LE NUOVE FRONTIERE DELL'INTELLIGENZA ARTIFICIALE ED I POTENZIALI RISCHI PER IL DIRITTO ALLA *PRIVACY*.

Di Angelo Viglianisi Ferraro

SOMMARIO*: 1. Premessa. L'Intelligenza artificiale e le possibili lesioni di vari diritti fondamentali (quello alla privacy in particolare). - 2. La non semplice garanzia dei principi generali in materia di tutela dei dati personali a fronte di trattamenti effettuati da software di IA. - 3. I rischi per la c.d. autodeterminazione informativa in presenza di operazioni automatizzate. - 4. La tutela dei (e dai) Big data, fra crescenti utilizzi di chatbot e sempre più sofisticate pratiche di business-analytics. - 5. L'Intelligenza artificiale ed i nuovi orizzonti della responsabilità civile per violazione della privacy - 6. Considerazioni conclusive. La necessità di un intervento normativo europeo.*

ABSTRACT. Questo saggio cerca di illustrare i principali problemi che il rapido sviluppo dell'Intelligenza artificiale pone con riferimento alla garanzia del diritto alla privacy, così come delineato dal recente GDPR europeo. Le non semplici questioni, riguardanti anche i profili della responsabilità civile, sembrerebbero imporre un intervento normativo, preferibilmente sovranazionale.

This article tries to illustrate the main problems that the rapid development of Artificial Intelligence poses with reference to the guarantee of the right to privacy, as outlined by the recent European GDPR. The arising non-trivial issues, which also involve the profiles of civil liability, would seem to require a normative, preferably supranational, intervention.

1. Premessa. L'Intelligenza artificiale e le possibili lesioni di vari diritti fondamentali (quello alla privacy in particolare).

La rete *Internet* è divenuta parte integrante della vita della maggior parte degli esseri umani, rivoluzionando telecomunicazioni, stampa e commercio, e contribuendo in tal modo alla creazione di relazioni umane sviluppate spesso, talvolta addirittura prevalentemente, in un ambiente *online*, in particolare sui *social network*[1], che hanno mostrato subito la pervicace capacità di rendere la persona umana vulnerabile, dentro e fuori il mondo virtuale[2].

Significativi sono, da questo punto di vista, gli sconvolgimenti che ha avuto lo stesso concetto di *privacy*: sicuramente non più considerabile l'oggetto del classico "*right to be left alone*", elaborato da Warren e Brandeis nel 1890[3], ma semmai "bene" dal contenuto molto più pregnante, in un'epoca che registra l'assoluta assenza di confini territoriali (come ha dimostrato un *virus*, quale il Covid-19, capace di circolare in tutto il globo in maniera repentina e di fatto inarrestabile, comportando la compressione di una serie di diritti fondamentali, tra loro inscindibilmente connessi, al fine di garantire la sicurezza sanitaria di tutti i Paesi del mondo)[4].

Se in passato la riservatezza rischiava di essere minata dalla ricerca di informazioni o fatti riguardanti una persona, oggi va considerato che è spesso quest'ultima direttamente a fornire una molteplicità di dati (non solo personali, ma sovente anche sensibili), in maniera spontanea, e con la piena consapevolezza delle potenziali o effettive violazioni della sua sfera di intimità[5], rendendoli accessibili a tutti tramite i più comuni *search engine*[6].

Più che un diritto ad essere dimenticati dalla rete (che in alcuni casi è emerso con particolare *pathos* e, magari, senza un reale fondamento giuridico), a volte sembra registrarsi al contrario negli ultimi anni il desiderio spasmodico di dimostrare a tutti di esistere, ad imperitura memoria[7], e di voler dire la propria in ogni settore (anche lontanissimo dalle proprie competenze), grazie ai *post* lasciati sulle varie reti sociali virtuali o applicazioni di messaggistica[8], attraverso i quali non è difficile per le imprese poter giungere alla formazione di *Big data*[9] e alla elaborazione di *dossier* più o meno completi per ogni individuo (c.d. "profilazione"[10]).

---

[11] In tale contesto, secondo R. Messinetti, *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. impr.*, 2019, p. 861, emergerebbe un vero e proprio nuovo diritto fondamentale a "controllare i processi di costruzione e utilizzazione dell'identità personale quale 'dispositivo di socializzazione'".

[2] Dei rischi connessi alla "dittatura dell'algoritmo" aveva già fatto ampiamente menzione S. Rodotà, *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014. Si veda, inoltre, E. Calzolaio (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Padova, 2020.

[3] S. D. Warren, L. D. Brandeis, *The right to privacy*, in *Harvard Law Review*, 1890, p. 193 ss.

[4] Molto interessante è, al riguardo, la Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19, adottata il 19 marzo 2020 dal Comitato europeo per la protezione dei dati. Occupandosi della *data protection* sul posto di lavoro o con riferimento all'uso dei dati di localizzazione da dispositivi mobili, il documento, prima ancora di entrare *in medias res*, sottolinea che "anche in questi momenti eccezionali [...] occorre [...] tenere conto di una serie di considerazioni per garantire la liceità del trattamento di dati personali e, in ogni caso, si deve ricordare che qualsiasi misura adottata in questo contesto deve rispettare i principi generali del diritto e non può essere irrevocabile. L'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza".

[5] R. van Den, H. van Genderen, *Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics*, in *Eur. Data Protection Law Review*, 2017, p. 338 ss.

[6] In questo lavoro, per comodità, non si effettuerà alcuna distinzione fra i concetti di riservatezza, *privacy*, tutela dei dati personali, *et similia*, nonostante si tratti di beni giuridici non del tutto sovrapponibili. Sul punto, si veda, fra i tanti, M. Tzanou, *Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures*, in *Journal of Internet Law*, 2013, p. 20 ss.

[7] Di una vera e propria "immortalità digitale" hanno parlato, in effetti, U. Ruffolo, A. Amidei, *Intelligenza Artificiale e diritti della persona: le frontiere del ''transumanesimo''*, in *Giur. it.*, 2019, p. 1658.

[8] Secondo D. Poletti, *GDPR tra novità e discontinuità - Le condizioni di liceità del trattamento di dati personali*, in *Giur. it.*, 2019, p. 2785, "sono soprattutto i più recenti sviluppi delle tecnologie della comunicazione e il diffuso uso dei *social media* che sorreggono il bisogno della condivisione delle informazioni ad avere alimentato una irrefrenabile tendenza alla divulgazione delle informazioni personali".

[9] Come ha sottolineato R. Moro Visconti, *Valutazione dei* Big data *e impatto su innovazione e* digital branding, in *Dir. ind.*, 2016, p. 46 ss., "la diffusione di dispositivi portatili (smartphones, tablet, i-watch …) è in continuo aumento e la maggior parte delle transazioni viene da tempo effettuata on-line. Le azioni, attività e comportamenti degli individui sono ormai misurabili da dati che possono essere combinati con altri dati e analizzati da appositi strumenti. Grazie alle possibilità offerte dai sensori tecnologici e dall'identificazione biometrica, è inoltre possibile arrivare ad una raccolta di dati quantitativi sempre più rappresentativi sugli abitanti del mondo". Sul tema, si rinvia anche a V. Mayer-Schömberg, K. Cukier, *Big Data*, Milano, 2013; V. Zeno-Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 2, 2018; M. Bogni, A. Defant, Big Data: *diritti* IP *e problemi della* privacy, in *Dir. ind.*, 2015, p. 117 ss.; L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017.

[10] Il significato di tale espressione è ben enunciato nel considerando n. 71 e, soprattutto, nell'art. 4 del GDPR, a mente

Del resto, tutto ciò può avvenire ormai oggi anche in maniera passiva, grazie alle nuove frontiere della *Internet of Things* (IoT), che ha favorito l'espansione della raccolta di informazioni tramite veicoli, attrezzature ed elettrodomestici[11].

Una delle più grandi preoccupazioni della società contemporanea non è più legata solo (o tanto) alla diffusione di informazioni private – o alla difficoltà a veder tutelato il proprio diritto ad un corrette utilizzo delle stesse (in termini di aggiornamento e cancellazione) – quanto al rischio di non poter contenere il potere manipolativo della realtà, realizzato mediante la circolazione su *Internet* delle c.d. "*fake news*", ad opera di sistemi capaci di arrivare a distorcere i processi elettorali e – di conseguenza – ad effettuare un vero e proprio controllo politico all'interno di una determinata collettività[12].

La pericolosità delle nuove tecnologie si è mostrata in tutta la sua gravità più recentemente, con lo svilupparsi della c.d. Intelligenza artificiale, definita nella Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni COM(2018) 237, del 25 aprile 2018[13], come quell'insieme di "sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi".

L'idea di fondo dei precursori di tale "rivoluzione informatica" è sempre stata proprio quella di generare un insieme di "*routine* logiche", che, applicate all'informatica, consentano ai *computer* di non necessitare più della supervisione umana nel processo decisionale e nell'interpretazione dei messaggi analogici e digitali[14], ma – una volta stabilita la capacità del sistema di adattarsi ai bisogni umani, attraverso l'uso di dati provenienti da esperienze passate archiviate in memoria – siano in grado di prendere decisioni con un livello più o meno elevato di "libero arbitrio"[15].

Oggi, come è noto, ci sono diversi algoritmi di Intelligenza artificiale con prestazioni nettamente

---

del quale la "profilazione" è "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

[11] Come ha ben spiegato E. BATTELLI, Big data *e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi*, in *Corr. giur.*, 2019, p. 1520 ss., rinviando a K. ASHTON, *That "Internet of Things" Thing*, in RFID Journal, 2009; e G. NOTO LA DIEGA, I. WALDEN, *Contracting for the "Internet of Things": Looking into the Nest*, in *Queen Mary School of Law Legal Studies Research*, Paper No. 219, 2016, l'espressione si riferisce ad un sistema "di *devices* connessi alla rete e capaci di interagire a distanza con l'utente utilizzatore od operare in automatico sulla base della valutazione di determinati dati secondo le impostazioni predefinite. Il termine si riconduce allo studioso inglese Kevin Ashton, fondatore del Centro Auto-ID presso il MIT ed alle sue ricerche sul tema verso la fine degli anni Novanta". E R. MORO VISCONTI, *Valutazione dei* Big data, cit., p. 47, ha elencato i principali campi nei quali l'IoT opera con discreto successo (domotica e robotica; avionica; industria automobilistica; biomedicale; biometria; monitoraggio in ambito industriale; telemetria; reti *wireless* di sensori; sorveglianza, e rilevazione di eventi avversi, con monitoraggio del territorio; *smart grid* e *smart cities*; sistemi *embedded*; telematica). Sul tema, cfr. J. RIFKIN, *La società a costo marginale zero. L'Internet delle cose, l'ascesa del Commons Collaborativo e l'eclissi del capitalismo*, Milano, 2014; e F. GIOVANNELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2018, *passim*.

[12] Si veda, sul punto, l'interessante riflessione di E.S. GOMI, *Robôs são usados para divulgar notícias falsas na internet*, in *Jornal da USP*, visionabile anche in *https://jornal.usp.br/atualidades*.

[13] Il documento, dal titolo *L'intelligenza artificiale per l'Europa*, è reperibile sul sito *https://ec.europa.eu/transparency/regdoc/rep/1/2018/IT/COM-2018-237-F1-IT-MAIN-PART-1.PDF*.

[14] Se l'idea di costruire macchine pensanti si può attribuire già agli inventori dei primi calcolatori (Leibniz e Babbage) o al creatore della logica binaria, utilizzata nei computer, facilmente adattabile alle apparecchiature elettroniche (George Boole), certamente al matematico Alan Turing è comunemente attribuito il ruolo di fondatore del concetto di Intelligenza artificiale. Cfr. il suo noto articolo *Computing Machinery and Intelligence*, pubblicato nel 1950 sulla rivista *Mind*. Il lavoro si apriva con le emblematiche parole "*I propose to consider the question, 'Can machines think?'*".

[15] Questa intuizione produsse, ovviamente, un grande entusiasmo, perché si immaginò da subito la possibilità di scrivere una partitura musicale, sulla base dei suoni emessi da un pianoforte, e di svelare teoremi matematici o, ancora, di arrivare ad interpretare la personalità umana (fino a giungere, poi, negli anni '70, a prefigurare la possibilità di condurre diagnosi mediche mediante Intelligenza artificiale). V., sul punto, S. J. RUSSELL, P. NORVIG, *Artificial Intelligence. A Modern Approach*, Upper Saddle River, 2015; nonchè A. SANTOSUOSSO, *Diritto, scienza e nuove tecnologie*, Padova, 2016, p. 330 ss. Il metodo di base per la risoluzione dei problemi più semplici è quella utilizzata per il gioco degli scacchi, che, per calcolare tutte le possibilità di mosse future, usa a modello dinamico di rappresentazione quello degli spazi vuoti in una matrice 8x8. Ma, particolarmente interessanti sono apparse subito anche le operazioni di *alternative test* (utilizzate, ad esempio, nella soluzione del "problema del commesso viaggiatore", in cui l'algoritmo calcola il percorso più breve per giungere da un posto ad un altro) o le c.d. "ricerche euristiche" (attraverso le quali si chiede all'algoritmo di individuare rapidamente all'interno di un computer la risposta più soddisfacente e non quella migliore, tenendo conto che a volte all'utente potrebbe interessare di più risparmiare tempo e non avere una soluzione assolutamente precisa). V. E.A. RICH, *Artificial Intelligence*, New York, 1991, *passim*, e le sue riflessioni anche sugli schemi logici basati su "domande e risposte", nonché quelli sulla rappresentazione logica del processo di conoscenza umana.

superiori rispetto a quelle realizzate dai sistemi che si limitavano a mere elaborazioni di base[16] e si producono *computer* con *software* sofisticatissimi in grado di svolgere attività specifiche senza interruzione, come l'invio di *email*, l'elaborazione di un linguaggio naturale, l'apprendimento, e lo sviluppo di alcuni sensi (quali la vista, l'udito e perfino l'olfatto e il gusto), la generazione di soluzioni ragionevoli[17]; sino, ad arrivare, in tempi recenti alla creazione di *robot*[18] davvero molto simili agli esseri umani e dotati del cosiddetto *deep learning*[19].

