, *A legal framework for AI training data—from first principles to the Artificial Intelligence Act. Law*, in *Innovation & Tech.*, 13, 2, 2021, p. 257 ss.; M. Ebers, *Standardizing AI-The Case of the European Commission's Proposal for an Artificial Intelligence Act*, in *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*, a cura di L.A. DiMatteo - C. Poncibò - M. Cannarsa, Cambridge University Press, 2021, *passim*; J. De Cooman, *Humpty dumpty and high-risk ai systems: the* ratione materiae *dimension of the proposal for an EU Artificial Intelligence Act*, in *Mkt. & Competition L. Rev.*, 6, 1, 2022, p. 49 ss.; D. Chiappini, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*, in *Rivista italiana di informatica e diritto*, 4, 2, 2022, p. 95 ss.; U. Pagallo - J.C. Sciolla - M. Durante, *The environmental challenges of*

 ISSN 2037-5662

Con questa proposta di regolamento si stabiliscono «a) regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale ('sistemi di IA') nell'Unione; a) il divieto di determinate pratiche di intelligenza artificiale; b) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi; c) regole di trasparenza armonizzate per i sistemi di IA destinati a interagire con le persone fisiche, i sistemi di riconoscimento delle emozioni, i sistemi di categorizzazione biometrica e i sistemi di IA utilizzati per generare o manipolare immagini o contenuti audio o video; d) regole in materia di monitoraggio e vigilanza del mercato» (così art. 1 dell'*Artificial Intelligence Act*).

Più precisamente l'*Artificial Intelligence Act* classifica le pratiche di intelligenza artificiale in base a quattro livelli di rischio: (i) i rischi inaccettabili (disciplinati dal titolo II); (ii) i rischi elevati (disciplinati dal titolo III); (iii) i rischi limitati (disciplinati dal titolo IV); e (iv) i rischi minimi (disciplinati dal titolo IX)[44]. In particolare i sistemi di intelligenza a rischio inaccettabile sono quelli che: (i) utilizzano «tecniche subliminali che agiscono senza che una persona ne sia consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico» (così art. 5, par. 1, lett. a)); (ii) sfruttano «le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico» (così art. 5, par. 1, lett. b)); (iii) sono utilizzati «da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato pe-

AI in EU law: lessons learned from the Artificial Intelligence Act (AIA) with its drawbacks, in *Transforming Government: People, Process and Policy*, 16, 3, 2022, p. 359 ss.; J. Mökander - P. Juneja - D.S. Watson - L. Floridi, *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?*, in *Minds and Machines*, 32, 4, 2022, p. 751 ss.; G. Finocchiaro, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubb.*, 4, 2022, p. 1085 ss.; J. Schuett, *Risk management in the artificial intelligence act*, in *Eur. J. Risk Reg.*, 2023, p. 1 ss.

[44] Sulla classificazione dei sistemi di intelligenza artificiale in base al livello di rischio proposta dall'*Artificial Intelligence Act* v. in particolare M. Veale - F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, in *Computer L. Rev. Int'l*, 4, 2021, p. 97 ss.; J. Chamberlain, *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, in *Eur. J. Risk Reg.*, 14, 2023, p. 1 ss.

 ISSN 2037-5662

riodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi i seguenti scenari: i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti; ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di interi gruppi di persone fisiche che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità» (così art. 5, par. 1, lett. c)). Ora, questi sistemi secondo la proposta di regolamento sono da considerarsi vietati anche se è previsto un divieto (non assoluto) di utilizzo dei «sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto» (così art. 5, par. 1, lett. d)). Più precisamente l'uso di questi sistemi è ammesso solo se strettamente necessario per perseguire uno dei seguenti obiettivi: «i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, par. 2, della decisione quadro 2002/584/GAI del Consiglio, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni, come stabilito dalla legge di tale Stato membro» (così art. 5, par. 1, lett. d)). Ed in ogni caso il loro utilizzo «è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso» (così art. 5, par. 3).

