Intelligenza artificiale e ruolo della protezione dei dati personali. L’analisi di Ginevra Cerrina Feroni (Garante Privacy)

Intelligenza artificiale e ruolo della protezione dei dati personali. L’analisi di Ginevra Cerrina Feroni (Garante Privacy)
Intervento di Ginevra Cerrina Feroni, vice Presidente del Garante per la protezione dei dati personali
(AKey4biz, 14 febbraio 2023)

Il rapporto tra intelligenza artificiale e protezione dei dati personali è un tema enorme solo considerati i differenti profili che abbraccia: tecnico, normativo, etico[1]. L’intelligenza artificiale, del resto, non è solo una sfida infrastrutturale, ma anche antropologica e filosofica: «è un mezzo, ma anche un mondo»[2]. Nel presente contributo si intende affrontare il tema dell’intelligenza artificiale con riferimento ai più significativi aspetti, contenutistici e organizzativi, che riguardano ruolo e prospettive dell’Autorità di protezione dei dati personali.

Come è noto, con il passaggio dalla società digitale alla società algoritmica, l’intelligenza artificiale è divenuto uno strumento sempre più utilizzato a supporto della funzione gestoria, della definizione degli indirizzi strategici privati e pubblici e del controllo sull’attività amministrativa.

In questo contesto il ruolo del Garante privacy nella tutela dei diritti digitali a fronte di trattamenti automatizzati dei dati personali è stato sempre di primo piano, anche quando il tema non era ancora diventato, per così dire, da grande pubblico.

La giurisprudenza dell’Autorità è, in questa prospettiva, la prova di tale “presenza” a presidio dei diritti fondamentali in settori svariati.

Sin dai primi tentativi di applicazione delle tecnologie d’intelligenza artificiale ai trattamenti di dati personali, il Garante ha compreso il rischio rappresentato dall’esposizione delle persone fisiche (e delle loro vite) a processi di decisione automatizzata basati sulla lettura e l’elaborazione algoritmica di dati, ma anche di meta-dati. Già nella vigenza del Codice pre-novella del 2018 il Garante si era espresso su trattamenti di analisi comportamentale degli utenti di siti commerciali in base alle loro modalità di navigazione online, così come aveva bocciato un sistema di rating reputazionale che, attraverso un processo di data scraping in Rete, attribuiva punteggi e stilava classifiche dei soggetti interessati[3]. