



GIANLUCA CONTALDI*

INTELLIGENZA ARTIFICIALE E DATI PERSONALI

SOMMARIO: – 1. I lavori preparatori di una regolamentazione europea dell'intelligenza artificiale. – 2. La proposta di regolamento presentata dalla Commissione europea lo scorso mese di aprile. – 3. L'applicazione cumulativa del reg. 2016/679 sulla protezione dei dati personali e della proposta di regolamento sull'intelligenza artificiale (quando sarà adottata dal Parlamento e dal Consiglio). – 4. *Segue*. L'individuazione del titolare del trattamento. – 5. L'applicazione concreta di talune previsioni del regolamento sulla protezione dei dati personali alla futura disciplina dell'intelligenza artificiale. La raccolta dei dati ed i principi di minimizzazione, di prestazione del consenso e di anonimizzazione. – 6. *Segue*. I dati a carattere discriminatorio e il diritto alla spiegazione della logica sottesa al funzionamento dei sistemi di intelligenza artificiale. – 7. I c.d. «spazi di sperimentazione». – 8. Conclusioni.

1. I lavori preparatori di una regolamentazione europea dell'intelligenza artificiale

Con l'espressione intelligenza artificiale si fa abitualmente riferimento a macchine dotate di una relevantissima capacità di calcolo. I sistemi di intelligenza artificiale sono, infatti, dei computer (e dei programmi per elaboratore) che combinano grandi quantità di dati (c.d. *Big Data*), con la finalità di imparare a gestire i futuri processi decisionali. In realtà, l'epiteto di intelligenza è, probabilmente, eccessivamente enfatico¹: è, infatti, evidente che non si tratta di macchine capaci di assumere vere e proprie decisioni, ma più semplicemente di trarre determinate conclusioni dai dati desumibili dalle esperienze pregresse². Peraltro la capacità di questi sistemi consiste nell'elaborare e combinare elementi anche fortemente eterogenei, per trovare nessi e giungere a determinazioni che non sarebbe possibile cogliere in altro modo.

Attualmente, le tecnologie più innovative sono nel possesso degli Stati Uniti e della

* Professore ordinario di Diritto dell'Unione europea nell'Università degli Studi di Macerata. Il testo riproduce, con talune modifiche, la relazione presentata in occasione del Seminario di Napoli, del 12 luglio 2021, dal titolo *Le piattaforme digitali tra mercato e diritti*.

¹ Si riporta che il termine venne scelto accuratamente, nel 1956, dai ricercatori americani del Dartmouth College di Hanover, con il preciso intento di motivare le future generazioni di scienziati a spendere energie nel campo delle scienze computazionali e, dall'altro, di attrarre gli investitori (v. L. FLORIDI, F. CABITZA, *Intelligenza artificiale. L'uso delle nuove macchine*, Lavis (TN), 2021, p. 9 s.).

² T. GILLESPIE, *The Relevance of Algorithms*, in T. GILLESPIE, P.J. BOCZKOWSKI, K.A. FOOT (eds.), *Media Technologies: Essays on Communication, Materiality, and Society*, Massachussets, 2014, p. 167 ss.

Cina, con il risultato che l'Unione europea si è trovata in difetto nello sfruttamento economico dell'intelligenza artificiale. Tali sistemi sono d'altronde così sofisticati che, di fatto, sono capaci non solo di comprendere l'evoluzione del gusto degli utenti, ma, entro certi limiti, anche di prevedere eventi futuri, come l'esito di talune tornate elettorali o lo sviluppo geografico di determinate pandemie³. Gli impieghi dell'intelligenza artificiale sono, oggi, a tal punto estesi, che essi trascendono lo stesso ambito economico, per investire settori quali il controllo dell'ordine pubblico nei grandi centri urbani⁴, la gestione della rete dei trasporti pubblici, i flussi di traffico, il controllo delle fonti di inquinamento, la sanità pubblica e la telemedicina⁵. In altri termini, una serie di settori che finiscono per influire anche sullo sviluppo umano e sul benessere collettivo della società. Questo ha determinato la consapevolezza nella Commissione europea che vi sia un *gap* da recuperare in termini economici, sociali e giuridici nei confronti dei predetti paesi extraeuropei.

I lavori per l'elaborazione di una regolamentazione europea dell'intelligenza artificiale cominciarono con un'iniziativa del Parlamento europeo, con la quale venne conferito l'incarico ad un gruppo di esperti, coordinato dalla relatrice Mady Delvaux, di predisporre un rapporto preparatorio e di individuare i principi giuridici, etici e deontologici ai quali avrebbe dovuto rispondere un'eventuale proposta di regolamento sull'intelligenza artificiale.

Il rapporto Delvaux fu poi approvato con la risoluzione del 16 febbraio 2017⁶. Il rapporto, per la verità, è stato oggetto di critiche, dal momento più che elaborare autonomi, sembrava piuttosto ricalcare talune regole etiche ipotizzate in altri contesti⁷. A parte la scarsa originalità nel contenuto⁸, forse imputabile più all'andamento dei lavori preparatori che al rapporto in sé, la Risoluzione finale del Parlamento europeo contiene indubbiamente anche diverse riflessioni utili. Innanzitutto essa afferma chiaramente che la materia necessita di una regolamentazione specifica e che l'assetto giuridico esistente non sia sufficiente a disciplinare

³ Sul tema, v. A. VESPIGNANI, *L'algoritmo e l'oracolo*, Milano, 2019.

⁴ Tali sistemi consentono, infatti, di individuare le zone potenzialmente più pericolose. In questo modo si riescono a gestire le forze di polizia in maniera più efficiente (C. CASTETS-RENARD, *Human Rights and Algorithmic Impact Assessment for Predictive Policing*, in H.W. MICKLITZ, O. POLLICINO, A. REICHMAN, A. SIMONCINI, G. SARTOR, G. DE GREGORIO (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2022 (versione online già accessibile), p. 93 ss.).

⁵ V. le linee guida elaborate dall'Organizzazione mondiale della sanità (*Ethics and Governance of Artificial Intelligence for Health, WHO Guidance*, consultabili al sito file:///C:/Users/utente/Downloads/WHO_Ethics+and+Governance+of+AI.pdf).

⁶ V. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, (2015/2013(INL)), 2018/C 252/25, in GU C 252/239, del 18.7.2018.

⁷ V. la Relazione presentata il 27.1.2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), punti U e V: «considerando che le leggi di Asimov devono essere considerate come rivolte ai progettisti, ai fabbricanti e agli utilizzatori di robot, compresi i robot con capacità di autonomia e di autoapprendimento integrate, dal momento che tali leggi non possono essere convertite in codice macchina; considerando che è necessaria una serie di norme che disciplinino in particolare la responsabilità, la trasparenza e l'assunzione di responsabilità e che riflettano i valori intrinsecamente europei, universali e umanistici che caratterizzano il contributo dell'Europa alla società; che tali regole non devono influenzare il processo di ricerca, innovazione e sviluppo nel settore della robotica». Le leggi della robotica, menzionate nel passaggio ora riportato, vennero elaborate dal noto autore russo, naturalizzato statunitense, nel corso di uno scritto del 1942 e vennero successivamente riprese in altri lavori («(1) Un robot non può recar danno a un essere umano né può permettere che, a causa del proprio mancato intervento, un essere umano riceva danno. (2) Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non contravvengano alla Prima Legge. (3) Un robot deve proteggere la propria esistenza, purché questa autodifesa non contrasti con la Prima o con la Seconda Legge»; v. la raccolta di racconti di I. ASIMOV, *Io robot*, recentemente ripubblicata in Italia da Mondadori, Milano, 2021).

⁸ V. A. ZORNOVA, A. LAUKYTE, *Robotica e diritto: riflessioni e critiche sull'ultima iniziativa di regolamentazione in Europa*, in *Contr. impr. Eur.*, 2016, p. 808 ss., 811 ss.

l'industria che sfrutta i meccanismi dell'intelligenza artificiale. In secondo luogo, la risoluzione fa presente che la macchina, in quanto tale, non può assumere una personalità giuridica. Discende da tale riflessione la conseguenza che gli obblighi che deriveranno dagli strumenti legislativi che saranno introdotti a livello europeo si applicheranno agli ideatori del sistema ovvero ai progettisti; ma mai alla macchina in sé, che è insuscettibile di essere destinataria di situazioni giuridiche soggettive⁹.

Successivamente, il tema della regolamentazione dell'intelligenza artificiale venne posto all'ordine del giorno dal Consiglio europeo di Tallin del 29 settembre 2017, nel corso del quale, gli Stati membri rinnovarono l'impegno a completare rapidamente il c.d. mercato unico digitale¹⁰. Di fatto, non vi fu nessun passo avanti significativo, fino alla Dichiarazione sulla cooperazione in materia di intelligenza artificiale, firmata da venticinque Stati membri in data 10 aprile 2018. Con essa i paesi firmatari, oltre a rinnovare l'impegno ad incrementare gli investimenti per consentire la creazione di un'industria digitale europea, stabilirono che la successiva regolamentazione dell'intelligenza artificiale avrebbe dovuto essere frutto di un "bilanciamento" con gli altri diritti fondamentali, quali, in particolare, la tutela della *privacy*¹¹.