Se i vantaggi di tutto ciò sono sotto abbastanza evidenti, spesso sfuggono i gravi rischi che tuttavia emergono, per i diritti fondamentali (di ogni essere umano, ma delle categorie più deboli in particolare)[20]. Non a caso, un illustre studioso francese del tema si è chiesto se l'umanità non si stia dirigendo verso forme di "*domination programmée*"[21].

Vari interessi di rango primario della persona, in effetti, possono essere violati da un uso improprio dell'Intelligenza artificiale: si pensi, oltre che al diritto alla vita e all'integrità fisica (si è parlato, a tal proposito, di un "diritto a ''potenziare'' il proprio corpo come nuovo diritto a disporre di sé stessi ed autodeterminarsi"[22], con tutte le implicazioni etiche che ne derivano sotto il profilo della costante tensione verso l'immortalità o un pericoloso modello di perfezione estetica[23]), a situazioni giuridiche soggettive fondamentali come l'onore, l'immagine, l'identità personale[24], e, *in primis* forse, la riservatezza.

---

[16] P. DOMINGOS, *L'Algoritmo Definitivo: la macchina che impara da sola e il futuro del nostro mondo*, Torino, 2016.

[17] Cfr. S. J. RUSSELL e P. NORVIG, cit.

[18] A. LAURENT, J. BESNIER, *Do Robots make love? From AI to immortality – Understanding transhumanism in 12 questions*, Londra, 2018; D. BERRY, A. FAGERJORD, *Digital humanities*, Cambridge, 2017.

[19] Sul quale anche il Consiglio di Stato ha per la prima volta preso posizione, con la sentenza n. 2270 dell'8 aprile 2019, evidenziando che "l'utilizzo di procedure 'robotizzate' di decisione della P.A., tramite algoritmi, per quanto legittimo, non può essere motivo di elusione dei princìpi che conformano il nostro ordinamento e che regolano lo svolgersi dell'attività amministrativa", e, pertanto, "la regola algoritmica [...] vede sempre la necessità che sia l'amministrazione a compiere un ruolo *ex ante* di mediazione e composizione di interessi, anche per mezzo di costanti test, aggiornamenti e modalità di perfezionamento dell'algoritmo (soprattutto nel caso di apprendimento progressivo e di *deep learning*)".

[20] Il tema è centrale anche nelle discussioni istituzionali delle organizzazioni internazionali operanti nel Vecchio continente. Una ricerca del Consiglio d'Europa ("*Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*", in *https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5*) ha dimostrato quante ripercussioni su numerosi diritti fondamentali potrebbe avere un uso inappropriato dell'Intelligenza artificiale. Ed ecco perché, agendo all'interno dello stesso organo, la *European Commission for the Efficiency of Justice* ha elaborato il 3-4 dicembre 2018 una Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziari e in ambiti connessi (in *https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348*). E significative sono, inoltre, sul versante dell'Unione europea, la citata Comunicazione della Commissione COM(2018) 237 del 25 aprile 2018 (con un Allegato, intitolato Piano coordinato per lo sviluppo e l'utilizzo dell'Intelligenza artificiale "*Made in Europe"*) e la Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e Intelligenza artificiale. Nel Libro bianco dello scorso 19 febbraio 2020, si legge chiaramente che "l'uso dell'IA può pregiudicare i valori su cui si fonda l'Unione e causare violazioni dei diritti fondamentali, compresi i diritti alle libertà di espressione e di riunione, la dignità umana, la non discriminazione fondata sul sesso, sulla razza, sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale (ove applicabili in determinati settori), la protezione dei dati personali e della vita privata o il diritto a un ricorso giurisdizionale effettivo e a un giudice imparziale, nonché la tutela dei consumatori".

[21] J.-G. GANASCIA, *Intelligence artificielle: vers une domination programmée*?, Paris, 2017. Nel febbraio 2018, uno studio di M. BRUNDAGE e altri suoi colleghi di Cambridge e Oxford, dal titolo *The malicious use of artificial intelligence: forecasting, prevention, and mitigation*, University of Cambridge, 2018, ha indicato tre tipi di rischi che possono derivare dall'Intelligenza artificiale: quello per la c.d. "sicurezza digitale" (che può essere minata da intensi attacchi informatici diffusi), quello per la sicurezza fisica (legato a possibili lesioni causati da droni o armi gestiti attraverso l'IA), ed infine quello per la "sicurezza politica" (considerata la possibilità di monitoraggi collettivi derivanti dall'analisi dei dati di massa, di manipolazioni attraverso video e mediante lo studio del comportamento umano, dei costumi e delle credenze). Il rapporto propone quattro forti raccomandazioni in materia. Il primo è che legislatori e scienziati collaborino per una approfondita indagine del problema e l'individuazione di divieti o controlli nei potenziali usi dannosi di questa tecnologia. Il secondo è che ricercatori e ingegneri prendano sul serio il doppio possibile uso (benefico e malefico) dell'Intelligenza artificiale. La terza raccomandazione è che siano identificate e diffuse le buone pratiche nel settore. La quarta e ultima riguarda l'estensione del dibattito al maggior numero di parti interessate ed esperti della materia.

[22] Cfr., per tutti, U. RUFFOLO, A. AMIDEI, cit., p. 1664.

[23] Secondo U. RUFFOLO, A. AMIDEI, cit., p. 1658, "gli sviluppi dell'Intelligenza Artificiale e della robotica avanzata, sinergicamente uniti a forme di '*genetic engineering*' (genomica migliorativa, *doping* genetico, *gene-editing*, pratiche di *life-extension*), potranno [...] dare vita a commistioni uomo-macchina suscettibili di rappresentare la 'via umana alla immortalità', quantomeno come prolungamento della vita o della coscienza anche dopo la morte del corpo. Tanto, grazie ad una sempre più stretta interazione tra macchina e *framework* neuronale umano; interazione che conduce taluni a teorizzare la (ancora molto lontana) possibilità di trasferire una coscienza umana su supporti artificiali, magari per garantire la sopravvivenza ad una mente altrimenti prigioniera di un corpo in decadimento e destinata a perire con esso".

[24] Sempre U. RUFFOLO, A. AMIDEI, cit., p. 1670, segnalano che la stessa prospettiva del trapianto di un cervello non sembra così remota e lo stesso dicasi per la possibilità di impiantare addirittura la testa su corpo altrui, con conseguenti "problemi

La recente pandemia ha dimostrato quanto fragile sia ormai già solo lo stesso diritto ad una reale autodeterminazione "informatica" o "informativa"[25] (e quindi a scegliere se entrare o meno a far parte del mondo virtuale e comunque a decidere realmente della sorte dei propri dati personali[26]), a fronte, ad esempio, di emergenze globali, capaci di far prevalere in modo "tirannico" (sia pur legittimamente, forse) un contrapposto diritto (superindividuale) alla salute, che può costringere tutti a ricorrere alle nuove tecnologie, senza avere alcuna alternativa – né poter esprimere un proprio consenso al riguardo – (salvo voler rinunciare al lavoro, allo studio e allo svolgimento di qualsiasi attività idonea ad una – seppur fortemente limitata – realizzazione della propria personalità)[27].

2. La non semplice garanzia dei principi generali in materia di tutela dei dati personali a fronte di trattamenti effettuati da *software* di IA.

Uno dei maggiori rischi legati ad un non corretto utilizzo dell'Intelligenza artificiale riguarda la possibilità che quest'ultima leda, con una sola operazione ed in pochi secondi, il diritto alla *privacy* di milioni di individui.

Del resto, è sufficiente analizzare i "principi applicabili al trattamento dei dati personali"[28], indicati nell'art. 5 del GDPR europeo[29], per verificare come, in linea di principio, appaia oggettivamente complicato pensare che il crescente utilizzo di sistemi digitali e di macchine dotate di *deep learning* non ponga grossi (e spesso difficilmente risolvibili) problemi con riguardo alla possibile violazione della riservatezza degli utenti.

Secondo il Regolamento europeo, i *personal data* vanno, anzitutto, "trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ('liceità, correttezza e trasparenza')". Come precisa anche il considerando n. 39, insomma, per un verso, dovrebbero risultare trasparenti per le persone fisiche "le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati"[30], e, per un altro, andrebbe garantito, sulla *home page* del sito *Internet* ad esempio, che "le informazioni e le comunicazioni relative al trattamento [...] siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro"[31]. Ciò implica un doppio (e non semplice) sforzo nello sviluppo e nell'uso dei sistemi di IA: anzitutto, la capacità di riuscire a spiegare a soggetti non esperti del settore i processi e le modalità con i quali operano le nuove tecnologie utilizzando dati personali (circostanza che diventa quasi impossibile nel caso in cui si tratti di far comprendere, ad esempio, come le informazioni recuperate da una *black box* sono correlate e ponderate in un processo specifico[32]), e poi quella di riuscire a bilanciare tra obblighi di trasparenza (e diritto di accesso ai dati) e divieto di rivelare segreti commerciali e diritti di proprietà intellettuale (così come previsto dal considerando n. 63[33]). Del resto, secondo quanto è stato ben

persino circa la 'identità' del trapiantato (tali trapianti sono attualmente vietati. Ma in caso di violazione del divieto – forse prossimo a venir meno – tutti i richiamati problemi permarrebbero)".

[25] G. SARTOR, *Privacy, reputazione, e affidamento: dialettica e implicazioni per il trattamento dei dati personali*, in F. BERGADANO, A. MANTELERO, G. RUFFO, G. SARTOR, *Privacy digitale. Giuristi ed informatici a confronto*, Torino, 2005, p. 81 ss.

[26] Si tratta di un diritto già di per sé assolutamente debole, anche secondo D. POLETTI, cit., p. 2785, considerando che "come dimostrato anche da recenti indagini comportamentali, proporzionalmente alle reiterate richieste di consenso si riduce la soglia di attenzione, anche per l'informativa, con conseguente debolezza cognitiva e compromissione del processo decisionale". Per cui, segnala la studiosa, si sta assistendo ad un vero e proprio paradosso: "mentre cresce sempre di più la richiesta di consenso, per garantire il titolare piuttosto che l'interessato, questi si limita a fornire sempre più distrattamente un mero assenso al trattamento determinato dal primo, senza alcuna possibilità di incidenza sulle modalità e sulla scelta dei mezzi del trattamento, se non quella affidata all'esercizio dei suoi diritti e alla possibilità di revoca del consenso, che non sempre sarà dotata di effettività quando la circolazione dei dati, per esempio, sia ormai divenuta virale nella rete".

[27] Si registrano già numerosi contributi dottrinali *online* su questi importanti temi in *www.unicost.eu*, www.*sistemapenale*.it, *www.federalismi.it*, *www.rivistaaic.it*, ecc.

[28] Sull'argomento, si veda G. FINOCCHIARO, cit., p. 1673 ss.

[29] Il secondo comma del par. 1 stabilisce che "il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ('responsabilizzazione')". E nel considerando n. 74 si sottolinea che il soggetto in questione "dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche".

[30] Non a caso, gli articoli 13 e 14 del GDPR si occupano delle informazioni da fornire qualora i dati personali siano stati raccolti presso l'interessato stesso o tramite altri soggetti.

[31] Secondo le modalità indicate nell'art. 12 del GDPR.

[32] Si veda E. PELLECCHIA, *Profilazione e decisioni automatizzate*, cit., p. 1210 ss.

[33] Nel quale si legge che "ogni interessato dovrebbe [...] avere il diritto di conoscere e ottenere comunicazioni [...] in relazione alla finalità per cui i dati personali sono trattati, ove possibile al

segnalato ad esempio dalla *Norvegian Data Protection Authority*, il principio impone al "*data controller to implement measures to prevent the arbitrary discriminatory treatment of individual persons* [...]. *The model must not emphasise information relating to racial or ethnic origin, political opinion, religion or belief, trade union membership, genetic status, health status or sexual orientation if this would lead to arbitrary discriminatory treatment*"[34].