I sistemi di intelligenza artificiale sono invece considerati ad alto rischio se «il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II; b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II» (così art. 6, par. 1). Inoltre «sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III» (così art. 6, par. 2). E con riferimento a questi sistemi l'*Artificial Intelligence Act* ammette il loro l'utilizzo

3/2023

 ISSN 2037-5662

prevedendo però al tempo stesso una serie di tutele anche nell'ambito della privacy, tra cui l'introduzione di un «sistema di gestione dei rischi» al fine di identificare e valutare i rischi, nonché adottare adeguate misure per la gestione di essi (così art. 9) e l'obbligo di redigere una documentazione tecnica prima della loro immissione sul mercato o messa in servizio (così art. 11), oltre alla previsione di cautele nello sviluppo e nella progettazione di questi sistemi (così artt. 14 e 15).

I sistemi di intelligenza artificiale che comportano rischi limitati sono invece: (i) quelli destinati a interagire con le persone fisiche; (ii) i sistemi di riconoscimento delle emozioni e quelli di categorizzazione biometrica; (iii) nonché i sistemi che generano o manipolano immagini o contenuti audio o video che assomigliano molto a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero sembrare falsamente autentici o veritieri. E con riferimento a questi sistemi l'*Artificial Intelligence Act* ammette il loro l'utilizzo a condizione che vengano rispettati determinati obblighi di trasparenza. Più precisamente (i) i fornitori devono assicurare che «i sistemi di IA destinati a interagire con le persone fisiche siano progettati e sviluppati in modo tale che le persone fisiche siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo»; (ii) «gli utenti di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema»; e (iii) «gli utenti di un sistema di IA che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ("deep fake") sono tenuti a rendere noto che il contenuto è stato generato o manipolato artificialmente» (così art. 52, parr. 1, 2 e 3).

Ed infine i sistemi di intelligenza artificiale a minimo rischio sono quelli che non possiedono i requisiti per essere classificati come sistemi di intelligenza artificiale a rischio inaccettabile, ad alto rischio e a rischio limitato e sono ad esempio i giochi per computer o i sistemi di assistenza clienti. Qui la proposta di regolamento consente il loro sviluppo ed utilizzo nell'Unione senza imporre alcun obbligo[45]. E resta da dire che rispetto a questi sistemi

[45] Rimane poi da precisare che la proposta di regolamento prevede misure a sostegno dell'innovazione (così il titolo V), introduce un Comitato europeo per l'intelligenza artificiale

3/2023

972

 ISSN 2037-5662

di intelligenza artificiale che comportano rischi minimi, la proposta di regolamento promuove e ad un tempo incoraggia l'elaborazione di codici di condotta (così art. 69).

In sintesi. L'*Artificial Intelligence Act* diversifica le forme di intervento a seconda del rischio del servizio seguendo un approccio basato sul rischio e imponendo «oneri normativi soltanto laddove un sistema di» intelligenza artificiale «possa comportare rischi alti per i diritti fondamentali e la sicurezza» mentre «per altri sistemi […] non ad alto rischio sono imposti soltanto obblighi di trasparenza molto limitati, ad esempio in termini di fornitura di informazioni per segnalare l'utilizzo di un sistema di IA nelle interazioni con esseri umani»[46]. Ne deriva un quadro normativo dove la regolazione è incentrata non tanto sulle caratteristiche soggettive del fornitore del servizio, quanto su quelle oggettive del servizio di intelligenza artificiale che a seconda del rischio subirà maggiori limitazioni anche nel trattamento dei dati di una persona.

9. In questo quadro viene da chiedersi come si coordineranno la normativa in materia di privacy e quella di intelligenza artificiale ove quest'ultima verrà adottata. A questo proposito la relazione introduttiva dell'*Artificial Intelligence Act* specifica chiaramente che intende introdurre una disciplina volta (non a sostituire, ma) ad integrare le previsioni del GDPR: «la proposta non pregiudica il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva (UE) 2016/680) e li integra con una serie di regole armonizzate»[47]. Ma al di là di questa formula generale di coordinamento l'*Artificial Intelligence Act* prevede una serie di specifiche disposizio-

(così il titolo VI), istituisce una banca dati dell'UE contenente le informazioni relative ai sistemi di intelligenza artificiale ad alto rischio (così il titolo VII) e prevede specifiche disposizioni volte sia a monitorare i sistemi di intelligenza artificiale dopo la loro immissione sul mercato che a condividere le informazioni su di essi (così il titolo VIII).

[46] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, SWD(2021) 84 final, Brussels, Explanatory Memorandum, April 21, 2021, p. 7.

[47] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*, SWD(2021) 84 final, Brussels, Explanatory Memorandum, April 21, 2021, p. 4.