A tale dichiarazione comune fece poi seguito una Comunicazione della Commissione europea, del 25 aprile 2018, con la quale, a fronte degli ingenti investimenti necessari, l'organo esecutivo ravvisava la necessità di coinvolgere anche i privati nella raccolta dei dati e nello sviluppo degli strumenti tecnici idonei. Per quanto concerne l'impatto dell'uso dei sistemi di intelligenza artificiale la tutela dei diritti fondamentali, l'organo esecutivo ometteva, in realtà, di assumere una determinazione conclusiva, limitandosi a conferire il mandato ad un apposito

⁹ La Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, cit., par. 59, lett. f, suggeriva alla Commissione di prevedere: «l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome». Questo punto della Risoluzione ha suscitato svariate critiche, anche a livello degli organi europei. In via esemplificativa, il Comitato economico e sociale, nel parere del 31 agosto 2017, ha espressamente raccomandato: «di adottare, nei confronti dell'IA, l'approccio «human-in-command», con la condizione essenziale che l'IA sia sviluppata in maniera responsabile, sicura e utile, e che la macchina rimanga macchina e l'uomo ne mantenga il controllo in ogni momento» (*Parere del Comitato economico e sociale europeo su «L'intelligenza artificiale — Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società» (parere d'iniziativa)*, GU C 288, 31.8.2017, p. 1–9). Il punto è che l'attribuzione di una personalità giuridica, allo stato di attuale evoluzione giuridica, implicherebbe anche una forma di responsabilità patrimoniale del sistema di intelligenza artificiale in sé, che in luogo di quella degli ideatori, produttori ed utilizzatori del sistema. Per la discussione del tema v. G. DE ANNA, *Automi, responsabilità e diritto*, in *Rivista di filosofia del diritto*, 2019, p. 125 ss.; A. DRIGO, *Sistemi emergenti di Intelligenza Artificiale e personalità giuridica: un contributo interdisciplinare alla tematica*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era della intelligenza artificiale*, Pisa, 2020, p. 179 ss.; R. TREZZA, *Diritto e intelligenza artificiale. Etica-Privacy-Responsabilità-Decisione*, Pisa, 2020, p. 49 ss.; P. MORO, *Alle frontiere della soggettività: indizi di responsabilità delle macchine intelligenti*, in U. RUFFOLO (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, p. 55 ss.; U. RUFFOLO, *La personalità elettronica tra "doveri" e "diritti" della macchina*, ivi, p. 115 ss.; G.P. CIRILLO, *I soggetti giuridici digitali*, in *Contr. impr.*, 2020, p. 574 ss.

¹⁰ Le conclusioni del Vertice di Tallin si trovano allegate alle conclusioni del Consiglio europeo del 19 ottobre 2017, Bruxelles, 19 ottobre 2017, EUCO 14/17, CO EUR 17, CONCL 5.

¹¹ *EU Declaration on Cooperation on Artificial Intelligence*, 10 aprile 2018, consultabile al sito <https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence>: «Ensuring an adequate legal and ethical framework, building on EU fundamental rights and values, including privacy and protection of personal data, as well as principles such as transparency and accountability».

gruppo di esperti¹². In una successiva comunicazione, del dicembre 2018, con la quale fu approvato un vero e proprio piano coordinato per lo sviluppo dell'intelligenza artificiale¹³, la Commissione chiarì, tuttavia, che lo sviluppo dei sistemi di intelligenza artificiale avrebbe dovuto tenere conto del quadro giuridico preesistente e, per quanto ci riguarda ai fini del prosieguo di questo scritto, di quello posto a protezione dei dati personali¹⁴.

Le conclusioni del Gruppo di esperti chiamato ad elaborare i principi etici che devono soprassedere allo sviluppo dell'intelligenza artificiale vennero infine presentate, in forma definitiva, nel marzo 2019, con la significativa denominazione di *Orientamenti*¹⁵. In essi si sottolineava che qualunque regolamentazione dell'IA dovesse essere incentrata sull'uomo (dovesse essere, in altri termini, antropocentrica). Questo implicava che i programmi di intelligenza artificiale dovevano sempre consentire un intervento umano per assumere le decisioni necessarie, eventualmente anche escludendo in concreto il sistema di intelligenza artificiale.

Con specifico riferimento alla tutela dei dati personali, gli Orientamenti precisavano che: «(i) sistemi di IA devono *garantire la riservatezza e la protezione dei dati durante l'intero ciclo di vita del sistema*»¹⁶. In secondo luogo, il Gruppo di esperti ribadiva la necessità, già individuata dalla Commissione, che occorresse sempre garantire una qualche forma di supervisione da parte dell'essere umano¹⁷.

In definitiva gli orientamenti del Gruppo di esperti sembrano suggerire due aspetti che troveremo anche nella successiva proposta di regolamento sull'intelligenza artificiale. Innanzitutto, la necessità che vi sia sempre un controllo da parte di un soggetto umano sul funzionamento dei sistemi di IA; e, in secondo luogo, che non si possa prescindere dalla protezione dei diritti fondamentali e, per quanto ci interessa ai fini del prosieguo del nostro lavoro, quella sulla protezione dei dati personali.

¹² Comunicazione della Commissione, *L'intelligenza artificiale per l'Europa*, Bruxelles, 25.4.2018, COM(2018) 237 final: «Come primo passo per affrontare i problemi etici, un progetto di orientamenti etici per l'IA sarà elaborato entro la fine dell'anno, nel rispetto della Carta dei diritti fondamentali dell'Unione Europea. La Commissione radunerà tutti le parti interessate allo scopo di aiutare a elaborare questo progetto di orientamenti. Il progetto affronterà temi quali il futuro del lavoro, l'equità, la sicurezza, l'inclusione sociale e la trasparenza degli algoritmi. Più in generale esso esaminerà l'impatto sui diritti fondamentali, tra cui la vita privata, la dignità, la tutela dei consumatori e la non discriminazione».

¹³ Comunicazione della Commissione al Parlamento europeo, al Consiglio Europeo, Al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Piano coordinato sull'Intelligenza Artificiale*, Bruxelles, 7.12.2018, Com(2018) 795 Final.

¹⁴ Comunicazione della Commissione al Parlamento europeo, al Consiglio Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Piano coordinato sull'Intelligenza Artificiale*, cit.: «(l)'apertura ai flussi di dati internazionali continuerà ad essere garantita nel pieno rispetto delle norme dell'UE per la protezione dei dati personali e in conformità agli strumenti giuridici applicabili».

¹⁵ Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea nel giugno 2018, *Orientamenti etici per un'IA affidabile*, consultabile online al sito file:///c:/users/utente/appdata/local/temp/ethics_guidelines_for_trustworthy_ai-it_87fea6d2-977e-4064-0532c4315eb55247_60430.pdf.

¹⁶ Gruppo indipendente di esperti ad alto livello, *Orientamenti etici per un'IA affidabile*, cit., punto 72.

¹⁷ Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, *Orientamenti etici per un'IA affidabile*, cit., punto 65: «La sorveglianza umana aiuta a garantire che un sistema di IA non comprometta l'autonomia umana o provochi altri effetti negativi. La sorveglianza può avvenire mediante meccanismi di governance che consentano un approccio con intervento umano (human-in-the-loop - HITL), con supervisione umana (human-on-the-loop - HOTL) o con controllo umano (human-in-command - HIC). L'approccio HITL prevede la possibilità di intervento umano in ogni ciclo decisionale del sistema, che in molti casi non è né possibile né auspicabile. L'approccio HOTL prevede l'intervento umano durante il ciclo di progettazione del sistema e il monitoraggio del funzionamento del sistema».

Tale approccio trova, d'altro canto, conferma anche nei lavori condotti in seno al Consiglio d'Europa, nell'ambito del quale, il Comitato consultivo (cd. T-PD) della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108), ha avuto modo di chiarire che «(i)n tutte le fasi del trattamento, compresa la raccolta dei dati, gli sviluppatori, i produttori e i fornitori di servizi di IA dovrebbero adottare un approccio volto a tutelare i diritti umani fin dalla progettazione dei tali servizi (“human rights by design”) ed evitare qualsiasi potenziale pregiudizio (*bias*), anche involontario o occulto, il rischio di discriminazione o altri effetti negativi sui diritti umani e le libertà fondamentali degli interessati. Gli sviluppatori di IA dovrebbero vagliare accuratamente la qualità, la natura, l'origine e la quantità di dati personali utilizzati, riducendo i dati inutili, ridondanti o marginali durante lo sviluppo e le fasi di addestramento e poi monitorando l'accuratezza del modello man mano che viene alimentato con nuovi dati»¹⁸.

Quindi, anche all'esterno dell'Unione europea, si ribadisce che spetta agli sviluppatori dei sistemi di IA progettare i sistemi tenendo conto del diritto dell'interessato a non essere sottoposto esclusivamente ad una decisione automatizzata, nonché di evitare che gli algoritmi posti alla base del sistema si fondino su pregiudizi ovvero siano, in sé, fonte di discriminazioni.

Da ultimo, nel mese di febbraio 2020, viene pubblicato il Libro bianco sull'intelligenza artificiale, secondo il quale, lo sviluppo di sistemi siffatti deve essere trasparente, consentire all'interessato di decidere, in piena autonomia, di non venire sottoposto solo ad una decisione automatizzata¹⁹.

Dopo la pubblicazione del Libro bianco gli eventi si sono susseguiti in maniera tumultuosa. Innanzitutto la Commissione lanciò un sondaggio, che coinvolse membri della società civile, imprese operanti nel settore e accademici, al fine di raccogliere le diverse opinioni.