La seconda regola fondamentale contenuta nel Regolamento europeo riguarda il dovere di raccogliere, e successivamente trattare, i dati solo "per finalità determinate, esplicite e legittime", pur con la precisazione che un utilizzo degli stessi "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"[35]. Anche tale principio (della c.d. "limitazione della finalità") diventa nevralgico nel caso di utilizzo di tecnologie dotate di *self-learning*. Il riutilizzo di informazioni può, infatti, essere essenziale per fornire analisi più accurate di quelle tecnicamente realizzabili in precedenza, ma rischia di porsi in contrasto con la previsione normativa or ora citata. Per questo, si renderà necessario l'arduo compito di valutare se il nuovo scopo sia compatibile con quello originale o se occorra un nuovo consenso da parte dell'interessato. Un esempio che si può fare al riguardo concerne la possibilità che il noto *social network Facebook* dia particolare enfasi alla scelta di alcuni utenti di condividere determinati *link*, o di aderire a qualche campagna antidiscriminatoria (in ipotesi, con una modifica della propria foto profilo), o addirittura trasferisca queste informazioni per finalità di *marketing*. Certamente, sembra possibile che – anche senza un nuovo consenso dell'interessato – tali informazioni siano utilizzate a fini statistici o in connessione con scopi di ricerca scientifica o storica, o per statistica, nell'interesse pubblico. Ciò implica, tuttavia, una complessa analisi di cosa rappresenti la ricerca scientifica e in che misura lo sviluppo e l'applicazione dell'Intelligenza artificiale possano rientrare in tale concetto. Un crescente numero di ricerche universitarie e ospedaliere sta avendo ad oggetto lo sviluppo di strumenti di IA. Si pensi ai modelli che possano consentire di identificare il rischio di frode fiscale o previdenziale o ai *software* riguardanti sistemi di riconoscimento di forme per effettuare diagnosi su un'ampia gamma di dati in forma di immagini (fondamentali ad esempio per poter riconoscere alcuni tumori[36]). Il problema riguardante la corretta individuazione di ciò che

periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento", ma anche all'accesso remoto a un sistema sicuro che gli consenta "di consultare direttamente i propri dati personali". Tuttavia, "tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software", benché "tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni". Pertanto, "se il titolare del trattamento tratta una notevole quantità di informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce".

[34] Così nel *Report "Artificial intelligence and privacy"* del gennaio 2018, reperibile sul sito *www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf*. Nel documento si precisa, peraltro, che "*if it is suspected, or claimed, that use of a model will entail unfair or discriminatory results, the Data Protection Authority can investigate whether the principle of fairness has been safeguarded in the processing of personal data*" e "*these investigations may include a review of the documentation underpinning the selection of data, an examination of how the algorithm was developed, and whether it was properly tested before it came into use*".

[35] Secondo tale disposizione, "il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo".

[36] V. R. KURZWEIL, *La singolarità è vicina*, 2008, Milano, p. 277. Secondo lo studioso, "tutti i principali sviluppatori di farmaci usano programmi di IA per il riconoscimento di forme e il *data mining* intelligente nella ricerca di nuove terapie farmacologiche. Per esempio, la SRI International sta costruendo basi di conoscenza flessibili che codificano tutto quello che sappiamo su una dozzina di agenti patogeni, fra cui quello della tubercolosi e H. *pylori* (i batteri che provocano l'ulcera). L'obiettivo è applicare strumenti di *data mining* intelligente (software in grado di cercare nuove relazioni nei dati) per trovare nuovi modi di distruggere o alterare il metabolismo di questi patogeni. Sistemi simili si applicano alla scoperta automatica di nuove terapie per altre malattie, e per capire la funzione dei geni e il loro ruolo nella malattia. Per esempio, gli Abbott Laboratories sostengono che nei loro nuovi laboratori sei ricercatori dotati di sistemi basati sull'IA, robotici e di analisi dei dati, possono ottenere gli stessi risultati di duecento scienziati nei loro vecchi laboratori di sviluppo. Gli uomini con livelli elevati di PSA (antigene prostato-specifico) normalmente devono subire una biopsia chirurgica, ma nel 75 per cento dei casi non hanno un tumore alla prostata. Un nuovo test, basato sul riconoscimento di proteine nel sangue, può ridurre il tasso dei falsi positivi a circa il 29 per cento. Il test è basato su un programma di IA [...] e si prevede che l'accuratezza del sistema migliori ulteriormente con il proseguimento dello sviluppo".

possa essere considerato realmente "ricerca scientifica" è legato anche all'assenza di chiarimenti sul punto da parte del GDPR (ad eccezione delle utili indicazioni contenute nel considerando n. 159, secondo il quale "il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE"[37]). Se, sicuramente quindi, l'utilizzo dell'Intelligenza artificiale per valutare l'affidabilità creditizia di un individuo non può essere considerato tra le attività finalizzate ad acquisire nuove conoscenze scientifiche, negli altri casi sopra citati non è sempre facile distinguere tra sviluppo e mera applicazione dell'IA.

La lettera c) del primo paragrafo dell'art. 5 del Regolamento europeo enuncia il terzo, importante principio in materia di utilizzo dei dati personali, in base al quale questi ultimi devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (c.d. "minimizzazione dei dati"). Anche questa regola crea non poche perplessità nel caso di utilizzo di meccanismi di Intelligenza artificiale. E ciò anzitutto perché non è possibile stabilire con la massima precisione cosa l'algoritmo apprenderà e quindi quali dati considererà necessari e direttamente collegati allo scopo da raggiungere (soprattutto nel caso in cui si tratti di *deep learning*, che, come è noto, può comportare significative variazioni "in corso d'opera" con riguardo a ciò che la macchina riesce ad imparare e sviluppare)[38]. Né è semplice garantire il citato principio di proporzionalità tra raccolta e obiettivo prefissato (sicuramente, la pseudonimizzazione o le tecniche di crittografia, rendendo difficile – se non quasi impossibile – l'identificazione degli interessati, potranno fornire a tal riguardo un ausilio non marginale). Centrale appare, sotto questo profilo, il compito di operare, e rendere documentabili, scelte idonee a garantire la minore invasività possibile per la riservatezza degli interessati (al fine di proteggere così i diritti di questi ultimi, ma anche una fiducia collettiva nei confronti delle macchine individuate per quel determinato obiettivo), partendo dalla consapevolezza che è importante selezionare bene i dati funzionali allo scopo (anche in termini di quantità e natura delle informazioni, poiché alcuni dettagli rivelano di più su una persona rispetto ad altri) e che occorre evitare di fornire indicazioni irrilevanti (ma, capaci, magari, di condurre l'algoritmo a trovare correlazioni del tutto casuali e non significative).

Particolarmente importante appare poi la previsione contenuta nella lettera "d" dello stesso paragrafo, secondo la quale i dati devono essere "esatti e, se necessario, aggiornati" e vanno "adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati". Si è a tal proposito parlato di un diritto, strettamente legato a quello alla propria identità personale, ad essere riconosciuti nei rapporti sociali per quelli che realmente si è (senza neppure "ritocchi migliorativi"). E ciò implica, ovviamente, l'adozione di misure adeguate di fronte alle nuove tecniche di trattamento dei *personal data* (artt. 25 e 32), anche al fine di tutelare l'eventuale legittima pretesa dell'interessato all'aggiornamento, alla rettifica e addirittura alla cancellazione dei dati inesatti (art. 17 GDPR)[39]. Uno dei problemi che può realizzarsi, con riferimento a *software* che si servono di algoritmi, è che si venga a tracciare un profilo (totalmente o parzialmente) inesatto della persona e, a partire da ciò, vengano adottate decisioni sbagliate. Le macchine che operano secondo le tecniche di Intelligenza artificiale

[37] Nello stesso considerando si precisa, peraltro, che "le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica. Per rispondere alle specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica. Se il risultato della ricerca scientifica, in particolare nel contesto sanitario, costituisce motivo per ulteriori misure nell'interesse dell'interessato, le norme generali del presente regolamento dovrebbero applicarsi in vista di tali misure".

[38] Per questo, si parla (come si vedrà a breve) di una responsabilità *by design*.

[39] Come segnala F. PIRAINO, *GDPR tra novità e discontinuità – I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in *Giur. it.*, 2019, p. 2794, "il diritto alla cancellazione" di cui parla la disposizione in questione ha una portata più ampia rispetto a quella legata al più specifico "diritto all'oblio", "presentandosi come il potere di riappropriarsi delle informazioni di carattere personale nel caso tanto di trattamento illecito o scorretto (art. 17, par. 1, lett. d), Regolamento) quanto di obbligo legale di cancellazione imposto al titolare dal diritto dell'Unione europea o dello Stato membro di appartenenza quanto ancora di esercizio del potere sostanziale di autodeterminazione informativa", se, ad esempio, "l'impiego e la circolazione di tali informazioni non vengono più reputati opportuni o comunque non risultano più graditi o ancora confliggono con gli obiettivi e le strategie dell'interessato in ordine alla costruzione o all'evoluzione della propria identità personale o anche soltanto con più limitati fini specifici". Sul tema, si veda inoltre R. SENIGAGLIA, *Il Reg. UE 2016/679 e il diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Leggi civ. comm.*, 2017, p. 1023 ss.

potrebbero non essere in grado, ad esempio, di distinguere i motivi che portano un soggetto a leggere un determinato argomento, o ad ascoltare un certo brano musicale, e da ciò potrebbero trarre conclusioni indebite e indesiderate. Il fatto che qualcuno faccia una ricerca tramite un motore di ricerca su certo tema controverso potrebbe essere erroneamente interpretato come segno del desiderio di aderire all'idea in questione, quando, in realtà, la volontà dell'interessato era esattamente opposta. Ma, si pensi anche all'ipotesi in cui, in un *social network*, un utente acceda alla pagina di un altro soggetto, estraneo alla sua rete di contatti, e l'algoritmo, interpretando tale contegno come indicativo dell'esistenza di un rapporto di amicizia "*offline*", suggerisca all'utente titolare dell'*account* "visitato" di "chiedere l'amicizia" alla persona che ha "controllato" il suo profilo. E lo stesso equivoco potrebbe realizzarsi a fronte di un *like* messo, in ipotesi, alla pagina di un personaggio politico, per puro sbaglio o per sarcasmo ovvero, ancora, al solo fine di essere aggiornato sui *post* da quello pubblicato (ma, non certo perché se ne condivida il pensiero).

Gli ultimi due principi, anch'essi rilevantissimi, in materia sono contenuti nelle lettere e) ed f) del primo comma dell'art. 5, e riguardano rispettivamente il dovere di conservare i dati personali "in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati [...] ('limitazione della conservazione')"[40] e quello di trattarli in maniera da garantire loro "un'adeguata sicurezza [...], compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ('integrità e riservatezza')".

Entrambi gli obiettivi sembrano di facile realizzazione nel caso di procedure che si servano dell'Intelligenza artificiale[41]. Il problema non concerne tanto il "dopo" (vari *social network*, come *facebook*, proprio per garantire una adeguata sicurezza ed il pieno rispetto del volere dei titolari degli *account*, consentono di individuare addirittura una persona di fiducia alla quale assegnare il compito di gestire il "profilo" dopo la loro morte), ma semmai cosa può accadere "durante" il trattamento.

3. I rischi per la c.d. autodeterminazione informativa in presenza di operazioni automatizzate.

In tema di tutela della riservatezza (anche e soprattutto a fronte delle nuove frontiere dell'Intelligenza artificiale), rimane centrale il problema del consenso informato (e della sua idoneità a tutelare gli interessi degli utenti).

Secondo taluni studiosi, un errore ascrivibile al modello normativo esistente in materia di diritto alla *privacy* riguarda proprio la scelta di basare il sistema di protezione dei dati su una sorta di preventiva autorizzazione dell'interessato[42]. Una siffatta impostazione può infatti funzionare correttamente quando si tratta di una singola informazione riguardante il soggetto in questione, come nel caso di un *database*, creato ad esempio nell'àmbito di un servizio di protezione del credito, nel quale è possibile ed agevole trovare le informazioni e richiedere la loro rettifica. Essa risulta, viceversa, impraticabile nel caso in cui centinaia di informazioni vengono raccolte ed elaborate automaticamente, utilizzando algoritmi[43].

---

[40] La stessa lett. e) stabilisce anche che "i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato".

[41] Il testo dell'OCSE, *Artificial Intelligence in Society*, cit., p. 88 evidenzia che "*AI also challenges personal data protection principles of collection limitation, use limitation and purpose specification" e rileva, in particolare, che "the increasing combination of AI and IoT technologies (e.g. IoT devices equipped with AI, or AI algorithms used to analyse IoT data) means that more data, including personal data, are constantly gathered. These can be increasingly linked and analysed. On the one hand, there is an increased presence of devices collecting information (e.g. surveillance cameras or autonomous vehicles [AVs]). On the other, there is better AI technology (e.g. facial recognition). The combination of these two trends risks leading to more invasive outcomes than either factor separately*".

[42] Per D. POLETTI, cit., p. 2785, "ammesso che il consenso al trattamento abbia mai avuto un periodo di reale fasto, sono sempre più frequenti oggi i richiami al suo declino, alla sua recessione, alla sua parabola discendente. L'architettura del regolamento e la sua diretta vincolatività per i cittadini degli stati membri hanno avuto effettivamente come conseguenza, intanto, l'eliminazione del ruolo decisivo del consenso [...] anche se [...] sembra rafforzarsi nella sua modalità di manifestazione, divenendo 'esplicito' e 'inequivocabile', e riveste un ruolo decisivo nel caso (rilevante soprattutto per le applicazioni di *intelligenza artificiale*) del trattamento automatizzato dei dati personali (art. 22)".