 ISSN 2037-5662

ni in materia di trattamento dei dati. (i) In particolare all'art. 5 ammette l'uso dei «sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto», solo se questo utilizzo è necessario per perseguire uno degli obiettivi stabiliti dall'art. 5, par. 1, lett. d)[48]; è autorizzato da un'autorità giudiziaria o da un'autorità amministrativa indipendente[49]. (ii) Inoltre specifica con riferimento ai dati biometrici che qualsiasi loro trattamento «come pure di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica, diverso da quello connesso all'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto disciplinato dal presente regolamento, compresi i casi in cui tali sistemi sono utilizzati dalle autorità competenti in spazi accessibili al pubblico per fini diversi dalle attività di contrasto, dovrebbe continuare a soddisfare tutti i requisiti derivanti dall'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, dall'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725 e dall'articolo 10 della direttiva (UE) 2016/680, a seconda dei casi» (così il considerando 24). (iii) Ancora introduce ulteriori forme di tutela della privacy dell'utente prevedendo che i sistemi di intelligenza artificiale ad alto rischio devono essere accompagnati da una serie di «informazioni concise, complete, corrette

[48] Secondo l'art. 5, par. 1, lett. d) dell'*Artificial Intelligence Act* «l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti obiettivi: i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; iii) il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio».

[49] L'art. 5, par. 3, prevede infatti che «per quanto riguarda il paragrafo 1, lettera d), e il paragrafo 2, ogni singolo uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità alle regole dettagliate del diritto nazionale di cui al paragrafo 4. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione e richiedere l'autorizzazione solo durante o dopo l'uso. L'autorità giudiziaria o amministrativa competente rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, lettera d), come indicato nella richiesta. Nel decidere in merito alla richiesta, l'autorità giudiziaria o amministrativa competente tiene conto degli elementi di cui al paragrafo 2».

 ISSN 2037-5662

e chiare che siano pertinenti, accessibili e comprensibili per gli utenti»[50] (così art. 13, par. 2), devono essere sviluppati e progettati «anche con strumenti di interfaccia uomo-macchina adeguati» (così art. 14, par. 1) e «in modo tale da conseguire, alla luce della loro finalità prevista, un adeguato livello di accuratezza, robustezza e cibersicurezza e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita» (così art. 15, par. 1). (iv) Ancora prevede che i sistemi di intelligenza artificiale ad alto rischio volti a prevedere l'uso di dati per l'addestramento di modelli devono essere sviluppati rispettando determinati criteri di qualità e precisamente «i set di dati di addestramento, convalida e prova devono essere pertinenti, rappresentativi, esenti da errori e completi» (così art. 10, par. 2) e «nella misura in cui ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, i fornitori di tali sistemi possono trattare categorie particolari di dati personali» a condizione che vengano garantite «tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata» (così art. 10, par. 5). (v) Ed infine prevede all'art. 54, par. 1, che «nello spazio di sperimentazione normativa per l'IA i dati personali legalmente raccolti per altre finalità sono trattati ai fini dello sviluppo e delle prove nello spazio di sperimentazione di determinati sistemi di IA innova-

[50] Secondo l'art. 13, par. 3, «le informazioni di cui al paragrafo 2 specificano: a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato; b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui: i) la finalità prevista; ii) il livello di accuratezza, robustezza e cibersicurezza di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato e che ci si può attendere, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersicurezza; iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali; iv) le sue prestazioni per quanto riguarda le persone o i gruppi di persone sui quali il sistema è destinato a essere utilizzato; v) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA; c) le eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni, che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità; d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte degli utenti; e) la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti software».

 ISSN 2037-5662

tivi alle seguenti condizioni». Ma al tempo stesso prevede le condizioni che legittimano questo trattamento come ad esempio l'esistenza di «meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti fondamentali degli interessati durante la sperimentazione» (così art. 54, par. 1, lett. c)), la garanzia che questi dati saranno «cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali» (così art. 54, par. 1, lett. g)), la presenza di «una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica» (così art. 54, par. 1, lett. i)[51].