Successivamente, il Consiglio europeo invitò espressamente la Commissione a presentare una proposta legislativa. Secondo il Consiglio europeo, la proposta avrebbe dovuto «salvaguardare i nostri valori nonché i nostri diritti fondamentali e la nostra sicurezza ed essere socialmente equilibrato. Tale approccio antropocentrico aumenterà l'attrattiva del

¹⁸ Strasburgo, 25 Gennaio 2019 T-PD(2019)01, Comitato consultivo (cd. T-PD) della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (convenzione 108), *Linee-guida in materia di intelligenza artificiale e protezione dei dati*. La Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione 108), è stata aperta alla firma a Strasburgo, il 29 gennaio 1981. Dal momento che il testo era stato concepito prima della diffusione massiva di internet, la stessa è stata recentemente oggetto di un Protocollo di modifica (Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)), approvato dal Consiglio in occasione della riunione del 17 e 18 maggio 2018, ad Elsinore, in Danimarca. Per l'Italia v. la 22 aprile 2021, n. 60, Ratifica ed esecuzione del Protocollo di emendamento alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, fatto a Strasburgo il 10 ottobre 2018, in GU, Serie Generale n.110 del 10-05-2021. Lo strumento non è ancora in vigore sul piano internazionale.

¹⁹ Commissione europea, Bruxelles, 19.2.2020, COM(2020) 65 final, *Libro bianco sull'intelligenza artificiale*. «La trasparenza è necessaria anche al di là degli obblighi di tenuta dei registri di cui al punto c). Al fine di conseguire gli obiettivi perseguiti, in particolare promuovere un uso responsabile dell'IA, rafforzare la fiducia e agevolare la riparazione del danno ove necessario, è importante che vengano fornite in maniera proattiva informazioni adeguate sull'uso dei sistemi di IA ad alto rischio». Tale pubblicazione fa seguito all'impegno politico assunto dalla stessa Presidente, nel luglio 2019, con il quale la stessa dichiarò che la Commissione avrebbe presentato una proposta per consentire all'Unione europea di stabilire gli standard regolativi globali della materia (v. U. VON DER LEYEN, *Orientamenti politici per la prossima Commissione europea 2019-2024*, consultabile al sito <https://op.europa.eu/it/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1>).

modello europeo»²⁰. La rilevanza del rispetto dei diritti fondamentali nel funzionamento dei sistemi di intelligenza artificiale non sarebbe stata, quindi, fine a se stessa, ma avrebbe contribuito a garantire l'affermazione del modello europeo a livello di regole globali²¹.

Infine, il Parlamento europeo, con una successiva risoluzione, chiese espressamente alla Commissione che la proposta in corso di elaborazione tenesse conto della legislazione esistente in materia di protezione dei dati²².

A conclusione di questo lungo *iter* preparatorio, si può affermare con certezza che la volontà delle istituzioni europee è nel senso che la regolamentazione dell'intelligenza artificiale avvenga attraverso una regolamentazione esaustiva, che tenga conto dei diritti fondamentali e, per quanto interessa ai fini del prosieguo del nostro discorso, della normativa posta a protezione dei dati personali.

2. La proposta di regolamento sulla disciplina dell'AI presentata dalla Commissione europea lo scorso mese di aprile

La proposta di regolamento sull'intelligenza artificiale è stata presentata dalla Commissione europea lo scorso mese di aprile²³. Per certi versi, la stessa è in parte sorprendente, perché essa sembra rispondere alla logica sottesa alla disciplina della responsabilità del produttore per prodotti difettosi, pur mantenendo, a differenza di questa, un'accentuata attenzione per il profilo della tutela dei diritti fondamentali²⁴.

²⁰ Consiglio europeo, Riunione straordinaria del Consiglio europeo (1° e 2 ottobre 2020) - *Conclusioni*, EUCO 13/20, 2020, punto 7.

²¹ Secondo la nota tesi propugnata da A. BRADFORD, *Effetto Bruxelles. Come l'Unione europea regola il mondo*, Milano 2021, 220 ss. Con specifico riferimento alla proposta di regolamento sull'intelligenza artificiale v. V. O. POLLICINO, G. DE GREGORIO, *Constitutional Law in the Algorithmic Society*, in H.W. MICKLITZ, O. POLLICINO, A. REICHMAN, A. SIMONCINI, G. SARTOR, G. DE GREGORIO (eds.), *Constitutional Challenges in the Algorithmic Society*, cit., p. 1 ss., 12-13: «the top-down approach of the Union, which aims to leave small margins to self-regulation, might be an attempt to protect the internal market from algorithmic tools which would not comply with the European standard of protection. Rather than making operators accountable for developing and implementing artificial intelligence systems, the regulation aims to prevent the consolidation of external standards».

²² Risoluzione del Parlamento europeo del 20 ottobre 2020 *recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate* (2020/2012(INL)): «nota che il quadro giuridico dell'Unione dovrebbe applicarsi all'intelligenza artificiale, alla robotica e alle tecnologie correlate, inclusi i software, gli algoritmi e i dati utilizzati o prodotti da tali tecnologie; prende atto che le opportunità basate sull'intelligenza artificiale, la robotica e le tecnologie correlate si basano sui Big Data e che è necessaria una massa critica di dati per addestrare gli algoritmi e perfezionare i risultati; si compiace, a tale proposito, della proposta della Commissione di creare uno spazio comune dei dati nell'Unione per rafforzare lo scambio di dati e sostenere la ricerca, nel pieno rispetto delle norme europee in materia di protezione dei dati».

²³ *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, Bruxelles, 21.4.2021, COM(2021)206 final, 2021/0106 (COD).

²⁴ In precedenza vi sono state talune proposte dirette ad estendere anche ai sistemi di intelligenza artificiale la normativa sui prodotti difettosi. Detta disciplina è stata introdotta con la direttiva 85/374/CEE, successivamente modificata dalla direttiva 99/34/CE (Direttiva 1999/34/CE del Parlamento europeo e del Consiglio, del 10 maggio 1999, che modifica la direttiva 85/374/CEE del Consiglio relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi, in *GU L* 141, 4.6.1999, p. 20–21). L'estensione di detta normativa ai sistemi di intelligenza artificiale avrebbe richiesto, perlomeno, un adattamento del testo della direttiva, dal momento che

Sulla falsariga della direttiva sul danno da prodotti difettosi, infatti, la proposta di regolamento sull'intelligenza artificiale introduce una sorta di responsabilità quasi oggettiva, nel senso che, nella sostanza, è il produttore del sistema di intelligenza artificiale che deve dimostrare di avere seguito tutte le prescrizioni del regolamento e che, conseguentemente, il danno non discende da un difetto di progettazione o di realizzazione del sistema.

La proposta distingue, al riguardo, tre tipologie di rischio, a seconda delle peculiarità di ogni sistema di intelligenza artificiale.

Nella prima tipologia rientrano i sistemi a rischio elevato. Tali sono, in via esemplificativa, quelli che distorcono i comportamenti; che determinano una classificazione degli utenti, al fine di attribuire loro un determinato punteggio sociale o di valutarne l'affidabilità economica. Per i sistemi riconducibili in tale categoria vige un divieto generalizzato di introduzione in commercio²⁵, al quale si può derogare solo per finalità di ordine pubblico, come la prevenzione dei crimini o degli attentati terroristici²⁶.

La seconda tipologia è quella oggetto del maggior numero di disposizioni (articoli 6-51). In tale categoria, definita ad alto rischio, rientrano i sistemi che presentano, in via cumulativa, due caratteristiche: che siano destinati ad essere utilizzati come componente di sicurezza di un prodotto oggetto di disposizioni di armonizzazione a livello sovranazionale²⁷;

questa si applica solo agli oggetti tangibili e all'elettricità, mentre i sistemi di intelligenza artificiale sono evidentemente caratterizzati da una preponderanza di elementi intangibili (programmi per elaboratore, algoritmi, dati personali e non personali, diritti di proprietà intellettuale). In dottrina v. U. PAGALLO, *The Laws of Robots: Crimes, Contracts, and Torts*, Dordrecht, 2013, spec. p. 98 ss.; ID., *From Automation to Autonomous Systems: A Legal Phenomenology with Problems of Accountability*, in *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence*, Melbourne, Australia, 19-25 August 2017, reperibile online al sito <https://www.ijcai.org/proceedings/2017/>, p. 17 ss., spec. 20 s.; G. COMANDÈ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giuridica dell'economia*, 2019, p. 169 ss.

²⁵ L'aspetto criticabile della disposizione menzionata nel testo è che il divieto (pressoché) assoluto di commercializzazione sembrerebbe valere solo per le autorità pubbliche, ma non per i soggetti privati (art. 5, par. 1, lett. c: «l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA da parte delle autorità pubbliche o per loro conto ai fini della valutazione o della classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste»). In altri termini, la formulazione letterale della disposizione sembra consentire, ad un datore di lavoro privato, il ricorso a sistemi di *social scoring* per valutare, seppure dietro la prestazione del consenso degli interessati (come previsto dall'art. 6, par. 1, lett. a, del GDPR), il comportamento extralavorativo dei propri dipendenti (v. l'editoriale di G. GHIDINI, D. MANCA, *Intelligenza artificiale: dubbi (e rischi) in Europa*, in *Corriere della sera*, 14 dicembre 2021, p. 32).

²⁶ In quest'ultimo caso, tuttavia, occorre sempre un provvedimento autorizzatorio dell'autorità pubblica preposta al mantenimento dell'ordine pubblico ovvero al controllo e alla prevenzione dei reati (v. art. 5, par. 3, della *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale*).