[43] Anche secondo G. FINOCCHIARO, cit., p. 1677, "il consenso, astrattamente il miglior modello possibile, si rivela spesso non adeguato nel fornire una tutela effettiva ed inefficace. 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".

Sebbene occorreranno anni per valutare come determinati parametri di protezione saranno accettati dagli Stati membri dell'Unione, è innegabile che il Regolamento europeo sia almeno molto dettagliato in merito alla protezione da accordare ai dati dei soggetti, sia dal punto di vista del dovere di informazione da dare in merito allo scopo per il quale essi sono stati raccolti, sia con riguardo ad una disciplina ben più rigorosa – consistente in un generale divieto di utilizzo, se non altro in linea di principio – per quel che concerne le informazioni idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, ovvero i dati genetici o biometrici (capaci di identificare in modo univoco una persona fisica), e quelli relativi alla salute o alla vita (o orientamento) sessuale della persona (art. 9 GDPR[44]). Il punto è che, stando a quanto ha rilevato anche l'OCSE, perfino all'interno dello stesso Regolamento europeo "*it is increasingly difficult to distinguish between sensitive and non-sensitive data* [...]" e "*some algorithms can infer sensitive information from 'non-sensitive' data, such as assessing individuals' emotional state based on their keyboard typing pattern (Privacy International and Article 19, 2018[10])*", così come, del resto, lo stesso "*use of AI to identify or re-identify data that originally were non-personal or de-identified* [...] *presents a legal issue*"[45].

Non va cioè dimenticato che, come già segnalato, effettuando delle analisi incrociate su diversi tipi di dati personali è possibile ricavare "informazioni sensibili" dei soggetti interessati. Ad esempio, una serie di "*like*" messi su *Facebook* a determinate pagine, combinata con alcune risposte date ad un semplice sondaggio, consentono con una elevata precisione (anche se non sicurezza massima) di individuare l'esistenza di un problema di salute o le tendenze sessuali o la fede religiosa degli utenti. Una qualsiasi attività che consenta di giungere a simili risultati dovrebbe essere, secondo alcuni studiosi, soggetta agli stessi obblighi previsti dal Regolamento per i trattamenti che sin dall'inizio riguardino i dati sensibili[46].

Interessante appare, a tal proposito, quanto sancito nel GDPR, agli artt. 15, comma 1 (concernente il diritto dell'interessato ad "ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni" circa "l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste"[47]), e 22, par. 3 (secondo il quale "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").

[44] Il secondo paragrafo della disposizione introduce una serie di deroghe al divieto stabilito nel primo comma, basate (sempre nel rispetto di varie condizioni dettagliatamente indicate) sul consenso esplicito dell'interessato o sulla scelta di quest'ultimo di renderli manifestamente pubblici, ovvero sulla necessità di un loro utilizzo per adempiere ad un obbligo o esercitare determinati diritti, o "per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso"; ovvero se "il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; o se il trattamento è necessario per motivi di ordine pubblico o di interesse collettivo nel settore della sanità pubblica e della medicina preventiva, medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali, ovvero a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica" o, ancora, "per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali".

[45] OCSE (2019), *Artificial Intelligence in Society*, Parigi, in *https://doi.org/10.1787/eedfee77-en*, p. 84.

[46] Sempre nel citato documento dell'OCSE, *Artificial Intelligence in Society*, p. 87, si sottolinea che "*AI can increasingly link different datasets and match different types of information with profound consequences. Data held separately were once considered non-personal (or were stripped of personal identifiers, i.e. "de-identified"). With AI, however, non-personal data can be correlated with other data and matched to specific individuals, becoming personal (or "re-identified"). Thus, algorithmic correlation weakens the distinction between personal data and other data. Non-personal data can increasingly be used to re-identify individuals or infer sensitive information about them, beyond what was originally and knowingly disclosed (Cellarius, 2017[9]). In 2007, for example, researchers had already used reportedly anonymous data to link Netflix's list of movie rentals with reviews posted on IMDB. In this way, they identified individual renters and accessed their complete rental history. With more data collected, and technological improvements, such links are increasingly possible. It becomes difficult to assess which data can be considered and will remain non-personal*".

[47] Sull'argomento, cfr. O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, p. 573 ss.

Ma, meritevole di considerazione è anche il c.d. diritto alla spiegazione[48], menzionato *apertis verbis* invero solo nel considerando n. 71 del GDPR[49], secondo il quale, nel caso di profilazione del soggetto, quest'ultimo dovrebbe avere "una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione". Per una parte della dottrina, parrebbe esserci solo un *desideratum*, ma non un obbligo vero e proprio di informazione dettagliata[50]. Per un'altra, invece, quest'ultimo rileverebbe, ma solo se la decisione è basata esclusivamente sul trattamento automatizzato: in presenza di un qualsiasi intervento umano, invece, non opererebbe il vincolo in questione[51]. Il vero problema resta quello di fornire una "spiegazione" che possa essere compresa dai "non addetti ai lavori" e questo non è assolutamente semplice o scontato[52].

4. *La tutela dei (e dai)* Big data, *fra crescenti utilizzi di* chatbot *e sempre più sofisticate pratiche di* business-analytics.

Tra i servizi informatici che l'Intelligenza artificiale ha reso molto più sofisticati e funzionali, nella "società digitale" del terzo millennio, ci sono sicuramente i *chatbot* per i consumatori e la c.d. *business-analytics* per le imprese.

Un *chatbot* intelligente altro non è che un programma informatico, molto diffuso ormai in vari settori (dall'*healthcare* al *customer service*), capace di consentire agli individui di interagire vocalmente o per iscritto con una macchina, la quale, dopo aver analizzato tutte le informazioni comunicatele, attraverso una razionale combinazione tra le domande poste dagli utenti e le risposte tipiche fornite dal servizio clienti, è in grado di suggerire soluzioni adeguate ai problemi segnalati dagli interessati[53]. Ovviamente, maggiore sarà il volume di informazioni di cui disporrà l'interfaccia conversazionale (che presenta il vantaggio di essere rapida, disponibile h 24 e 365 giorni l'anno, e talvolta magari perfino più chiara e gentile di un operatore umano) e migliore, dal punto di vista della precisione e accuratezza, sarà la sua risposta.

La *business-analytics*[54], strumento centrale ormai in quella che viene sempre più comunemente definita la *data-driven economy*[55], mira invece

[48] V., ad esempio, A. BURT, «*Is there a right to explanation for machine learning in the GDPR*?», in *https://iapp.org/news/a/is-there-a-right-toexplanation-for-machine-learning-in-the-gdpr/*.

[49] Secondo il quale, "l'interessato dovrebbe 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. Tale trattamento comprende la 'profilazione' [...]. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri [...], anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale [...], o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. 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. Tale misura non dovrebbe riguardare un minore [...]. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni".

[50] V. S. WATCHER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, p. 76 ss.

[51] Sul punto, si rinvia a P. HACKER, R. KRESTEL, S. GRUNDMANN, F. NAUMANN, *Explainable AI under contract and tort law: legal incentives and technical challenges*, in *https://doi.org/10.1007/s10506-020-09260-6*. Gli autori, con riguardo al contenuto di tale *duty of information*, segnalano che secondo alcuni studiosi esso riguarderebbe solo la struttura generale e l'architettura del modello di elaborazione, senza dover entrare nel merito delle decisioni individuali o pesi e caratteristiche concrete del modello. Per altri, viceversa, dovendo le informazioni essere idonee a garantire all'interessato la possibilità di esercitare i suoi diritti indicati nei parr. 1 e 3 dell'art. 22 (incluso quello alla contestazione della decisione) è implicitamente prevista la necessità di fornire spiegazioni specifiche, concernenti anche i fattori utilizzati per raggiungere la scelta, al fine di verificare l'accuratezza della protezione e per contestarne eventualmente la correttezza. Cfr., per tutti, E. PELLECCHIA, *Profilazione e decisioni automatizzate*, cit., p. 1224 ss.; R. MESSINETTI, cit., p. 477 ss., e G. FINOCCHIARO, cit., p. 1657 ss.

[52] Sulle difficoltà "ad intendersi" che potrebbero sorgere già solo nel dialogo tra gli esperti, ma in settori differenti, quali informatici e giuristi, si rinvia a I. GIUFFRIDA, F. LEDERER e N. VERMEYS, *A legal perspective on the trials and tribulations of AI: how artificial intelligence, the Internet of Things, Smart Contracts, and other technologies will affect the Law*, in *Case Western Reserve Law Review*, 2018, p. 747 ss.

[53] Studi scientifici hanno dimostrato che grazie al c.d. NLP (*Natural Language Processing*), il *bot* riesce addirittura a comprendere i quesiti dei clienti nei casi in cui essi sono posti in maniera non del tutto chiara, o utilizzando abbreviazioni, termini arcaici, modi di dire o termini formali, e perfino neologismi (dal significato facilmente intuibile).

[54] R. MORO VISCONTI, *L'intelligenza artificiale…*, cit., p. 423 ss., riporta alcuni esempi di applicazione dell'Intelligenza artificiale nell'ambito delle *business solution* (come il *Sensor processing*, la *knowledge representation*, la *FinTech*, o la realtà aumentata).

[55] Sulla quale, v., tra i tanti, E. BATTELLI, *Il paternalismo giuridico libertario nella prospettiva dell'autonomia privata tra vincoli strutturali e limiti funzionali*, in *Pol. dir.*, 2018, p. 579 ss.; G. PITRUZZELLA, *Big Data and antitrust enforcement*, in *Italian Antitrust Review*, 2017, p. 10 ss.; A. MINUTO RIZZO, *I profili* antitrust *del nuovo* web *e della nuova economia digitale*,

all'analisi predittiva di possibili *trend* e risultati futuri, partendo da un'indagine statistica e dallo studio dei *data mining* ed effettuando delle possibili modifiche intermedie, in vista del *goal* da perseguire. Servendosi dell'Intelligenza artificiale, questa strategia commerciale ha la possibilità di verificare quali sono i tipi di beni per i quali si è registrato un incremento di domanda da parte degli utenti, ma anche le ragioni che hanno indotto a tale scelta: una pubblicità di successo (mandata ad un certo orario della giornata), ad esempio, o il consiglio dato su *Internet* da qualche *fashion blogger* (sul quale occorre "investire" maggiormente), ovvero ancora un sito ben costruito (che va monitorato per verificare quanti accessi ha avuto e in quali giorni della settimana). Anche in questo caso, senza dubbio, uno dei mezzi più importanti oggi, per una adeguata strategia commerciale, è rappresentato dai c.d. *Big data*[56], i quali avrebbero il vantaggio di godere delle cosiddette "5 v"[57] (volume, velocità, varietà, veridicità e valore dei dati)[58] e sono quindi una risorsa importante, da tutelare e valorizzare (ad esempio per la ricerca, lo sviluppo scientifico e tutte le altre finalità di rilevanza sociale alle quali essi si prestano).

Sarebbero però proprio alcune delle caratteristiche tipiche di questi "megadati" a rappresentare uno dei veri rischi legati allo sviluppo dell'IA associata alla diffusione di massa di *Internet*[59].

Attraverso la conoscenza dei comportamenti delle persone, è possibile creare una pubblicità mirata ed indirizzare informazioni false (o solo semi-fondate, ma ben "confezionate") a soggetti privi degli strumenti per poter discernere la verità dalle *fake news*, al fine di manipolare il loro comportamento, non solo in termini di preferenze culturali o di consumo, ma anche di scelte politiche o religiose, creando così una sorta di "polizia del pensiero" ed imponendo un determinato "*ranking*" sociale a buona parte della collettività (come sta accadendo in Cina col *Social credit system*[60]).

E ciò diventa particolarmente pericoloso, ove si pensi che gli stessi trattamenti algoritmici potrebbero avere, come si è visto, dei dati di partenza "errati, imprecisi o incompleti" o essere "creati da decisori umani che, già in fase di progettazione, ne possono influenzare l'analisi e distorcere l'elaborazione, conducendo a risultati lesivi dei diritti e delle libertà individuali"[61].