[51] Più precisamente il trattamento di questi dati è legittimo alle seguenti condizioni: «a) i sistemi di IA innovativi sono sviluppati per salvaguardare un interesse pubblico rilevante in uno o più dei seguenti settori: i) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse, sotto il controllo e la responsabilità delle autorità competenti. Il trattamento si basa sul diritto degli Stati membri o dell'Unione; ii) la sicurezza pubblica e la sanità pubblica, compresi la prevenzione, il controllo e il trattamento delle malattie; iii) un elevato livello di protezione e di miglioramento della qualità dell'ambiente; b) i dati trattati sono necessari per il rispetto di uno o più dei requisiti di cui al titolo III, capo 2, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento anonimizzato, sintetico o di altri dati non personali; c) esistono meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti fondamentali degli interessati durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento; d) i dati personali da trattare nel contesto dello spazio di sperimentazione sono in un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo dei partecipanti e solo le persone autorizzate hanno accesso a tali dati; e) i dati personali trattati non devono essere trasmessi, trasferiti o altrimenti consultati da terzi; f) il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati; g) i dati personali trattati nell'ambito dello spazio di sperimentazione sono cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali; h) i log del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione e per 1 anno dopo la sua cessazione, al solo scopo di adempiere gli obblighi di rendicontazione e documentazione previsti dal presente articolo o da altre normative applicabili dell'Unione o degli Stati membri e solo per il tempo necessario per adempiere tali obblighi; i) una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica di cui all'allegato IV; j) una breve sintesi del progetto di IA sviluppato nello spazio di sperimentazione, dei suoi obiettivi e dei risultati attesi è pubblicata sul sito web delle autorità competenti» (così art. 54, par. 1).

 ISSN 2037-5662

10. Certo le due normative mi sembra mirino entrambe ad incentivare la circolazione dei dati personali. In particolare, il GDPR prevede una disciplina che non vuole ostacolare il flusso dei dati, ma anzi ne incentiva la circolazione. A questo proposito il GDPR ha anzitutto riconosciuto all'interessato la facoltà di consentire la circolazione dei propri dati con un consenso che può avere natura contrattuale[52] proponendo un modello di circolazione dei dati di tipo negoziale. Questo regolamento ha poi introdotto una serie di rimedi che consentono all'interessato di controllare la circolazione dei dati personali ulteriori rispetto alla direttiva sulla privacy come il diritto di revocare il consenso al trattamento dei dati, il diritto alla portabilità dei dati, il diritto di non essere oggetto di una decisione basata esclusivamente sul trattamento automatizzato e il diritto all'anonimato dei dati. In questo modo il GDPR mi sembra incoraggi l'interessato a prestare il proprio consenso al trattamento facendolo sentire maggiormente tutelato da una circolazione controllata dei dati. E tutto ciò ha chiaramente l'obiettivo di incentivare la circolazione dei dati personali. D'altro canto, il GDPR prevede al considerando n. 4 che «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo» e «non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice

3 / 2023

[52] Sulla natura contrattuale del consenso v. S. Patti, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, p. 455; G. Resta, *Autonomia privata e diritti della persona*, Napoli, 2005, p. 305; D.J. Solove, *Introduction: Privacy Selfmanagement and The Consent Dilemma*, in *Harv. L. Rev.*, 216, 2013, p. 1883; E. Kosta, *Consent in European Data Protection Law*, Leiden-Boston, 2013, p. 8; K. Pormeister, *Informed consent to sensitive personal data processing for the performance of digital consumer contracts on the example of «23andMe»*, in *EuCML*, 6, 2017, p. 17; G. Resta, *Diritti fondamentali e diritto privato nel contesto digitale: un inventario di problemi*, in *Effettività e Drittwirkung: idee a confronto. Atti del convegno Pisa, 24-25 febbraio 2017*, a cura di E. Navarretta, Torino, 2017, p. 182; F. Bravo, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. Finocchiaro, Torino, 2017, p. 162; S. Thobani, *Diritti della personalità e contratto*, cit., p. 187; R. Senigalia, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2020, p. 772.

 ISSN 2037-5662

imparziale, nonché la diversità culturale, religiosa e linguistica»[53]. Ne deriva un GDPR volto a tutelare e bilanciare anche in diverse disposizioni l'interesse della collettività a conoscere alcuni dati personali che possono essere di pubblico interesse come pure in altri casi delle banche dati nella raccolta dei dati. E tutto ciò viene effettuato dal legislatore per favorire la circolazione dei dati[54]. Infatti «per [...] prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese» e «per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali» (così il considerando 13 del GDPR)[55].

3/2023

[53] Il principio sancito in questo considerando è stato confermato dalla Corte di Giustizia: v. per esempio Corte di giustizia 24 settembre 2019, *GC, AF, BH, ED c. Commission nationale de l'informatique et des libertés*, C-136/2017, par. 57 secondo cui «il diritto alla protezione dei dati personali non è un diritto assoluto, ma deve, come sottolinea il considerando 4 di detto regolamento, essere considerato in relazione alla sua funzione sociale ed essere bilanciato con altri diritti fondamentali, conformemente al principio di proporzionalità»; Corte Giust. UE, 24 settembre 2019, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17, par. 60 secondo cui «il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»; Corte Giust. UE, 22 giugno 2021, *B c. Latvijas Republikas Saeima*, C-439/2019, par. 105 secondo cui «i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali non sono prerogative assolute, ma vanno considerati alla luce della loro funzione sociale e bilanciati con altri diritti fondamentali».

[54] Sull'evoluzione degli interessi coinvolti nella circolazione dei dati v. T.M. Ubertazzi, *Rethinking the withdrawal of consent in the functional perspective of privacy*, cit., p. 39 ss.

[55] Il tema della protezione della libera circolazione dei dati personali è stato trattato nei considerando del GDPR. In particolare il considerando n. 6 ha riconosciuto che «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali». Per garantire la libera circolazione dei dati personali, il considerando n. 10 ha precisato che «al fine di [...] e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle

 ISSN 2037-5662

Analogamente anche l'*Artificial Intelligence Act* ha dichiaratamente lo «scopo […] di migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale (IA) in conformità ai valori dell'Unione. Il presente regolamento persegue una serie di motivi imperativi di interesse pubblico, quali un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali, e garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento» (così il considerando 1). D'altro canto «i sistemi di intelligenza artificiale (sistemi di IA) possono essere facilmente impiegati in molteplici settori dell'economia e della società, anche a livello transfrontaliero, e circolare in tutta l'Unione» ed è «pertanto opportuno garantire un livello di protezione costante ed elevato in tutta l'Unione, mentre dovrebbero essere evitate le divergenze che ostacolano la libera circolazione dei sistemi di IA e dei relativi prodotti e servizi nel mercato interno, stabilendo obblighi uniformi per gli operatori» (così il considerando 2). Ne deriva che questo regolamento ha come primario obiettivo quello di regolare questa tecnologia senza impedirne l'utilizzo dato che «l'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, può contribuire al conseguimento di risultati vantaggiosi dal punto di vista sociale e ambientale nonché fornire vantaggi competitivi fondamentali alle imprese e all'economia europea». E per conseguenza in ragione degli innumerevoli vantaggi apportati dall'intelligenza artificiale la strategia europea in materia di intelligenza artificiale è volta a promuovere lo sviluppo di questa tecnologia favorendo la circolazione e la condivisione dei dati all'interno dell'UE.

libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri». Inoltre l'importanza della libera circolazione dei dati nel mercato interno è stata ulteriormente sottolineata nel considerando n. 13 in base al quale «per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

 ISSN 2037-5662

ABSTRACT

Oggigiorno si assiste all'avvento dell'intelligenza artificiale e dunque di una tecnologia che potrebbe per certi versi rideterminare un nuovo scenario in materia di dati personali. Infatti, la capacità di questa tecnologia di raccogliere dati e ad un tempo auto-apprendere la conoscenza di essi mette in crisi i precedenti modelli di circolazione delle informazioni. In questo quadro lo scenario che si sta delineando altro non è che una naturale evoluzione di un mercato delle informazioni che ormai non può più essere ostacolato ed anzi deve essere incentivato in quanto fonte di benessere per l'intera collettività. Questo studio analizza alcuni aspetti dei rapporti tra privacy e intelligenza artificiale.

Today, we are witnessing the advent of artificial intelligence, the technology which could in some ways shape a new scenario in the field of personal data. In fact, the ability of this technology to collect data and, at the same time, learn about them may undermine previous information circulation models. In this context, the scenario that emerges is nothing else than a natural evolution of the information market that can no longer be hindered and should even be encouraged as a source of wealth for the entire community. This paper analyses some aspects of the relationship between privacy and artificial intelligence.

3 / 2023

980

 ISSN 2037-5662