²⁷ L'elenco, contenuto nell'Allegato II della proposta della Commissione, comprende svariati atti normativi. Tra questi sembra opportuno ricordare le seguenti direttive: 2013/53/UE del Parlamento europeo e del Consiglio, del 20 novembre 2013, relativa alle imbarcazioni da diporto e alle moto d'acqua e che abroga la direttiva 94/25/CE (GU L 354 del 28.12.2013, pag. 90); 2014/33/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, per l'armonizzazione delle legislazioni degli Stati membri relative agli ascensori e ai componenti di sicurezza per ascensori (GU L 96 del 29.3.2014, pag. 251); 2014/34/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative agli apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva (GU L 96 del 29.3.2014, pag. 309); direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (GU L 153 del 22.5.2014, pag. 62); 2014/68/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di attrezzature a pressione (GU L 189 del

e che il prodotto in questione sia soggetto ad una valutazione di conformità da parte di terzi.

Rispetto a questi prodotti, la proposta di regolamento stabilisce taluni obblighi supplementari a carico dei “fornitori” dei sistemi di intelligenza artificiale: innanzitutto quello di stabilire un sistema di registrazione; poi, di disporre un monitoraggio continuativo sul funzionamento del sistema; quindi un obbligo di trasparenza e di informazione degli utenti finali sull’operatività complessiva del sistema.

I fornitori devono, infine, garantire che i sistemi di intelligenza artificiale ad alto rischio siano conformi alle prescrizioni del regolamento prima dell’immissione in commercio e devono comunque assicurare che sia sempre possibile una sorveglianza umana sui processi decisionali dell’intelligenza artificiale.

In pratica, per garantire il rispetto di tutti questi parametri, si segue una procedura di certificazione, presso determinati organismi appositamente autorizzati dall’autorità dello Stato membro, ricalcata sulla falsariga di quella già prevista per la marchiatura dei prodotti con il marchio “CE”²⁸. I certificati che vengono in tal modo rilasciati devono essere redatti in una delle lingue ufficiali dell’Unione e hanno validità per cinque anni²⁹.

La terza categoria di prodotti, che potremmo definire “a rischio moderato”, ricomprende tutti quei sistemi di intelligenza artificiale destinati ad operare con le persone, che non siano inclusi nelle due precedenti categorie. Rispetto a questi prodotti, la proposta di regolamento si limita a stabilire, a carico dei fornitori, solo uno specifico obbligo di informazioni degli utenti. In particolare, i fornitori, garantiscono che «le persone fisiche siano

27.6.2014, pag. 164)); e taluni regolamenti (tra i quali è opportuno segnalare: il regolamento (UE) 2016/426 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sugli apparecchi che bruciano carburanti gassosi e che abroga la direttiva 2009/142/CE (GU L 81 del 31.3.2016, pag. 99); il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1); il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176); e, infine, il regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio, del 5 febbraio 2013, relativo all’omologazione e alla vigilanza del mercato dei veicoli agricoli e forestali (GU L 60 del 2.3.2013, pag. 1).

²⁸ L’art. 48, della proposta della Commissione, prevede all’uopo un sistema sostanzialmente simile a quello previsto dal reg. 765/2008 per la marchiatura “CE”: «1. Il fornitore compila una dichiarazione scritta di conformità UE per ciascun sistema di IA e la tiene a disposizione delle autorità nazionali competenti per dieci anni dalla data in cui il sistema di IA è stato immesso sul mercato. La dichiarazione di conformità UE identifica il sistema di IA per il quale è stata redatta. Su richiesta, una copia della dichiarazione di conformità UE è messa a disposizione delle pertinenti autorità nazionali competenti. 2. La dichiarazione di conformità UE attesta che il sistema di IA ad alto rischio in questione soddisfa i requisiti di cui al capo 2 del presente titolo. La dichiarazione di conformità UE riporta come minimo le informazioni di cui all’allegato V ed è tradotta in una lingua o nelle lingue ufficiali dell’Unione richieste dallo Stato membro nel quale il sistema di IA ad alto rischio è messo a disposizione. 3. Qualora i sistemi di IA ad alto rischio siano soggetti ad altre normative di armonizzazione dell’Unione che richiedano anch’esse una dichiarazione di conformità UE, è redatta un’unica dichiarazione di conformità UE in relazione a tutte le normative dell’Unione applicabili al sistema di IA ad alto rischio. La dichiarazione contiene tutte le informazioni necessarie per identificare la normativa di armonizzazione dell’Unione cui si riferisce la dichiarazione. 4. Redigendo la dichiarazione di conformità UE, il fornitore si assume la responsabilità della conformità ai requisiti di cui al capo 2 del presente titolo. Il fornitore tiene opportunamente aggiornata la dichiarazione di conformità UE».

²⁹ Taluni obblighi specifici sono poi previsti a carico dei distributori, quali, in particolare, quello di verificare la sussistenza della documentazione atta a certificare la conformità e quello, correlato, dell’utilizzatore, di seguire le istruzioni del fornitore (ovvero, di comunicare al fornitore del sistema se ha apportato modifiche sostanziali al sistema): v. artt. 27 e 28, della proposta.

informate del fatto di stare interagendo con un sistema di IA» (art. 52).

La proposta di regolamento prevede, infine, l'istituzione di un Comitato per l'intelligenza artificiale, che svolge essenzialmente funzioni di raccordo e consultivi. Il Comitato ha il preciso compito di facilitare la diffusione delle tecniche per la costruzione dei sistemi di intelligenza artificiale, nonché quello di agevolare la concreta attuazione delle disposizioni del regolamento.

Ogni Stato membro deve, infine, istituire un'apposita autorità competente, con il compito di vigilanza e di riportistica degli eventuali eventi avversi che dovessero incorrere nel funzionamento dei sistemi di intelligenza artificiale. L'autorità di controllo, che in genere sarà la stessa preposta alla protezione dei dati personali, dispone del potere di irrogare sanzioni, che in talune ipotesi possono arrivare fino al sei per cento del fatturato mondiale della società operante nel settore³⁰.

Dopo questa analisi del contenuto della proposta, possiamo passare a verificare quale sia l'impatto della stessa sul funzionamento del regolamento sulla protezione dei dati personali.

3. L'applicazione cumulativa del reg. 2016/679 sulla protezione dei dati personali con la proposta di regolamento sull'intelligenza artificiale

È evidente che, per poter funzionare correttamente, i sistemi di intelligenza artificiale necessitano di una grande massa di dati. In un certo senso, più è vasta la quantità dei dati dei quali detti sistemi possono disporre, maggiormente accurate risultano le previsioni e gli annunci personalizzati indirizzati agli utenti.

Momento fondamentale per il funzionamento di un sistema di intelligenza artificiale, quindi, è la fase di raccolta dei dati. Al riguardo, il regolamento sull'intelligenza artificiale non si occupa della raccolta e del trattamento dei dati, i quali rimangono pertanto soggetti agli strumenti vigenti e, in particolare, al regolamento 2016/679, sulla protezione dei dati personali (spesso indicato con l'acronimo inglese, GDPR)³¹.

Una volta che i dati sono stati raccolti, rimane tuttavia da chiarire quale sia la disciplina ad essi applicabile, una volta che vengono immessi nel sistema. Con specifico riferimento a questo aspetto, è la stessa Commissione europea, nella relazione esplicativa di accompagnamento della proposta di regolamento sull'IA, a chiarire che essa «non pregiudica il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679)»³². Si tratta di

³⁰ La presentazione della proposta è stata accolta con favore. Non è, allo stato, del tutto chiaro quale sia il regime di responsabilità nell'ambito del quale inquadrare quella del fornitore di un sistema di intelligenza artificiale. Verosimilmente, il fatto stesso di prevedere obblighi estremamente dettagliati, induce ad includere la responsabilità dei fornitori di tali sistemi nel novero del *genus* della responsabilità oggettiva (v. G. DI ROSA, *Quali regole per i sistemi automatizzati "intelligenti"*, in *Riv. dir. civ.*, 2021, p. 823 ss., 853; G. FINOCCHIARO, *Considerazioni su intelligenza artificiale e dati personali*, in U. RUFFOLO (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, p. 331 ss., 338).

³¹ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in *GU L* 119, 4.5.2016, p. 1–88. Per i dati c.d. "non personali", invece, si dovrà fare riferimento al Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, in *GU L* 303, 28.11.2018, p. 59–68.

³² V. la relazione esplicativa alla Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce

una constatazione forse ovvia, dal momento che il regolamento sulla protezione dei dati mira a tutelare un diritto fondamentale, già previsto dagli articoli 8 della Carta dei diritti fondamentali dell'Unione europea e 16 TFUE³³. Da questa riflessione è agevole desumere la conseguenza secondo la quale non avrebbe senso risolvere i conflitti tra le due fonti normative sulla base del principio di specialità. Non avrebbe senso, infatti, invocare il principio di specialità della Proposta di regolamento sull'IA, rispetto a quello sulla protezione dei dati personali, perché la seconda fonte normativa è diretta a dare attuazione ad un diritto fondamentale espressamente previsto a livello di fonte primaria.

A questo punto, è agevole affermare che entrambe le fonti derivate in esame debbano essere applicate in maniera cumulativa. D'altro canto, vari elementi testuali della proposta di regolamentazione sull'intelligenza artificiale sembrano, in effetti, confermare tale conclusione.

Innanzitutto milita, in tal senso, il considerando n. 24, il quale, nel descrivere le modalità di raccolta di dati biometrici (ovvero di quei dati concernenti le caratteristiche fisiche, fisiologiche o comportamentali di un individuo, attraverso le quali si può indentificare, in maniera univoca, un determinato soggetto³⁴), prevede espressamente che «(q)ualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica... dovrebbe *continuare a soddisfare tutti i requisiti derivanti dall'articolo 9, paragrafo 1, del regolamento (UE) 2016/679*».