---

in *Riv. dir. ind.*, 2019, p. 113 ss.; V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten legal perspectives on the ''big data revolution''*, in *Conc. merc*., 2016, p. 39 ss.; B. LASSERRE, A. MUNDT, *Competition law and Big Data: the enforcers' view*, in Italian Antitrust Review, 2017, p. 17ss.; R. MORO VISCONTI, *Valutazione dei* Big data, cit.; M. E. STUCKE, A.P. GRUNES, *Big Data and Competition Policy*, Oxford, 2016, reperibile anche in *https://global.oup.com/academic/product/big-data-and-competition-policy-9780198788133?cc=fr&lang=en&*; G. MUSCOLO e A. MINUTO RIZZO, Big data, cloud computing *e concorrenza*, in M. FRANZOSI, O. POLLICINO, G. CAMPUS (a cura di), *Il Digital Single Market e i Cloud Services*, Roma, 2018, p. 39 ss.; M. BOURREAU, A. DE STREEL, I. GRAEF, *Big data and competition policy: market power, personalised pricing and advertising*, in *https://cerre.eu/sites/cerre/files/170216_cerre_compdata_finalreport.pdf*. V., inoltre, OCSE (2016), *Big data: bringing competition policy to the digital era - Background note by the Secretariat*, in *http://www.oecd.org/competition/big-data-bringing-competition-policy-tothe-digital-era.htm.*

[56] Sui quali, v., per tutti, E. BATTELLI, Big data *e algoritmi predittivi*, cit., p. 1517 ss.; M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019; M. SOFFIENTINI, *Il futuro della* privacy: *dall'*Internet of Things *ai* Big Data, in *Dir. prat. lav.*, 2015, *passim*; M. GIORGIANNI, *Il «nuovo» diritto della portabilità dei dati personali. Profili di diritto comparato*, in *Contr. impr*., 2019, p. 1387; M. MAGGIOLINO, *I big data e il diritto antitrust*, Milano, 2018; G. N. LA DIEGA, *Il* cloud computing: *alla ricerca del diritto perduto nel* web 3.0, in *Eur. dir. priv*., 2014, p. 577 ss.; M. OREFICE, *I big data e gli effetti su privacy, trasparenza e iniziativa economica*, Roma, 2018; V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, 2017; S. TROIANO, *Il diritto alla portabilità dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, p. 195 ss.; R.H. WEBER, *Data Portability and Big Data Analytics. New Competition Policy Challenges*, in *Conc. merc*., 2016, p. 23 ss. Si noti che un esplicito riferimento ai *big data* è contenuto, nell'ordinamento italiano, nel Decreto del Ministero dello Sviluppo Economico del 15 ottobre 2014 (nell'allegato n. 1, lett. A.5., "Tecnologie per la valorizzazione dei dati su modelli aperti e di grandi volumi - *Open Data and Big Data innovations*"), che prevede la concessione di agevolazioni per progetti di ricerca e sviluppo di rilevanti dimensioni in una serie di settori coerenti con la c.d. *Agenda digitale italiana*.

[57] Cfr. A. JAIN, *The 5 V's of big data,* in *IBM Big Data & Analytics Hub*; B. Marr, *Why only one of the 5 Vs of big data really matters*, *Ibidem*.

[58] Si veda R. MORO VISCONTI, *Valutazione dei* Big data, cit.

[59] Cfr. A. MANTELERO, Big data: *i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Dir. inf*., 2012, 1, p. 135 ss.

[60] Critica aspramente questo "programma-fedeltà", A. SORO, *La protezione dei dati nell'era digitale*, in *Nuova giur. civ. comm*., 2019, p. 344, segnalando che al fine di puntare "sulla deterrenza dello stigma sociale, in una regione cinese si è addirittura realizzato lo schermo 'della vergogna', su cui vengono proiettate le identità di indagati o di debitori insolventi".

[61] Così M. GAMBINI, *Algoritmi e sicurezza*, in *Giur. it.*, 2019, p. 1737. L'autrice evidenzia che "la diffusione dei trattamenti algoritmici non comporta solo la perdita di controllo sui dati personali, ma può influire anche su aspetti ulteriori, che superando il problema della riservatezza, investono la dignità umana, la libertà, l'autonomia e lo sviluppo delle persone, la sicurezza e la loro salute e implicare evidenti rischi di stigmatizzazione e discriminazione degli individui. Si pensi, alla portata di decisioni algoritmiche che impediscono ad un soggetto l'ingresso in uno Stato o l'accesso ad un sussidio o ancora all'erogazione di un servizio essenziale".

Da qui, l'esigenza di elaborare assetti normativi capaci di evitare che i *Big data*, utilizzati in processi basati sull'Intelligenza artificiale, possano diventare, per un verso, strumento di diffusione dell'odio o di gravi forme di discriminazione[62] e, per un altro, meccanismo di controllo delle reali volizioni dei soggetti monitorati[63].

Sotto il primo profilo, si potrebbero citare i tanti problemi che sta ponendo – e non riferimento a dati addirittura sensibili, non semplicemente personali – la neonata *App Immuni*[64], la quale non può assicurare in maniera assoluta la mancata identificazione (da parte di uno o più componenti della collettività) dei soggetti positivi al Covid-19. Se, in ipotesi, un individuo è uscito di casa nelle ultime settimane una sola volta, in occasione della quale è entrato in contatto unicamente con una persona, ricevendo la comunicazione relativa al pericolo di aver contratto il *virus*, non avrà grandi difficoltà a risalire all'identità del contagiato, con tutte le potenziali conseguenze negative che il legislatore avrebbe voluto neutralizzare (si pensi anche solo al possibile atteggiamento di diffidenza e di discriminazione verso l'infetto, e per un tempo indeterminabile, considerati anche i dubbi emersi tra gli stessi virologi circa l'esatta durata della contagiosità degli ammalati)[65].

Sotto il secondo, invece, va ricordato che, nel settore del *marketing* e delle *successful business practices*, da tempo si parla di una vera e propria "*sentiment analysis*"[66] (collegata al "*customer management*"[67]), ossia della possibilità di comprendere non soltanto il livello di gradimento del consumatore rispetto ad un bene (utile per capire, in ipotesi, se l'utente sta per cambiare gestore della telefonia mobile, per cui è il caso di adottare una strategia della persuasione, con un apprezzabile premio, ad esempio), ma addirittura il *mood* in generale e quindi la debolezza (con conseguente maggiore o minore disponibilità ad effettuare un certo tipo di acquisti) di un soggetto in un determinato momento (al rientro da un viaggio, magari, in base a quanto tempo sta su *Internet* e a quali siti visita, o al tipo di musica che ascolta su *youtube*). E tutto ciò non può che essere visto con diffidenza da chi ritiene addirittura che la stessa "personalizzazione dei prezzi"[68] (basata proprio su *Big data* che consentono all'impresa di conoscere una molteplicità di dati personali dei consumatori e, attraverso determinati algoritmi, di attuare forme di discriminazione nelle offerte commerciali agli *end users*), se realizzata da un'impresa in posizione dominante, potrebbe costituire una pratica abusiva[69]; né va, del resto, sottovalutato il rischio che anche altre norme a tutela della concorrenza siano lese, ed in particolare quelle relative al divieto di pratiche concordate (le quali si realizzerebbero, come si è fatto notare in dottrina, mediante la sostituzione del *meeting of algorithms* al vecchio *meeting of minds*)[70].

Servirà ricordare che uno dei più grandi scandali del nuovo millennio, di cui si è molto parlato sugli

---

[62] Sul tema, v. P. HACKER, *Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law*, in *Common Market Law Review*, 2018, p. 1143 ss. Interessante è l'esempio che E. BATTELLI, Big data *e algoritmi predittivi…,* cit., p. 1520, propone con riguardo al settore assicurativo, nel quale "la personalizzazione delle polizze e l'individuazione da parte delle imprese di assicurazioni di soggetti a più alto rischio potrebbe favorire i clienti 'migliori' da un punto di vista della rischiosità a discapito di quelli 'peggiori', erodendo in definitiva proprio il principio di mutualità su cui si basa l'attività assicurativa. Tale rischio potrebbe accentuarsi nelle ipotesi di assicurazione obbligatoria, come quelle da responsabilità civile automobilistica, o ancor di più in quella relativa all'attività medica o dell'avvocato. Se un algoritmo valutasse erroneamente il rischio di una attività o soggetto provocherebbe danni difficilmente emendabili. Lo stesso se ritenesse non assicurabile il contraente: questi si troverebbe inevitabilmente nella scelta di non porre in essere l'attività prevista o farla ma in contrasto a quanto previsto dalla legge. Ciò potrebbe tradursi, persino, in un ostacolo all'accesso al mercato del lavoro".

[63] Meritevoli di segnalazione sono i documenti di lavoro dell'OECD, sul tema "*Big data: Bringing competition policy to the digital era*", consultabili in *https://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm.*

[64] **V. D. BIANCHI, *APP IMMUNI E PRIVACY. SÌ DEL GARANTE MA OCCORRE INTERVENTO UMANO SULL'ALGORITMO*, IN *WWW.DIRITTOEGIUSTIZIA.IT*.**

[65] Il paradosso è che, in situazione come queste, a creare dei rischi per la *privacy* dei soggetti coinvolti, non sarebbe l'acquisizione di *Big data*, ma al contrario la *scarsity of data.*

[66] Sull'argomento, v. M. DELLA VOLPE, *Imprese tra web 2 0 e big data*, Padova, 2013, p. 103 ss.; E. FRONTONI, M. PAOLANTI, *AI-based decision support system: from theoretical background to real world applications*, in E. Calzolaio (a cura), cit., p. 9 ss.

[67] Cfr. T. SHIBATA, T. KURACHI, *Big Data Analysis Solutions for Driving Innovation in Onsite Decision Making*, in *Fujitsu Scientific & Technical Journal*, 2015, p. 33 ss.

[68] V., per tutti, L. PALADINO, *Intelligenza artificiale al servizio del* pricing, in *Economia & Management*, 2018, p. 57 ss.

[69] Sul tema, v. A. MINUTO RIZZO, *I profili* antitrust *del nuovo* web, cit., p. 118. Secondo l'autore, nonostante vi sia solitamente "una presunzione di non dannosità dei prezzi personalizzati, in quanto gli stessi possono determinare miglioramenti dell'efficienza allocativa sia dal punto di vista statico sia da quello dinamico", una loro applicazione "può determinare preoccupazioni concorrenziali per quelle autorità che adottano come standard valutativo il benessere dei consumatori".

[70] Ad evidenziarlo sono A. M. GAMBINO, M. MANZI, *Intelligenza Artificiale e tutela della concorrenza*, in *Giur. it.*, 2019, p. 1746. Secondo gli autori, "gli algoritmi, grazie alla loro capacità di influenzare qualsiasi condizione di mercato, favoriscono l'elevata trasparenza dei prezzi e la frequenza delle interazioni, condizioni strutturali necessarie che consentirebbero alle imprese di reagire in maniera rapida e precisa alle azioni dei concorrenti, contribuendo alla stabilità delle strategie collusive".

organi di stampa internazionale, ha riguardato la possibilità di una illegittima "invasione" nella *privacy* di persone, risultate vittime della formazione di "fascicoli" o "psicografie", elaborati attraverso l'analisi di dati raccolti, con l'intenzione di influenzare i risultati elettorali. Si tratta del noto caso *Cambridge Analytica*[71]: attraverso la raccolta di informazioni fornite volontariamente dagli utenti a fronte di domande apparentemente banali, è stato possibile mappare la personalità di milioni di ignari cittadini, individuando la comunicazione strategica migliore (basata su "messaggi personalizzati") per lo svolgimento di alcune campagne elettorali (come quella di Donald Trump o *pro Brexit*)[72].

Ma, problemi analoghi si sono posti con riferimento ai *Big data* adoperati per diagnosi mediche assolutamente approfondite, realizzate mediante il prezioso supporto dell'Intelligenza artificiale, che, però, se non ben governata potrebbe finire per ledere, oltre che la *privacy* dei pazienti, anche lo stesso diritto fondamentale alla dignità di questi ultimi. Ci sono, infatti, evidenti rischi che le informazioni raccolte vengano monitorate e analizzate per predire la reale aspettativa di vita degli interessati. E nulla esclude – secondo alcuni studiosi – che ciò finisca per incidere (più o meno indirettamente) sugli sforzi e sulle strategie terapeutiche dei medici e degli operatori sanitari, i quali potrebbero essere in sostanza indotti a non prestare la propria assistenza professionale con lo stesso "entusiasmo" (per non dire rigore) di prima[73].

Per non citare la possibilità che dall'eccessiva raccolta di dati della persona derivino attacchi informatici contro quest'ultima (una volta individuate le *password* delle *e-mail* o dell'*account* bancario attraverso gli "indizi" lasciati dalle persone nella navigazione in *Internet*) o che *software* di IA giungano a testare con una velocità inimmaginabile tutte le combinazioni numeriche sino ad individuare le "chiavi d'accesso" degli utenti.

Cosciente di tutto ciò è apparso il legislatore europeo, che – non a caso – nel GDPR ha posto dei ferrei limiti, tanto all'utilizzo di trattamenti interamente automatizzati, quanto alla portabilità dei dati[74].

E sia la Commissione europea che l'Autorità *antitrust* italiana sono intervenute in varie occasioni per sanzionare le richieste dei dati effettuate da alcune imprese in maniera non del tutto trasparente e leale[75]. Si pensi alle decisioni adottate in seno all'Unione nei confronti di *Google*[76] e *Facebook*[77] e a quelle prese, verso queste stesse società, dall'AGCM, a causa di una serie ripetute di violazioni del Codice del consumo italiano[78].

---

[71] Sul quale, cfr., per tutti, N. TIRINO, Cambridge Analytica. *Il potere segreto, la gestione del consenso e la fine della propaganda*, Lecce, 2019; F. FLORESTI, *Inteligência artificial entra no jogo da política. Mas isso é bom?*, in *https://revistagalileu.globo.com/Revista/noticia/2018/02/inteligencia-artificial-entra-no-jogo-da-politica-mas-isso-e-bom.html*; e P. PRZEMYSŁAW POLAŃSKI, *Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal*, in *Journal of European Consumer and Market Law*, 2018, p. 145 ss.

[72] V. E. GRAHAM-HARRISON, C. CADWALLADR, *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*, su *www.theguardian.com*; D. INGRAM, *Factbox: Who is Cambridge Analytica and what did it do?*, in *www.reuters.com*.

[73] Affronta questo problema, sottolineando quanto, nel campo della medicina, sia ancora centrale la sensibilità professionale, soprattutto nel processo decisionale, J. BROWN, *IBM Watson teria recomendado tratamentos contra câncer "inseguros e incorretos"*, in *https://gizmodo.uol.com.br/ibm-watson-saude-recomendacao-tratamentos-cancer-inseguros-incorretos*.

[74] Molto interessanti sono al riguardo le indicazioni fornite dal WP29 (Gruppo di Lavoro "Articolo 29"), nelle "*Guidelines on the right to data portability*", del 13 dicembre 2016. Nel documento si legge che, "*to prevent adverse effects on the third parties involved, the processing of such a directory by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs. A receiving 'new' data controller (to whom the data can be transmitted at the request of the user) may not use the transmitted third party data for his own purposes e.g. to propose marketing products and services to those other data subjects. Otherwise, such processing is likely to be unlawful and unfair, especially if the third parties concerned are not informed and cannot exercise their rights as data subjects*".

[75] L'Autorità garante della concorrenza e del mercato ha già avuto occasione di intervenire al riguardo: cfr. in particolare la decisione dell'11 maggio 2017, sulla quale v. G. CODIGLIONE, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "commercializzazione" della* privacy, in *Dir. inf. inform.*, 2017, 418 ss.

[76] La Commissione europea il 18 luglio 2018 ha condannato Google al pagamento di una multa particolarmente elevata (oltre 4 miliardi di euro), per una condotta volta a rafforzare la propria posizione dominante sul mercato (v. *http://europa.eu/rapid/press-release_IP-18-4581_it.pdf*), e poi nuovamente il 14 luglio 2016, per pratiche commerciali scorrette (cfr. *https://ec.europa.eu/commission/presscorner/detail/it/IP_19_1770*). V., inoltre, la decisione del 24 giugno 2017 (*https://ec.europa.eu/commission/presscorner/detail/it/IP_17_1784*), che ha inflitto un'ammenda pari a 2,42 miliardi di euro, per il vantaggio illegale conferito dalla società al proprio servizio di acquisti comparativi, realizzato mediante algoritmi progettati per eliminare la concorrenza sul mercato.

[77] V. la dura sanzione inflitta con la decisione della Commissione, 2017/C 286/06, del 18 maggio 2017, caso M. 8228 - *Facebook/WhatsApp*.

[78] Cfr., per tutti, il Provvedimento n. 27432 del 29 novembre 2018 ("PS11112 - Facebook Condivisione dati con terzi", in *www.agcm.it/dotcmsdoc/allegati-news/ps11112_scorr_sanz.pdf*) col quale l'Autorità Garante della Concorrenza e del Mercato ha constatato che Facebook non avrebbe fornito agli utenti una corretta informazione circa l'attività di raccolta dei loro dati con finalità commerciali e della trasmissione degli stessi in via automatica (in forza di una opzione preimpostata) a siti e applicazioni di terzi, sempre per attività di *marketing*. Ma, si veda anche la multa inflitta a

5. L'Intelligenza artificiale ed i nuovi orizzonti della responsabilità civile per violazione della *privacy*.

Lo sviluppo dei nuovi sistemi di *deep learning* sta, ovviamente, impegnando molto gli studiosi del diritto anche con riferimento all'individuazione delle norme da applicare in materia di responsabilità civile nel delicato settore in questione.

Quando l'illecito è realizzato da macchine controllate artificialmente, quali *robot* o droni, che possono mettere in pericolo la vita e l'integrità fisica delle persone, l'ordinamento giuridico dispone di un insieme di regole di diritto civile tutto sommato adeguato alla soluzione di questi problemi[79]. Si tratta, come è noto, delle norme in materia di responsabilità civile per fatto della cosa o del prodotto difettoso, a seconda del tipo di regime legale applicabile al rapporto giuridico di cui trattasi.

Problemi più delicati si pongono, viceversa, laddove i pregiudizi procurati ai privati siano realizzati da veicoli senza conducente: come si può leggere nel Libro bianco dello scorso 19 febbraio 2020, nel caso "delle auto a guida autonoma, può rivelarsi difficile provare che il prodotto è difettoso e dimostrare il danno cagionato e il nesso di causalità tra difetto e danno"[80].

Particolarmente complessa è anche la questione relativa all'individuazione del regime di responsabilità da adottare in presenza di danni provocati da *software* di Intelligenza artificiale, che violino, ad esempio, la riservatezza di milioni di utenti[81].

Nonostante l'Italia sia arrivata con estremo ritardo (rispetto ad altri Stati) all'adozione di una legge introduttiva del reato di *revenge porn*[82], sul piano dei rimedi civilistici già il vecchio art. 15 del c.d. Codice della *privacy* prevedeva che per i pregiudizi procurati dall'illecito trattamento dei dati personali si rispondesse ai sensi dell'art. 2050 c.c. (ossia come se si trattasse di attività pericolose). E

Samsung, con il *Provvedimento n. 26387 del 25 gennaio 2017 (www.agcm.it/dotcmsDOC/allegati-news/PS10207_chiusura.pdf)*, per aver, tra le altre cose, obbligato il consumatore a registrarsi alla piattaforma *online* predisposta dalla società, al fine di poter partecipare alle operazioni a premi indette dalla stessa, e a fornire così il proprio consenso al trattamento dei dati personali anche per finalità di *marketing*.

[79] V., per tutti, A. ALBANESE, *La responsabilità civile per i danni da circolazione di veicoli ad elevata automazione*, in *Eur. dir. priv.*, 2019, p. 995 ss.; A. SANTOSUOSSO, C. BOSCARATO e F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *Nuova giur. civ. comm.*, II, 2012, p. 494 ss.; E. PALMERINI, E. STRADELLA (a cura di), *Law and Technology. The Challenge of regulating technological development*, Pisa, 2013; U. RUFFOLO, E. AL MUREDEN, Autonomous vehicles *e responsabilita` nel nostro sistema ed in quello statunitense*, in *Giur. it.*, 2019, p. 1704 ss.; A. DAVOLA, R. PARDOLESI, *In viaggio con il robot: verso nuovi orizzonti della r.c. auto ("driveless")?*, in *Danno resp.*, 2017, p. 625 ss.; B. BROŻEK, M. JAKUBIEC, *On the legal responsibility of autonomous machines*, in *Artif Intell Law*, 2017, p. 293 ss. (*https://doi.org/10.1007/s10506-017-9207-8*); A. BERTOLINI, *Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules*, in *Law, innovation and technology*, 2013, p. 217 ss.; J. HAGE, *Theoretical foundations for the responsibility of autonomous agents*, in *Artif. Intell. Law*, 2017, p. 255 ss. (*https://doi.org/10.1007/s10506-017-9208-7*). Cfr., inoltre, la Risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica.

[80] Utili spunti di riflessione sono rinvenibili in G. VOTANO, *La responsabilità da circolazione stradale nella fase di transizione dai veicoli tradizionali alle auto a guida automatica*, in *Danno resp.*, 2019, p. 342. Secondo l'autore, i nuovi sistemi di mobilità intelligente comporteranno una radicale modifica del regime esistente in materia di responsabilità da circolazione stradale (basato sulla centralità del conducente), producendo una inesorabile obsolescenza delle norme sancite nei commi 1 e 3 dell'art. 2054 c.c. Molto più importante diventerà, viceversa, la figura del proprietario, il quale, però, ove si accerti che il sinistro sia dipeso da un difetto del *software* di guida automatica o da altro vizio di costruzione, "potrà traslare le conseguenze negative del sinistro sul produttore, avvalendosi della disciplina comune dettata a tutela del contraente contro i vizi della cosa che costituisce oggetto del contratto o della normativa in materia di illecito extracontrattuale (quando egli rivesta la qualifica di imprenditore), ovvero (quando rivesta la qualifica di consumatore) anche della normativa specificamente introdotta a tutela del consumatore contro i difetti del prodotto dalla Dir. 85/374/CEE". La posizione è in fondo simile a quella di A. DAVOLA, R. PARDOLESI, cit., p. 629, per i quali, occorrerebbe introdurre "un regime di responsabilità oggettiva limitata: sull'esempio di quanto avviene nel settore della responsabilità della struttura sanitaria per infezioni nosocomiali nell'ordinamento francese, coerentemente con il modello delineato dalla Loi Kouchner, in cui l'individuazione di un protocollo operativo *ex ante* permette di 'ancorare' l'imputazione di responsabilità – oggettiva – al mancato rispetto delle regole operative previste per l'attività condotta, demandandosi invece ad un fondo pubblico il ruolo di risorsa 'in via surrogata', destinata ad intervenire qualora la struttura sanitaria dimostri di essersi attenuta al protocollo, al fine di evitare che il costo del danno resti in capo alla vittima".

[81] Sul tema, cfr., per tutti, F. PIZZETTI, Privacy *e il diritto europeo alla protezione dei dati personali*, Torino, 2016, *passim*; E. BATTELLI, G. D'IPPOLITO, *Commento sub "Art. 35 – Valutazione d'impatto sulla protezione dei dati"*, in A. BARBA, S. PAGLIANTINI (a cura di), *Commentario del Codice Civile - Delle Persone, Leggi Collegate vol. II "Regolamento Parlamento Europeo 27 aprile 2016, n. 2016/679/UE*, Torino, 2019, p. 661 ss.; U. RUFFOLO (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2018; G. D'ACQUISTO, M. NALDI, Big Data *e* Privacy by design, Torino, 2017; F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018; A. CICCIA MESSINA, N. BERNARDI, Privacy *e Regolamento Europeo*, Assago, 2016, p. 41 ss.

[82] Si tratta, come è noto, della Legge n. 69 del 19 luglio 2019, che ha aggiunto l'art. 612-ter nel codice penale italiano.

l'attuale disciplina, derivante dalle regole del GDPR, non pare si discosti molto da una simile impostazione (rispetto alla quale si è già avuto modo di criticare, viceversa, l'orientamento restrittivo della Corte di Cassazione, secondo cui – anche in questi casi – i danni di natura non patrimoniale di modesta entità devono essere sopportati, in forza di un non meglio precisato dovere di solidarietà verso l'offensore[83]).

In base a quanto previsto dall'art. 24 del Regolamento n. 679/2016, presi in considerazione vari fattori (come la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché i possibili rischi, con le loro differenti probabilità e gravità, di possibili violazioni dei diritti e delle libertà delle persone fisiche), il titolare del trattamento è tenuto a predisporre "misure tecniche e organizzative" (all'occorrenza, riesaminate ed aggiornate) "adeguate per garantire, ed essere in grado di dimostrare", che il trattamento è conforme al GDPR[84].

La disposizione successiva ha introdotto, invece, i noti concetti di *data protection by design*[85] e *by default*[86], che avrebbero elaborato una sorta di "responsabilità da algoritmo" (come si è suggestivamente indicato in dottrina)[87].

La prima delle due regole ha l'obiettivo di far nascere in capo al titolare l'obbligo di provvedere, sin dalla fase di programmazione di un determinato trattamento, alla elaborazione di misure tecniche e organizzative adeguate (come la pseudonomizzazione), al fine di garantire il rispetto dei principi in materia di protezione dei dati (quali la minimizzazione, come precisa l'art. 25 del GDPR) e la tutela dei diritti degli interessati; il tutto, ovviamente, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento"[88]. E ciò, chiaramente, implicherà una meticolosa valutazione dei requisiti effettivi del sistema, legata anche alla selezione del numero e tipo di dati inseriti in sede di creazione del *software*, alla formazione iniziale della macchina, e/o alla scelta di un modello piuttosto che di un altro.

La seconda mira, viceversa, a favorire l'adozione di strumenti idonei ad assicurare che, in base ad una impostazione predefinita, siano trattati "solo i dati personali necessari per ogni specifica finalità del trattamento" ed essi non siano automaticamente resi accessibili "a un numero indefinito di persone fisiche". Il secondo comma dell'art. 25 si preoccupa di chiarire che "tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità"[89].

La Risoluzione del Parlamento europeo del 12 febbraio 2019 ha ribadito l'importanza del rispetto di questi due doveri, invitando la Commissione ad assicurare, tra le tante altre cose, che "qualsiasi futuro quadro normativo dell'Unione europea in materia di Intelligenza artificiale garantisca [...] la

---

[83] Sia consentito rinviare sul tema ad A. VIGLIANISI FERRARO, *Danno da illegittimo trattamento dei dati personali, tra "inasprimento sanzionatorio" europeo ed "interpretazioni restrittive" della giurisprudenza italiana*, in *Riv. dir. priv.*, 2020, p. 85 ss.

[84] Secondo una studiosa, emergerebbe da questa disposizione un principio di *accountability*, termine che "può essere tradotto con responsabilità e, insieme, prova della responsabilità" e "comporta, pertanto, che sia il titolare del trattamento a determinare le misure di sicurezza adeguate al trattamento dei dati personali che effettua, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (e ciò anche in base a quanto previsto dall'art. 32 del GDPR). A sostenerlo è G. Finocchiaro, cit., p. 1676, segnalando che il titolare del trattamento ha "l'onere di individuare in che modo adempiere alle prescrizioni dettate dalla norma, calandole nella fattispecie concreta, assumendosi la responsabilità non solo dell'implementazione, ma anche della valutazione [...] fra il legittimo interesse al trattamento e gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali".