A favore dell'applicazione cumulativa dei due strumenti depone poi anche il considerando 72, della proposta di regolamento sull'intelligenza artificiale, il quale prevede che la creazione di spazi di sperimentazione dei sistemi di intelligenza artificiale - ovvero di quegli spazi nei quali si procede a sviluppare ed istruire i sistemi di intelligenza artificiale - avvenga tenendo conto delle prescrizioni dell'art. 6, paragrafo 4, del regolamento 2016/679, nell'ipotesi in cui la raccolta dei dati non possa avvenire dietro il consenso dell'interessato³⁵.

regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, cit., p. 4.

³³ Mentre la Carta dei diritti fondamentali dell'Unione europea distingue il diritto alla vita privata e familiare da quello della protezione dei dati personali (oggetto, rispettivamente, degli articoli 7 e 8), la Corte europea dei diritti dell'uomo è solita ricomprendere la seconda nell'ambito della prima, in modo da estendere alla protezione dei dati personali la tutela prevista dall'art. 8 della Convenzione europea (v. O. POLLICINO, M. BASSINI, *Art. 8. Protezione dei dati personali*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 134 ss., 136 ss.; S. CALZOLAIO, *Protezione dei dati personali*, in *Digesto delle Discipline Pubblicistiche, Aggiornamento*, Torino, 2017, p. 594 ss., 618).

³⁴ L'art. 4, par. 1, n. 14, del reg. 2016/679, definisce i dati biometrici come i «dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici».

³⁵ Art. 6, par. 4, reg. 2016/679: «Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione».

Da questa serie di elementi testuali troviamo, quindi, una chiara indicazione legislativa che ci consentono di giungere alla conclusione che i due strumenti normativi debbano essere applicati in maniera cumulativa. A questo punto possiamo passare ad analizzare i principali problemi di coordinamento.

4. Segue. *L'individuazione del titolare del trattamento*

Il primo problema che si pone nell'applicazione cumulativa dei due strumenti (la proposta di regolamento sull'intelligenza artificiale ed il regolamento sulla protezione dei dati personali) concerne l'individuazione del titolare del trattamento.

Mentre infatti la proposta di regolamento sull'intelligenza artificiale si indirizza ai "fornitori" dei sistemi, il regolamento sulla protezione dei dati pone determinati obblighi specifici a carico del "titolare del trattamento".

In altri termini, il regolamento sulla protezione dei dati ruota chiaramente intorno all'ipotesi che, a maggior tutela dei diritti degli utenti, vi sia un unico titolare, il quale è responsabile per la raccolta e per il trattamento; e che diviene il destinatario di tutte le richieste dell'utente, quali l'esercizio da parte di quest'ultimo del diritto di rettifica, del diritto all'oblio, nonché delle richieste di limitazione o di trasferimento dei dati³⁶.

I sistemi di intelligenza artificiale, al contrario, presuppongono spesso l'operatività di una serie di rilevazioni effettuate attraverso strumenti diversi, quali sensori acustici, telecamere, tecnologie per il riconoscimento facciale ovvero altri oggetti connessi, capaci di percepire ed elaborare dati (tanto è vero che è diffusa l'espressione di "internet delle cose"). Gli elementi di accesso al sistema capaci di raccogliere dati sono, quindi, necessariamente molteplici e

³⁶ Come è noto, il diritto all'oblio non era espressamente previsto dal testo normativo originario. Esso discende da un'interpretazione della Corte di giustizia degli articoli 12, lett. b, e 14, lett. a, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (in *GU*, 23 novembre 1995, L 281, p. 31 ss.; la direttiva è stata abrogata a seguito dell'entrata in vigore del GDPR). Tale diritto consiste nell'obbligo di un motore di ricerca di deindicizzare i *link*, di modo che non sia più possibile collegare determinate notizie ad un persona specifica, attraverso una ricerca nominativa, allorché la notizia stessa abbia perso di attualità (v. la sentenza della Corte del 13 maggio 2014, causa C-131/12, *Google Spain c. AEPD e a.*, ECLI:EU:C:2014:317). Successivamente la Corte ha chiarito che tale obbligo è valido ed efficace solo per le ricerche che vengono effettuate online a partire dal territorio europeo (Corte giust., sent. 24 settembre 2019, causa C-507/17, *Google c. Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772). In dottrina v.: J.W. KROPE, *Google Spain v. Agencia Espanola de Protección de Datos (AEPD)*, in *Am. Jour. Int. Law*, 2014, 3, pp. 502- 509; F. PIZZETTI, *Le autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il "velo di Maya"*, in *Il diritto dell'informazione e dell'informatica*, 2014, 4-5, p. 805 ss.; G.M. RICCIO, *Diritto all'oblio e responsabilità dei motori di ricerca*, ivi, p. 753 ss.; A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di) *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Torino, 2017, p. 195 ss.; S. MARTINELLI, *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla de-indicizzazione*, in *Il diritto dell'informazione e dell'informatica*, 2017, 3, pp. 565-581; C. GRIECO, *L'attuazione in Italia del diritto all'oblio*, in G. CONTALDI (a cura di), *Il mercato unico digitale*, numero speciale di *Diritto, mercato e tecnologia*, 2017, p. 161 ss. (consultabile online al sito www.dimt.it); S. VLACHOPOULOS, *Freedom of Expression in the Internet: the Example of the "Right to Be Forgotten"*, in *European Review of Public Law*, 2018, 1, p. 113 ss.; P. JONASON, *The Right to Be Forgotten: The Balance between the Right to Privacy and Freedom of Expression*, ivi, p. 213 ss.; F. DI CIOMMO, *Diritto alla cancellazione, diritto alla limitazione del trattamento e diritto all'oblio*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di) *I dati personali nel diritto europeo*, Torino, 2019, p. 353 ss.; F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019, p. 223 ss.; F. BALDUCCI ROMANO, *La Corte di giustizia "resetta" il diritto all'oblio*, in *federalismi.it*, 2020, p. 31 ss.

diversificati. Essi, pertanto, male si adattano rispetto all'idea dell'esistenza di una figura unitaria, che viene considerata come il titolare di tutte le situazioni giuridiche attive e passive che discendono dall'uso di determinati dati personali.

Al riguardo, è stato sostenuto che il titolare del trattamento sia il sistema di intelligenza di artificiale³⁷. Secondo questa impostazione, se consideriamo lo sviluppo della tecnologia, potremmo – con un notevole sforzo di fantasia – considerare i sistemi di intelligenza artificiale come una sorta di esseri senzienti, capaci di assumere decisioni indipendentemente dal controllo umano³⁸.

Questa tesi non sembra tuttavia reggere al riscontro degli elementi normativi. Innanzitutto essa si pone in contrasto con le risultanze dei lavori preparatori riportati nel primo paragrafo, dai quali emerge chiaramente la volontà delle istituzioni europee di escludere, nello stato di attuale elaborazione della maniera, qualunque forma di soggettività giuridica all'intelligenza artificiale³⁹.

Vari elementi testuali del regolamento sulla protezione dei dati, poi, consentono di escludere la possibilità di assimilare il sistema di intelligenza artificiale al titolare del trattamento ai fini dell'applicazione del regolamento sulla protezione dei dati personali. Depone in tal senso, innanzitutto l'art. 4, par. 1, n.7, del GDPR, nel definire il titolare del trattamento, riferisce espressamente che è la «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento». La disposizione, se da un lato include chiaramente nel novero dei titolari anche enti privi di una soggettività giuridica («il servizio o altro organismo»), sembra comunque richiedere un minimo di personificazione per assumere la veste di titolare del trattamento⁴⁰.

In secondo luogo, milita nel senso di escludere la possibilità di identificare il titolare del trattamento con il sistema di intelligenza artificiale, l'art. 22 GDPR, che prevede che l'interessato può chiedere di non essere sottoposto esclusivamente ad una decisione automatizzata⁴¹. Se il soggetto passivo, che viene influenzato da un determinato trattamento, può sempre chiedere di non essere assoggettato ad una decisione automatizzata, significa che il sistema di intelligenza artificiale deve essere concepito in modo da consentire, sempre e comunque, un intervento umano; ovvero l'intervento di un soggetto, con piena capacità

³⁷ V. G. SIMONE, *Machine Learning e tutela della Privacy alla luce del GDPR*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, p. 275 ss., 283.

³⁸ V., invero in termini un po' sibillini, F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 5 ss., 45 s.: «Merita, inoltre, sottolineare che il titolare del trattamento può operare nel quadro di una pluralità di trattamenti che abbiano una comune finalità ma facciano capo a titolari diversi, così come può operare nell'ambito di una catena di trattamenti che abbiano ciascuno finalità diverse, che riguardano l'ambito dei singoli trattamenti da ciascun "anello" operanti, ma che, connessi l'un con l'altro, producono effetti che nessuno dei trattamenti in catena potrebbe determinare da solo. Un fenomeno, questo, che specialmente nel mondo della robotica e del c.d. IoT [Internet of Things, ndr] si sta delineando con riguardo al tema della responsabilità civile nel caso che le macchine producano danni sulla base di comportamenti o azioni a determinare i quali concorrono pluralità di trattamenti in catena uno con l'altro, compresi quelli che possono aver determinato l'utilizzazione da parte dell'algoritmo finale di dati imprecisi o inadeguati prodotti dai trattamenti precedenti».

³⁹ V. *supra*, nota 9 e testo relativo.

⁴⁰ V. G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, p. 1670 ss., 1674: «La definizione di titolare contenuta nel Regolamento chiaramente indica che il titolare debba essere persona giuridica o fisica o comunque soggetto giuridico».

⁴¹ Art. 22, GDPR: «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».

giuridica, dotato del potere di escludere la macchina e di assumere le relative decisioni in sua vece⁴².

A ciò si aggiunga che le disposizioni del regolamento sulla protezione dei dati, allorché prevedono il potere delle autorità nazionali competenti di imporre talune sanzioni, riconnettono l'eventuale diversa graduazione della pena pecuniaria anche al carattere di volontarietà del comportamento dell'autore dell'illecito⁴³. Le "decisioni" di un sistema di intelligenza artificiale, infatti, sono sempre il frutto di calcoli; esse non discendono mai da scelte discrezionali, indicative, come tali, di un certo atteggiamento psicologico.

Deve quindi recisamente negarsi che, nell'attuale panorama giuridico, si possa concepire un sistema di intelligenza artificiale completamente automatizzato, tale da operare al di fuori di qualunque intervento umano.

Esclusa la soluzione più semplicistica, rimane tuttavia aperto il quesito su chi debbano gravare gli obblighi discendenti dall'applicazione del GDPR nel funzionamento di un sistema di intelligenza artificiale. Verosimilmente, al riguardo, non è possibile fornire una risposta univoca; e sul punto sarebbe, pertanto, auspicabile un intervento chiarificatore del legislatore europeo.

Normalmente gli obblighi principali discendenti dalla proposta di regolamento sulla IA finiranno infatti per gravare sul fornitore del sistema di intelligenza artificiale, il quale, nel predisporre ed addestrare il sistema, dovrà necessariamente tenere conto anche delle prescrizioni normative discendenti dal diritto dell'Unione europea; ed in particolare di quelle contenute nel regolamento sulla protezione dei dati personale. Questi dovrà pertanto concepire il sistema di IA, non solo in modo da rendere possibile l'intervento umano, come previsto dal citato art. 22, GDPR, ma anche per consentire all'utente di far valere gli altri diritti previsti a favore degli interessati dagli articoli 16-20 GDPR, quali, in particolare, il diritto di rettifica, di richiedere la deindicizzazione (ovvero, la cancellazione dei dati personali e dei *link* alle pagine del web che lo riguardano), di chiedere la limitazione del trattamento o, infine, di esercitare la portabilità dei propri dati in un altro sistema di trattamento⁴⁴.

Laddove il sistema di intelligenza artificiale sia stato concepito in ossequio alle prescrizioni del regolamento 2016/679 e venga immesso sul mercato, gli obblighi discendenti da detta fonte normativa graveranno sulla società che eserciterà un diritto di possesso e di uso del sistema di intelligenza artificiale, alla quale spetterà in concreto garantire l'esercizio dei diritti garantiti dal GDPR durante tutta la fase di operatività del sistema. In altri termini, la concreta individuazione del titolare del trattamento, in questo caso, finirà per dipendere anche dal diritto nazionale.

Così identificato il titolare del trattamento, possiamo passare ad individuare le

⁴² V. A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era della intelligenza artificiale*, Pisa, 2020, p. 13 ss., 23.

⁴³ V. art. 83, par. 2, GDPR: «Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso *si tiene debito conto dei seguenti elementi*: a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) *il carattere doloso o colposo della violazione*».

⁴⁴ V. EDPB-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, par. 60 (il parere è consultabile al sito https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en).

principali problematiche che si porranno nell'applicazione cumulativa del regolamento sui dati personali e di quello (*in fieri*) sull'intelligenza artificiale⁴⁵.

5. *L'applicazione concreta di talune previsioni del regolamento sui dati personali alla futura disciplina dell'intelligenza artificiale. La raccolta dei dati ed i principi di minimizzazione, di prestazione del consenso e di anonimizzazione*

Procediamo ora ad applicare le principali disposizioni del regolamento sulla protezione dei dati personali ai sistemi di intelligenza artificiale.

Il primo aspetto problematico concerne la “raccolta” dei dati. Questa, come è noto, deve rispondere ai principi di cui agli articoli 5 e 6 GDPR. Tali disposizioni stabiliscono, rispettivamente, che la collazione dei dati avvenga secondo il principio di minimizzazione e dietro espresso consenso dell'interessato. Il principio di minimizzazione impone che vengano raccolti solo i dati necessari per una finalità specifica e che questi vengano cancellati una volta terminato il trattamento; il principio del consenso, viceversa, rappresenta il cuore intorno al quale ruotano le prerogative dell'interessato nella protezione dei dati che lo riguardano.

Entrambi questi principi appaiono, in verità, poco rispondenti al funzionamento concreto dei sistemi di intelligenza artificiale. Tali sistemi, infatti, utilizzano dati collazionati con finalità diverse per elaborare i propri modelli predittivi. Ad esempio, i dati anagrafici, il luogo di residenza, l'occupazione, il livello di scolarizzazione e, infine, il reddito medio della popolazione stabilita in determinate zone urbane, possono venire impiegati, congiuntamente ad altri dati, quali, in via esemplificativa, il numero di reati che si sono verificati e la vicinanza con parchi o con altre aree scarsamente illuminate, come elementi per l'operatività di un sistema di prevenzione dei reati, al fine di suggerire alla polizia locale come impiegare più efficacemente le pattuglie disponibili. In questo contesto è evidente che sono normalmente proprio le finalità non dichiarate – o, perlomeno, non evidenti – al momento della raccolta dei dati che assumono rilievo, in un secondo momento, per il funzionamento del sistema di intelligenza artificiale⁴⁶.

Per quanto riguarda il consenso è invece sostanzialmente accertato che la maggior parte degli utenti tende a prestare poca attenzione nel momento in cui presta il proprio assenso⁴⁷. Normalmente, i siti che si visitano durante una normale sessione di navigazione invitano, infatti, a cliccare sul “bottono” denominato «accetta tutto», lasciando come seconda opzione, in genere non posta in primo piano e non sempre agevolmente praticabile, quella di “rifiuta” o “gestisci preferenze”. Ed in genere è molto più semplice limitarsi ad accettare, in maniera indiscriminata, qualunque uso dei propri dati personali, piuttosto che selezionare le preferenze, in funzione delle esigenze specifiche di ogni utente o semplicemente tenendo in

⁴⁵ È opportuno avvertire che la tutela dei diritti dell'interessato in ipotesi di ricorso a sistemi di intelligenza artificiale per contattare gli utenti (ad es.: telefonate tramite un centralino automatico che individua i potenziali clienti) sarà regolato, al momento della sua entrata in vigore, dal relativo regolamento (v. la Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), Bruxelles, 10.1.2017, COM/2017/010 final - 2017/03 (COD).

⁴⁶ V. T.Z. ZARSKY, *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 2017, p. 995 ss., 1009 ss. (l'articolo è reperibile online al sito <https://scholarship.shu.edu/shlr/vol47/iss4/2>).

⁴⁷ V. G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del DGPR*, in *federalismi.it*, n. 16/2020, p. 266 ss., 282.

mente quelli che possono essere i futuri impieghi che verranno fatti dei propri dati. Anche perché questa seconda opzione richiede un maggiore dispendio dal punto di vista temporale, che l'utente medio, spesso, non è disposto a sopportare.

Il punto è che i principi di base del GDPR, quali quelli della minimizzazione e del consenso, già esistevano nella direttiva 95/46. Come tali, essi erano stati concepiti prima della diffusione massiccia di internet e dello sviluppo dell'industria dei dati. Tuttavia, essi, benché poco rispondenti al funzionamento concreto dei sistemi di intelligenza artificiale, costituiscono tuttora il principale argine alla preponderanza delle multinazionali e agli abusi della *privacy* che possono porre in essere le imprese attive nel mercato della raccolta e dello scambio dei dati⁴⁸. Discende da questa osservazione che, anche dopo l'elaborazione della proposta sull'intelligenza artificiale, i dati personali non possono essere utilizzati al di là dei perimetri del consenso prestato dall'interessato e delle finalità espressamente dichiarate in quella sede.

Una volta raccolti i dati, incombe sul titolare del trattamento l'obbligo di procedere all'anonimizzazione dei dati, come previsto dall'art. 25 GDPR. In tal modo i dati diventerebbero "non personali": per effetto di questo processo, non dovrebbe essere possibile collegarli, in un momento successivo, ad una determinata persona fisica⁴⁹. Laddove i dati non consentano di risalire all'utente che li ha generati, si ricadrebbe, in effetti, nella diversa disciplina dei dati non personali, che – come è noto – sono liberamente cedibili e trasferibili⁵⁰.

6. Segue. I dati a carattere discriminatorio e il diritto alla spiegazione della logica sottesa al funzionamento dei sistemi di intelligenza artificiale

Un regime particolare vale, poi, per i dati personali a carattere discriminatorio. L'art. 9 GDPR vieta di «trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare

⁴⁸ Secondo la nota impostazione di S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019, e di T. WU, *The Attention Merchants. The Epic Struggle to Get inside Our Heads*, New York, 2016.

⁴⁹ I c.d. *big data* sono appunto i dati che, in linea di principio, non consentono di determinare chi è il soggetto che li ha generati. Essi consistono in enormi volumi di dati, provenienti da fonti diverse e analizzati per mezzo di algoritmi. Abitualmente, si riporta che i c.d. *big data* si caratterizzano per le c.d. tre "v" ovvero: il volume (enormi quantità di dati), la varietà (l'eterogeneità della tipologia e le fonti di provenienza dei big data), la velocità (capacità di acquisizione e di analisi in tempo reale). Secondo alcuni autori, vi sarebbero poi anche una quarta ed una quinta "v", che identificerebbe il valore (il profitto economico discendente dai *big data*) e la veridicità (la qualità e l'accuratezza dell'analisi). In dottrina, v. V. MAYER-SCHÖNBERGER, T. RAMGE, *Reinventare il capitalismo nell'era dei Big data*, Milano, 2018; G. DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018; A.C. AMATO MANGIAMELI, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 2019, pp. 107 ss.; M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019, p. 10 ss.; F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019, pg. 160 ss.; ID., *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *federalismi.it*, n. 16/2020, p. 79 ss., 83, nota 16.

⁵⁰ La distinzione tra le due previsioni menzionate nel testo è determinata dalla natura dei dati. I dati oggetto del regolamento 2016/679 sono i dati personali, che consentono di individuare l'utente che li ha generati. L'oggetto del regolamento 2019/1807 sono, invece, i dati anonimi: ovvero quelli che non consentono di risalire all'interessato (v. F. FAINI, *La dimensione giuridica dei big data*, in S. FARO, T.E. FROSINI, G. PERUGINELLI (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, p. 113 ss., 116 s.; G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2020, p. 160-162).

dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

Anche in questo caso, la disposizione non è strutturata in funzione degli attuali impieghi dell'intelligenza artificiale. Il fatto è che un sistema di intelligenza artificiale, pur escludendo di trattare dati che rivelino origine razziale o credenze religiose, potrebbe indirettamente assumere detta conformazione, pur utilizzando elementi che non sono in sé discriminatori. In via esemplificativa, possiamo ipotizzare un sistema concepito per selezionare i candidati idonei per una certa tipologia di impiego di alto profilo in campo ingegneristico. Detto sistema sarà stato "istruito" sulla base dell'esperienza pregressa: e, verosimilmente, esso si fonderà sugli elementi comuni ai candidati che hanno già ricoperto quell'incarico in passato, che, per ipotesi, saranno il titolo di studio conseguito in determinati atenei, una buona conoscenza delle lingue straniere e la conseguente capacità di assumere incarichi dirigenziali, la propensione a viaggiare frequentemente all'estero, un voto di laurea elevato, un'esperienza presso aziende multinazionali operanti nel settore. Un sistema così concepito, pur non essendo in sé discriminatorio, potrebbe diventarlo nell'utilizzo concreto, laddove si accerti che in passato tutti i soggetti che rispondevano a tali requisiti provenivano da classi economicamente agiate, con elevati livelli di istruzione e con la capacità di iscrivere i propri figli in atenei con elevatissime rette annuali (soprattutto se si tratta di università situate oltreoceano). È evidente che, pur non avendo il programmatore inserito dati che siano "all'origine" discriminatori, il sistema finirà per selezionare candidati che, per provenienza familiare, livello culturale, possibilità economiche, apparterranno a determinati classi sociali e saranno, verosimilmente, della stessa razza dalla quale provenivano in passato i candidati che hanno occupato analoghe posizioni lavorative.

È singolare notare che, mentre il profilo della discriminazione diretta è oggetto di disciplina nel regolamento sulla protezione dei dati, quello della discriminazione indiretta, che potrebbe discendere dall'uso di dati privi di carattere discriminatorio all'origine, è rimasto sostanzialmente non regolato. L'unico elemento normativo è rintracciabile nel considerando 71, GDPR, ai sensi del quale: «(a) al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti».

Si tratta di una disposizione evidentemente incompleta, peraltro espressa solo in un considerando ed in una forma che sembra escludere un carattere di precettività della stessa («è opportuno che il titolare del trattamento utilizzi procedure... appropriate»).

Insomma, sul punto, il regolamento sulla protezione dei dati presenta una vera e propria lacuna⁵¹, che non sembra essere colmata neppure dalla proposta di regolamento sull'intelligenza artificiale. Il regolamento sull'intelligenza artificiale si limita, infatti, a

⁵¹ V. G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del DGPR*, cit., p. 294.

prevedere che i dati di addestramento rispondano a determinati principi: questi devono essere pertinenti, rappresentativi, esenti da errori e completi⁵². In altri termini devono possedere tutti i requisiti statistici adeguati alla finalità dell'addestramento: ma come è evidente questo non impedisce che il risultato prodotto sia in sé discriminatorio e possa, magari in maniera involontaria, escludere taluni candidati che, all'origine, non possiedano certe caratteristiche specifiche. Anche sotto questo aspetto è, pertanto, necessario un intervento chiarificatore del legislatore europeo.

Il titolare del trattamento è poi tenuto a rispettare le prescrizioni dell'art. 15 GDPR (diritto di accesso)⁵³. Egli deve, infatti, fornire – dietro richiesta dell'interessato – una serie di informazioni aggiuntive, quali la finalità del trattamento, i destinatari, il periodo di conservazione dei dati, i diritti che l'interessato può esercitare, nonché la logica utilizzata e le conseguenze del trattamento automatico utilizzato.

Su questo punto, è stato notato, il regolamento sulla protezione dei dati personali non prevede un obbligo specifico a carico del titolare di spiegare la “logica” sottesa all'operatività del sistema di intelligenza artificiale⁵⁴. In altri termini, il titolare del trattamento è tenuto a fornire svariate informazioni sull'utilizzo dei dati, ma non a chiarire le modalità attraverso le quali un determinato sistema di IA è pervenuto ad un determinato risultato. Anche in questo caso l'unico riferimento espresso è contenuto nel considerando 71 del GDPR, il quale, sempre in una forma ipotetica si limita a chiarire che «In ogni caso, tale trattamento *dovrebbe* essere subordinato a garanzie adeguate, che *dovrebbero* comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione». In questo caso, l'uso stesso del “condizionale” sembrerebbe escludere la possibilità per l'interessato di invocare direttamente tale diritto di spiegazione della logica

⁵² Art. 10, della Proposta di regolamento sull'intelligenza artificiale: «I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5. 2. I set di dati di addestramento, convalida e prova sono soggetti ad adeguate pratiche di governance e gestione dei dati. Tali pratiche riguardano in particolare: a) le scelte progettuali pertinenti; b) la raccolta dei dati; c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione; d) la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino; e) una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari; f) un esame atto a valutare le possibili distorsioni; g) l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate. 3. I set di dati di addestramento, convalida e prova devono essere pertinenti, rappresentativi, esenti da errori e completi. Essi possiedono le proprietà statistiche appropriate, anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone sui quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o di una combinazione degli stessi. 4. I set di dati di addestramento, convalida e prova tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato. 5. 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 di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725, fatte salve le 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, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita».

⁵³ V. A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, cit., p. 24.

⁵⁴ V. S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a "Right to an Explanation of Automated Decision-Making Does not Exist in General Data Protection Regulation*, in *International Data Privacy Law*, 2017, p. 76 ss.

sottostante al sistema di intelligenza artificiale nei confronti del titolare dei dati.

In realtà, pur in assenza di riferimenti normativi espliciti, si potrebbe argomentare che un obbligo siffatto discenda dal combinato disposto del citato considerando 71, oltre che degli articoli 12 e 13 (comprendenti il diritto ad ottenere tutte le informazioni riguardanti il trattamento),¹⁴ (obbligo di notifica, qualora i dati non siano ottenuti presso l'interessato) e 22 (che contempla il diritto dell'interessato di non essere assoggettato ad una decisione automatizzata), secondo una loro interpretazione funzionale ed attualizzata del GDPR⁵⁵. E comunque, un obbligo in tal senso, in capo ai fornitori dei sistemi di IA, una volta che entrerà in vigore la relativa proposta sull'intelligenza artificiale, sarà ricavabile dal disposto dell'art. 13, par. 1: «I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente». Insomma, sembra che il legislatore europeo, consapevole dei dubbi ermeneutici che vertevano sull'interpretazione del GDPR, abbia cercato di risolverli introducendo una previsione *ad hoc*. Semmai, è singolare che una disposizione normativa, che concerne i diritti dell'interessato al trattamento dei propri dati, trovi collocazione nella proposta di regolamento sull'intelligenza artificiale, piuttosto che in una modifica *ad hoc* del regolamento sulla protezione dei dati.

7. I c.d. «spazi di sperimentazione».

Norme specifiche valgono, da ultimo, per i c.d. spazi di sperimentazione, concernenti lo sviluppo dei nuovi sistemi di intelligenza artificiale ed il loro addestramento alle masse dei dati necessari per il funzionamento. La creazione di spazi di sperimentazione aperti a più partecipanti consente, soprattutto alle imprese di dimensioni medie, di prendere parte allo sviluppo dei sistemi di intelligenza artificiale, ai quali non potrebbero altrimenti partecipare, a causa degli ingenti investimenti normalmente occorrenti in questo ambito.

L'art. 53, par. 6, della proposta di regolamento sull'IA rimette, nella sostanza, la regolamentazione specifica di questi spazi di sperimentazione a future linee guida che saranno emanate da un istituendo Comitato europeo sull'intelligenza artificiale. Pertanto spetterà a tale organo introdurre disposizioni per contemperare i diritti e gli obblighi discendenti dall'uso di dati personali con il funzionamento degli spazi di sperimentazione dei sistemi di intelligenza artificiale.

Naturalmente, è auspicabile che, anche all'interno dello spazio di sperimentazione, siano garantiti i diritti discendenti dal GDPR. Tuttavia, l'assetto normativo della proposta sembra ammettere una deroga al riguardo. L'art. 54 della proposta di regolamento sull'IA, stabilisce, infatti, taluni obblighi aggiuntivi per le imprese partecipanti allo spazio di sperimentazione, quali in particolare quello di trattarli in uno spazio «separato, isolato e protetto», sotto il diretto controllo dei partecipanti alla sperimentazione e precludendo l'accesso a terzi; il divieto di trasmissione dei dati all'esterno dello spazio; l'obbligo di cancellazione dei dati una volta conclusa la sperimentazione; e, infine, la conservazione di una descrizione accurata del processo di sperimentazione e della logica ad esso sottesa. In altri termini, tale previsione prevede che la raccolta ed il trattamento dei dati per gli spazi di

⁵⁵ V. G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del DGPR*, cit., p. 291; in senso affermativo v., seppure sulla base di una diversa impostazione, R. MESSINETTI, *La privacy ed il controllo dell'identità algoritmica*, in *Contr. impr./Eur.*, 2021, p. 121 ss.

sperimentazione si svolga secondo una serie di cautele specifiche.

La struttura complessiva della disposizione ora menzionata, sembrerebbe, pertanto, precludere agli interessati, i cui dati vengono immessi nello spazio di sperimentazione, l'esercizio di ulteriori diritti, quali, in particolare, quelli previsti dai citati articoli da 15 a 20 del GDPR (concernenti l'accesso, la rettifica, la cancellazione, la limitazione e, infine, la portabilità dei dati). In altri termini, proprio perché la disposizione in esame stabilisce determinate cautele aggiuntive nella predisposizione di uno spazio di sperimentazione, la stessa sembra disporre, al contempo, consistenti limitazioni ai diritti degli interessati. Si tratta di una ricostruzione attendibile, laddove si ponga attenzione al fatto che la volontà del legislatore, nel disciplinare gli spazi di sperimentazione, sia quella di favorire lo sviluppo di sistemi di intelligenza artificiale innovativi.

Se così stanno le cose, è verosimile pensare che la deroga, avendo una portata rigorosamente circoscritta nello spazio e nel tempo, corrisponda ad una precisa scelta legislativa. La soluzione appare, in definitiva, condivisibile. Tanto più che i diritti degli interessati, di cui alle menzionate disposizioni del GDPR, non sono concepiti come diritti assoluti, quanto piuttosto come prerogative che devono, di volta in volta, essere subordinate ad esigenze di carattere collettivo, quali il desiderio del pubblico ad avere accesso ad una determinata notizia (per il diritto all'oblio) ovvero che devono essere contemperati con i diritti e le libertà altrui⁵⁶. In altri termini, è come se il legislatore europeo accettasse l'introduzione di deroghe limitate ad una piena protezione dei dati personali, al fine di favorire lo sviluppo di un'industria europea, nonché di creare le condizioni per un più ampio sfruttamento delle tecnologie dell'intelligenza artificiale. Se queste riflessioni sono corrette, sembra esatto affermare che la deroga ai diritti degli interessati, essendo rigorosamente circoscritta, risulti compatibile con il funzionamento complessivo del GDPR. Si tratta, in conclusione, di un compromesso accettabile, tenuto conto dello sforzo complessivo dell'Unione europea di recuperare il *gap* accumulato in questo settore nei confronti di altri paesi.

8. Conclusioni

La creazione di sistemi di intelligenza artificiale è ormai necessaria per il progresso economico e sociale della collettività. È, infatti, del tutto evidente che, senza sistemi con elevate capacità di calcolo, che siano stati adeguatamente istruiti con una consistente mole di dati, diverse funzioni proprie di uno Stato moderno, quali il mantenimento dell'ordine pubblico, la gestione efficiente dei medicinali, l'uso consapevole delle risorse, risultano di fatto irrealizzabili in un mondo altamente articolato e iperconnesso.

Allo stato, la proposta di regolamento sull'intelligenza artificiale appare abbastanza completa. Sarebbe tuttavia opportuno che, nel corso dell'*iter* legislativo, vengano chiariti taluni aspetti critici nel rapporto intercorrente tra la regolamentazione dell'intelligenza artificiale ed il regolamento sulla protezione dei dati personali.

In particolare ci sembra che debba essere precisato come si ripartiscono gli obblighi

⁵⁶ D'altro canto, la stessa formulazione delle disposizioni, rende evidente tale esigenza di bilanciamento con le esigenze collettive (v., rispettivamente, art. 15, par. 4, GDPR, per il diritto di accesso e art. 17, par. 3, per il diritto all'oblio). V. G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, cit., p. 1675.

discendenti dal GDPR, tra il fornitore e l'utilizzatore dei sistemi di intelligenza artificiale, nel caso, che si verificherà con maggiore frequenza nella prassi, in cui questi ruoli non coincidano.

Occorre poi chiarire, in via definitiva, quale sia la disciplina degli algoritmi a carattere indirettamente discriminatorio (ovvero, di quei sistemi che, pur non essendo stati concepiti secondo algoritmi discriminatori, finiscono poi per assumere tale conformazione). Ci sembrerebbe, infatti, che il disposto dell'art. 21 della Carta dei diritti fondamentali dell'Unione europea, laddove vieta «qualsiasi forma di discriminazione» sia sufficientemente ampio da escludere anche le discriminazioni che possono indirettamente discendere, nell'applicazione della normativa europea, da determinate impostazioni di base degli algoritmi introdotte dai fornitori dei sistemi di intelligenza artificiale.

L'attuale contesto normativo, tuttavia, non sembra fornire adeguate garanzie contro l'uso di algoritmi che producono risultati indirettamente discriminatori. Sul punto, dovrebbe, a nostro sommo avviso, intervenire il legislatore nel corso dell'iter per l'adozione del regolamento sull'intelligenza artificiale, chiarendo quali siano le conseguenze che discendono in capo al fornitore del sistema di intelligenza artificiale ovvero al titolare del trattamento, nell'ipotesi in cui si riscontri che il funzionamento di un determinato algoritmo ha, in concreto, prodotto un risultato discriminatorio. All'uopo, infatti, il legislatore dovrebbe chiarire quali siano i poteri di intervento dell'autorità di controllo; e si dovrebbe, del pari, introdurre talune sanzioni specifiche, nell'ipotesi in cui il fornitore del sistema di intelligenza artificiale ovvero il titolare del trattamento non ottemperino alle prescrizioni adottate dall'autorità competente al fine di ridurre rischi siffatti in futuro.

Occorre, infine, che il legislatore intervenga per chiarire quale è la portata del diritto di spiegazione alla logica sottesa al funzionamento di un determinato sistema di intelligenza artificiale e delle ragioni per le quali perviene ad un determinato risultato. L'art. 13, della proposta di regolamento sull'intelligenza artificiale, risulta infatti troppo generico («I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente»). Sul punto occorre, infatti, introdurre obblighi stringenti, precisando quali informazioni devono essere fornite, nonché introdurre al riguardo uno specifico apparato sanzionatorio. L'art. 71, par. 4, della proposta di regolamento sull'intelligenza artificiale, nel disporre le sanzioni per la violazione degli obblighi generici previsti dal citato regolamento, risulta infatti gravare solo sui fornitori del sistema, mentre nessuna sanzione specifica è prevista, dal GDPR, a carico del titolare del trattamento, laddove la violazione del diritto di spiegazione sia imputabile solo a quest'ultimo⁵⁷.

Al di là di qualunque considerazione specificamente attinente al tema oggetto di indagine, è infine opportuno porre in rilievo come la pluralità delle discipline che costituiscono il c.d. mercato unico digitale risulti ormai alquanto estesa⁵⁸. Oltre al GDPR e al

⁵⁷ Art. 71, par. 4, della proposta di regolamento sull'intelligenza artificiale: «La non conformità del sistema di IA ai requisiti o agli obblighi previsti dal presente regolamento, diversi da quelli di cui agli articoli 5 e 10, è soggetta a sanzioni amministrative pecuniarie fino a 20.000.000 di EUR o, se l'autore del reato è una società, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore». D'altro canto, tutta la proposta del regolamento ruota intorno agli obblighi dei fornitori. Sul punto, pertanto, occorrerebbe chiarire la portata degli obblighi in capo al titolare del trattamento e le relative conseguenze della violazione, nel corpo del GDPR.

⁵⁸ V. gli scritti raccolti nel volume G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea sui mercati ed i servizi digitali*, in corso di pubblicazione.

regolamento 2018/1807 sui dati non personali, alla proposta di regolamento sull'intelligenza artificiale, sono in corso di elaborazione una pluralità di altre fonti normative, quali il *Digital Markets Act*⁵⁹, il *Digital Services Act*⁶⁰ e, infine, il *Digital Governance Act*⁶¹. Sarebbe il caso di pianificare, in un futuro non lontano, un'opera di codificazione e di coordinamento delle fonti normative applicabili. Detta opera di risistemazione della materia appare tanto più urgente, proprio per evitare di produrre un effetto opposto a quello auspicato dal legislatore europeo: ovvero di bloccare l'innovazione dell'industria dei dati situata nel territorio degli Stati membri, a causa della molteplicità dei vincoli normativi incombenti alle società fornitrici di servizi digitali che operano nel mercato interno, piuttosto che di favorire il loro sviluppo.

⁵⁹ Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), Bruxelles, 15.12.2020, COM(2020) 842 final, 2020/0374(COD).

⁶⁰ Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, Bruxelles, 15.12.2020, COM(2020) 825 final, 2020/0361(COD).

⁶¹ Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati), del 25.11.2020, COM(2020) 767 final, 2020/0340(COD).