[85] L'espressione parrebbe essere stata coniata dal Commissario dell'Autorità Garante canadese della provincia dell'Ontario, nel 2009, nel documento "*Privacy by design, the 7 fundamental principles*", in *www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf*. Sul tema, v. F. PIRAINO, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuova giur. civ. comm.*, 2017, p. 388.

[86] Nel più volte menzionato testo dell'OCSE, *Artificial Intelligence in Society*, p. 88, viene ben evidenziato che "*AI systems around principles of privacy by design and privacy by default are ongoing within a number of technical standards organisations. For the most part, they use and adapt privacy guidelines, including the OECD Privacy Guidelines. Additionally, AI is used to offer individuals tailored personalised services based on their personal privacy preferences, as learned over time* [...]. *These services can help individuals navigate between the different personal data processing policies of different services and ensure their preferences are considered across the board. In so doing, AI empowers meaningful consent and individual participation. A team of researchers, for example, developed Polisis, an automated framework that uses neural network classifiers to analyse privacy policies*".

[87] L'espressione è di U. RUFFOLO, *Intelligenza Artificiale*, machine learning *e responsabilità da algoritmo*, in *Giur. it.*, 2019, p. 1692.

[88] Così sempre nel primo paragrafo della disposizione citata. Cfr. M. GAMBINI, *Algoritmi e sicurezza*, cit., p. 1726 ss.

[89] Sull'argomento, v., per tutti, A. MANTELERO, *Responsabilità e rischio nel Regolamento UE n. 2016/679*, in *Nuova giur. civ. comm.*, 2017, p. 144 ss.; e M. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, Napoli, 2018.

protezione dei dati fin dalla progettazione e per impostazione predefinita".

Il problema serio riguarda la possibilità che le violazioni dei diritti in questione, quello alla *privacy* in particolare (ma, non solo), vengano realizzate da "sistemi intelligenti capaci di apprendere dall'esperienza, programmati per 'crescere' e decidere autonomamente la condotta da tenere nelle diverse situazioni che si trovano a fronteggiare, anche *bypassando* e sfuggendo al controllo di colui che li progetta, li programma e/o li costruisce"[90].

Non è del tutto chiaro chi sarà chiamato a rispondere dei danni in questi casi[91].

La dottrina si sta interrogando sulla possibilità di invocare, anche in tali ipotesi, in base all'art. 12 delle disposizioni preliminari al codice civile, le norme in materia di responsabilità per cosa in custodia (*ex* art. 2051 c.c.)[92], oppure ancora – dando credito ad una particolare impostazione di origine germanica che immagina la configurabilità di una sorta di "personalità elettronica" e di "oggettivazione dell'illecito" – per fatto altrui, ed in particolare, dei propri commessi (che rileverebbero quali "dipendenti digitali"), ai sensi dell'art. 2049 c.c.[93].

E non è mancato chi, rilevando come "in presenza di A.I. dotata di capacità di autoapprendimento ma priva di idonei meccanismi inibitori di comportamenti malevoli o devianti si pone [...] oltre al problema dell'eventuale responsabilità sia del suo produttore che dell'ideatore dell'algoritmo, anche quello delle responsabilità quantomeno concorrenti di chi addestra o comunque espone il bene intelligente ad esperienze idonee ad istruirlo o indirizzarlo"[94], ha escluso che si possa ricorrere – sia pur solo analogicamente – alle norme contenute negli artt. 2047 e 2048 (o, addirittura nell'art. 2052[95]) del codice civile e ha ritenuto più utile immaginare applicabile il regime di responsabilità per "attività pericolosa atipica"[96] (secondo il citato art. 2050 c.c.)[97].

La tesi che porta a preferire la stessa soluzione adottata dal vecchio Codice della *privacy* per i danni da non corretto utilizzo dei dati personali (e che concorrerebbe in Italia, nel settore in questione, con quella da prodotto difettoso[98]) potrebbe essere la più convincente, ma non si può trascurare di considerare che recentemente la Corte di Cassazione ha negato la risarcibilità del danno da

[90] N.F. FRATTARI, cit., p. 462.

[91] U. RUFFOLO, *Intelligenza Artificiale,* machine learning…, cit., p. 1692. L'autore, partendo proprio dalla constatazione che l'"A.I. self-learning, evolvendo con l'autoapprendimento, e dunque con l''esperienza', possa radicalmente mutare attitudini o comportamenti in direzioni non sempre immaginate da chi la ha generata", e che "la fallibilità dell'A.I. può, inoltre, essere anche frutto di *bias* imputabili all''addestramento' direttamente o indirettamente ricevuto", si chiede se "a fronte di potenziali fenomeni di distorsione del funzionamento dell'A.I., occorre deresponsabilizzare il suo 'produttore' ed il suo 'custode', corrispondentemente responsabilizzando invece chi la 'addestra', o chi comunque la impiega accompagnandola nel processo di autoapprendimento" o se, invece, "la responsabilità di quest'ultimo soggetto deve cumularsi a quella dei primi". Sul tema, si veda anche G. CAPILLI, *Responsabilità e robot,* in *Nuova giur. civ. comm.*, 2019, p. 621 ss.

[92] M. COSTANZA, *L'Intelligenza Artificiale e gli stilemi della responsabilità civile*, in *Giur. it.*, 2019, p. 1687, evidenzia che "la cosa, nel disegno dell'art. 2051 c.c., è entità lontana dalla A.I., se essa si identifica con l'agente munito in sè di motilità e di operatività, che pur predisposte o programmate non rimandano alle ragioni sottese alla responsabilità del custode. Se alla intelligenza artificiale fosse affidato compito inappropriato o se di essa si facesse un uso diverso o non adeguato, la causa efficiente tornerebbe ad essere un diretto fattore umano e la norma di riferimento non potrebbe che essere quella prevista dalla clausola generale".

[93] Ma, in effetti, anche la regola del *cuius commoda cuius et incommoda* non sembra praticabile in questo caso, se non si vuole davvero arrivare ad equiparare la macchina all'essere umano. Come osserva ancora M. Costanza, cit., p. 1688, "il fatto illecito del sottoposto implica la sua imputabilità c.d. soggettiva. L'A.I. in quanto ente non equiparabile al soggetto munito della necessaria capacità non sarebbe equiparabile all'autore dell'illecito compiuto nell'ambito delle mansioni affidategli". Anche secondo U. RUFFOLO, *Intelligenza Artificiale,* machine learning…, cit., p. 1698, "potrebbe non essere congruo, allora, estendere la *eadem dispositio* ad entità non umane, insuscettibili di compiere 'illeciti' e di agire con dolo o colpa. Non si dimentichi, poi, che il committente risponde non per qualsiasi danno cagionato dal commesso, ma solo di quello che consegue ad un 'fatto illecito' dal medesimo posto in essere".

[94] Così U. RUFFOLO, *Intelligenza Artificiale, machine learning*, cit., p. 1697.

[95] Sul tema, si veda G. TEUBNER, *Soggetti giuridici digitali? Sullo* status *privatistico degli agenti* software *autonomi*, a cura di P. Femia, Napoli, 2019.

[96] Ossia, attività che, "per la loro spiccata potenzialità offensiva, implicano un'elevata possibilità di recar danno a terzi [...] (v. Cass. 15 febbraio 2019, n. 4545; Cass. 19 luglio 2018, n. 19180)". Così *A.* TORRENTE, P. SCHLESINGER, *Manuale di diritto privato*, a cura di F. ANELLI e C. GRANELLI, Milano, 2019, p. 909.

[97] M. COSTANZA, cit., p. 1688, segnala, invece, che "le perfezioni che s'attribuiscono all'A.I. stridono con la qualificazione di pericolose. Esiste tuttavia un limite negativo della perfezione: il riconoscimento delle imperfezioni, delle anomalie della realtà, di quelle zone d'ombra che esulano dai paradigmi conosciuti e riconoscibili dalla intelligenza artificiale [...]. Queste lacune possono dipendere da difettosità genetiche di impostazione, che soltanto se ascrivibili ad una incompetenza varrebbero quale ragione d'imputazione di responsabilità. In assenza di presupposti per la rilevazione di colpe, scatterebbe il regime delle esenzioni. L'ipotesi d'una zona franca non è esclusa dalla legislazione. Anche là dove la riparazione del danno si propone come fine da perseguire in modo non debole, uno spazio per sottrarsi alle responsabilità permane, pur con qualche strettoia. Il prodotto difettoso o insicuro, ma allineato allo stato delle conoscenze tecnico-scientifiche non espone il fabbricante a responsabilità".

[98] Cfr. G. CAPILLI, cit., p. 628.

fumo di sigarette, "in applicazione del principio della causa prossima di rilievo costituito, nel caso di specie, da un atto di volizione libero, consapevole ed autonomo di un soggetto dotato di capacità di agire: la scelta di fumare nonostante la notoria nocività del fumo"[99]. Presa di posizione forse criticabile, perché rende ancora più discrezionale il ruolo del giudice nella scelta di quali siano le "attività pericolose note come tali" (che, sfuggono al regime di *favor* per il danneggiato previsto dall'art. 2050 c.c.), e quali le attività per così dire "non notoriamente pericolose" (soggette allo statuto speciale)[100].

Anche alla luce di questo orientamento giurisprudenziale, andrebbe forse immaginato un differente regime di responsabilità, a seconda che il danno sia provocato a chi fruisce della *smart machine* o a terzi.

A giocare un ruolo centrale sarebbe, comunque, il "consenso informato"[101], perché dimostrerebbe l'accettazione del rischio: ma, il problema riguarderebbe a questo punto la disciplina delle modalità concrete attraverso le quali documentare la mancata o inesatta informazione fornita al cliente circa i pericoli legati all'utilizzo dei sistemi di *deep learning* (su chi graverebbe l'*onus probandi*? E come si potrebbe dimostrare di aver fornito le informazioni adeguate – oltre che comprensibili da tutti –, posto che spesso i rischi derivanti dallo strumento di IA potrebbero essere addirittura poco conosciuti o poco conoscibili anche per lo stesso creatore, oltre che *a fortiori*, per chi lo vende? Si aprirà una nuova stagione per il neoformalismo contrattuale[102], nonostante possa sembrare un controsenso nell'era delle nuove tecnologie[103]?).

Teoricamente, si potrebbero forse configurare quattro ipotesi teoriche, nel caso di illecito da non corretto utilizzo di apparecchiature o *software* intelligenti: 1) danni provocati da un sistema automatico, non dotato di *self-learning*, in presenza di un'adeguata informazione fornita all'utente sui rischi legati al suo utilizzo; 2) danni provocati da un sistema automatico, non dotato di *self-learning*, in assenza di un'adeguata informazione; 3) danni provocati da un sistema dotato di *self-learning*, in presenza di un'adeguata informazione; 4) danni provocati da sistemi dotati di *self-learning*, in assenza di un'adeguata informazione.

Nel primo caso, stando all'impostazione proposta dal Supremo Collegio con riguardo al danno da fumo, non si potrebbe probabilmente invocare il regime speciale di cui all'art. 2050 c.c., ma andrebbe applicata la regola ordinaria di cui all'art. 2043 c.c. (in quanto, i rischi erano chiari e l'utente li ha voluti correre). Nel secondo e quarto caso, invece, sì, a meno che il professionista non riesca a dimostrare che anche in presenza di una corretta informazione l'utente avrebbe comunque accettato di correre il rischio (qualsiasi rischio, anche non prevedibile, nell'ipotesi di sistema dotato di *deep learning*). Più complessa è la situazione con riferimento alla terza ipotesi. Perché l'informazione che è stata fornita potrebbe risultare inevitabilmente vaga, non potendo concretamente tenere conto di cosa accadrà, in quanto neanche il produttore lo può immaginare. Dovrebbe, quindi, operare una sorta di esimente simile a quella legata al c.d. rischio da sviluppo (già noto all'utente, che lo ha comunque accettato). A meno che il danneggiato non riesca a dimostrare che nella realizzazione del pregiudizio c'è un concorso di colpa del produttore (il quale è, ad esempio, intervenuto durante lo svolgimento del

[99] Così nella sentenza n. 11272 del 10 maggio 2018, in *Danno resp.*, 2018, p. 589 ss., con nota di M. TOPI, *La Cassazione torna sui danni da fumo attivo.* Il Supremo Collegio è qui perfino più *tranchant* rispetto alla posizione assunta con la pronuncia n. 26516 del 17 dicembre 2009 (con i commenti di G. PONZANELLI, *I danni da fumo: la nuova giurisprudenza milanese*, in *Danno resp.*, 2014, p. 1361 ss.; ID., *La produzione di sigarette è attività pericolosa*, in *Danno Resp.*, 2010, p. 569; P.G. MONATERI, *La Cassazione e i danni dal fumo: evitare un ennesimo ''isolamento'' italiano*, in *Corr. giur.*, 2010, p. 488 ss.). In quella occasione, infatti, aveva negato il risarcimento del danno da fumo di sigarette definite "*light*", segnalando che non si può configurare alcuna responsabilità in capo al professionista, se il consumatore non riesca a provare "l'esistenza del danno, il nesso di causalità tra pubblicità e danno, nonché (almeno) la colpa di chi ha diffuso la pubblicità, concretandosi essa nella prevedibilità che dalla diffusione di un determinato messaggio sarebbero derivate le sanzionate conseguenze dannose".

[100] Si consideri, per converso, che nell'applicare l'art. 2050 c.c., il Giudice di legittimità sta negli ultimi anni seguendo un orientamento di particolare *favor* verso il soggetto leso: all'offensore è stato infatti chiesto, non soltanto di dimostrare "di aver adottato tutte le misure idonee per evitare il danno", ma addirittura di fornire "la prova *positiva* della *causa esterna* (fatto naturale, fatto del terzo, fatto dello stesso danneggiato) che, per imprevedibilità, eccezionalità ed inevitabilità, sfugge completamente alla sfera di controllo dell'esercente l'attività pericolosa" [...] ed è "*idonea ad interrompere il nesso causale* tra quest'ultima e l'evento dannoso sofferto dalla vittima". Così *A.* TORRENTE, P. SCHLESINGER, *cit.*, p. 909, rinviando alle pronunce della Corte di Cassazione n. 27544 del 21 novembre 2017, e n. 24549 del 30 ottobre 2013.

[101] L'informazione avrebbe, forse, in questa materia un'importanza maggiore rispetto a quella che ha sempre avuto nel settore della responsabilità del produttore *tout court* (sulla quale si veda G. PONZANELLI, *Responsabilità oggettiva del produttore e difetto di informazione*, in *Danno resp.*, 2003, p. 1006 ss.

[102] Sul collegamento tra forma e responsabilizzazione del consenso, cfr. C.M. BIANCA, *Diritto civile, Vol. III, Il contratto*, Milano, 2000, p. 278 ss.

[103] Come già 20 anni fa rilevava P. RESCIGNO, *Trasparenza bancaria e diritto comune dei contratti*, in *Banca borsa tit. cred.*, 1999, p. 305.

servizio o dell'attività, modificando le impostazioni del *software*, senza avere l'assenso dell'utente).

Dubbi altrettanto spinosi ha, del resto, posto la questione relativa alla possibilità di applicare anche in questo settore la norma "eccentrica"[104] sancita nell'art. 122, comma 2, del codice del consumo, che esclude l'obbligo risarcitorio "quando il danneggiato sia stato consapevole del difetto del prodotto e del pericolo che ne derivava e nondimeno vi si sia volontariamente esposto"[105].

Secondo una studiosa, occorrerebbe, viceversa, "superare il paradigma basato sull'errore e sulla colpa e [...] affrontare il problema sotto il profilo dell'allocazione del rischio", poiché "non è rilevante chi sbagli e la ricerca dell'errore è attività costosa e dispendiosa che può essere superata", e andrebbero introdotti "meccanismi di allocazione del costo del danno cagionato su quei soggetti che astrattamente potrebbero essere responsabili, ad esempio mediante la costituzione di un fondo al quale attingere, prescindendo dall'individuazione delle modalità dell'incidente o dell'errore", proprio come si fa "nel circuito delle carte di credito, per il caso di clonazione o furto"[106].

Bisognerebbe, invero, riflettere meglio su questa soluzione, perché potrebbe produrre un doppio inconveniente e, da un lato, frenare la creazione di sistemi dotati di sempre maggiori capacità di *deep learning* (con i vantaggi che hanno per la collettività) e, dall'altro, favorire forse eccessivamente la posizione del danneggiato (che non sarebbe incoraggiato ad impegnarsi per evitare il sorgere o l'espandersi del pregiudizio).

Sembra, invece, condivisibile la tesi di chi – sia pur con riferimento ad uno specifico settore applicativo dell'IA – ha immaginato che un fondo di garanzia (pubblico, però) debba essere attivato (solo) a copertura dei danni derivanti dal caso fortuito: un tale sistema di responsabilità garantirebbe effettivamente un adeguato contemperamento dei diversi interessi coinvolti[107].

6. Considerazioni conclusive. La necessità di un intervento normativo europeo.

È, invero, auspicabile che, come già accaduto per il danno da illecito *antitrust* o da prodotto difettoso, ovvero ancora da violazione della *privacy tout court*, sia l'Unione europea ad intervenire tempestivamente per fissare delle linee-guida il più possibile precise[108].

In questo settore, infatti, appare quanto mai fondamentale che vi sia una uniformazione delle discipline. E realizzare tale obiettivo, prima che siano gli Stati ad operare delle scelte concrete (diventando poi più o meno gelosi sostenitori delle proprie decisioni), renderebbe sicuramente meno complicata un'operazione di – indefettibile – convergenza normativa[109].

L'esistenza di un Libro bianco in materia rappresenta un buon punto di partenza in tale direzione.

Come è stato rilevato da più parti, una normativa simile a quella adottata in materia di responsabilità per "prodotto" difettoso (opportunamente estesa al "servizio") parrebbe essere la soluzione migliore, tenendo conto che i danni potrebbero essere ascrivibili alla condotta di una pluralità di soggetti: non solo di colui "che crea il *software* o l'algoritmo, oppure a colui che lo configura o che lo custodisce", bensì anche di quanti "hanno contribuito alla realizzazione del prodotto dotati di intelligenza artificiale e, quindi, il progettista dell'algoritmo, l'editore del *software*, il proprietario del database, l'assemblatore/produttore, il fornitore di rete, in alcuni casi il proprietario o l'utente"[110].

---

[104] A. ALBANESE, cit., p. 1029.

[105] Per una posizione assolutamente critica nei confronti di questa disposizione, cfr. C. CASTRONOVO, *La nuova responsabilità civile*, Milano, 2006, p. 724.

[106] Ad asserirlo è G. FINOCCHIARO, cit., p. 1676. Secondo l'autrice, "uno degli obiettivi perseguiti con questo tipo di sistema di allocazione del rischio è immediatamente evidente ed è quello di rassicurare i potenziali utilizzatori sul fatto che, a prescindere dagli esiti di una costosa ricerca sull'errore, otterranno un risarcimento".

[107] Si veda G. VOTANO, cit., p. 342. Un assetto normativo di tal fatta garantirebbe molteplici benefici. Anzitutto, le imprese, essendo tenute a rispondere esclusivamente dei danni causati da vizi dei loro prodotti, sarebbero indotte ad aumentare il livello di sicurezza dei beni stessi. La conseguente limitazione del rischio economico legato ai pregiudizi in questione assicurerebbe nuovi investimenti nel settore della guida automatica. Inoltre, questo sistema consentirebbe di non addossare interamente al proprietario del veicolo i rischi connessi alle nuove tecnologie di trasporto. Infatti, la responsabilità del proprietario sussisterebbe soltanto in relazione ai danni causati dalla sua negligenza (per omessa manutenzione della macchina). Infine, i terzi danneggiati avrebbero la sicurezza di ottenere il risarcimento del danno subito, gravando detta obbligazione risarcitoria o sul proprietario o sul produttore ovvero su quella stessa collettività che gode dei vantaggi assicurati dalle nuove tecnologie.

[108] La pensa così anche A. ALBANESE, cit., p. 1023 ss.

[109] Sia consentito rinviare, sull'argomento, a E. TOMASEVICIUS FILHO, A. VIGLIANISI FERRARO, *Le nuove sfide dell'umanità e del diritto nell'era dell'Intelligenza artificiale*, in *Direitos culturais*, 2020, p. 401 ss.

[110] Così G. CAPILLI, cit., p. 628. L'autrice evidenzia che "porre a carico solo dei produttori il costo derivante da possibili danni causati da robot intelligenti potrebbe avere conseguenze in termini di aggravio di costi per i consumatori e utenti ed in termini di un disincentivo per la produzione e diffusione di robot sempre più complessi", ecco perché alcuni studiosi "hanno prospettato una soluzione di compromesso – che allo stato dell'arte potrebbe essere meritevole di accoglimento – in

Si consideri, però, che la stessa Commissione europea nel testo dello scorso 19 febbraio 2020 ha segnalato una serie di limiti che tale disciplina – un po' datata – presenta, se riferita all'Intelligenza artificiale: ad esempio, "non è chiaro come e in che misura si applichi la direttiva sulla responsabilità per danno da prodotti difettosi nel caso di alcuni tipi di difetti, ad esempio per quelli risultanti da carenze della cibersicurezza del prodotto"[111].

Per concludere, è bene evidenziare che quanto segnalato anni fa in dottrina, circa una intelligenza solo presunta o teorica dei *computer* – poiché questi ultimi avrebbero "la capacità di trattare con precisione problemi ben definiti e sono molto abili nello svolgere questa funzione, ma sono del tutto inadatti ad affrontare situazioni non previste (dal programmatore)"[112] –, nel giro di tre lustri sembra messo in discussione da chi sostiene la necessità di iniziare a confrontarsi, semmai, con macchine sempre più dotate della c.d. "Intelligenza Artificiale Forte" (ossia del potere di ragionare in maniera estesa, proprio come un essere umano)[113].

Anzi, alcuni studiosi immaginano che agenti evoluti e sempre più sofisticati potranno presto rivelarsi addirittura dotati di una super-intelligenza in grado di battere completamente quella umana in ogni settore[114]. Per cui, non occorrerà più ricorrere – ad esempio – a *test* come quelli effettuati da alcune aziende cinesi, per analizzare – attraverso sensori intelligenti inseriti in appositi caschi ("*neuro-cap*") – gli impulsi nervosi dei lavoratori, "desumendo così lo stato emotivo del soggetto e, quindi, la sua eventuale inidoneità a svolgere certe mansioni"[115]: una serie di macchine, instancabili e tendenzialmente indistruttibili, incapaci di ammalarsi e di provare emozioni (come paura, stress, sfiducia), e disponibili h24 per 365 giorni l'anno (senza mai pensare di scioperare o andare in maternità), sostituiranno direttamente gli uomini.

È ora che di tutto questo prenda coscienza anche il diritto, ed intervenga, nel tentativo di non arrivare *more solito* a disciplinare alcuni fenomeni (in continuo mutamento), con eccessivo (e colpevole) ritardo.

Come è stato correttamente sottolineato in tempi non sospetti da un grande giurista italiano, in passato "i confini dell'azione umana erano segnati da leggi naturali che escludevano o limitavano fortemente la possibilità di decisioni autonome. Oggi molti di quei confini sono stati cancellati [...] e si invocano leggi giuridiche in grado di fissare quei limiti che le leggi naturali non sono più in grado di indicare"[116].

---

cui il regime di responsabilità oggettiva sia mitigato dalla previsione di un sistema indennitario che intervenga in tutti i casi in cui sia dimostrato che il produttore abbia adottato tutte le misure necessarie per l'immissione sul mercato di un robot sicuro".

[111] Cfr., per ulteriori approfondimenti, la "Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità", che accompagna proprio il Libro bianco del 2020 e che "analizza il quadro giuridico pertinente, individuando le incertezze riguardanti l'applicazione di tale quadro giuridico in relazione ai rischi specifici derivanti dai sistemi di IA e da altre tecnologie digitali". Secondo la Commissione, "la legislazione vigente in materia di sicurezza dei prodotti sostiene già un concetto ampio di sicurezza, con l'obiettivo di proteggere da tutti i tipi di rischi derivanti dal prodotto in funzione dell'uso dello stesso", ma "per garantire una maggiore certezza del diritto si potrebbero tuttavia introdurre disposizioni che contemplino esplicitamente i nuovi rischi derivanti dalle tecnologie digitali emergenti".

[112] Così R.M. DI GIORGI, *L'intelligenza artificiale: teoria e applicazioni nel diritto*, in R. BORRUSO, R.M. DI GIORGI, L. MATTIOLI, M. RAGONA, *L'informatica del diritto*, Milano, 2004, p. 188.

[113] Idea sviluppatasi dagli anni Cinquanta agli anni Ottanta e poi abbandonata, per dare spazio a quella di una *Light AI* (la quale, in base ad "un approccio sostanzialmente funzionalista, [...] tende, semmai, a emulare solo alcune funzioni del cervello umano e porta a creare macchine che riescono a svolgerle, talora anche meglio degli umani", come ricordano A. Santosuosso, C. BOSCARATO, F. CAROLEO, cit., 2012, p. 494), ma che oggi sta tornando, invece, alla ribalta con prepotenza. Cfr., al riguardo, N. BOSTROM, *Superintelligenza – Tendenze, pericoli, strategie*, Torino, 2018 e U. RUFFOLO, A. AMIDEI, cit., *passim.*

[114] N. BOSTROM, *Superintelligence: Paths, Dangers, Strategies*, Oxford, 2014. Ma, vedi già J. HABERMAS, *The future of Human Nature*, Cambridge, 2003.

[115] A segnalarlo è A. SORO, cit., p. 344. Il Garante parla a tal proposito di una "postmodernità che ripropone l'uomo-automa, rappresentando una minaccia quando invece aveva promesso speranza" e sottolinea che "in questa regressione neo-fordista, la tecnica che avrebbe dovuto liberare l'uomo dal peso e dall'alienazione della catena di montaggio rischia invece di costringerlo in nuove catene elettroniche, riducendolo a mero ingranaggio".

[116] S. RODOTÀ, *La vita e le regole: tra diritto e non diritto*, Milano, 2006, p. 174.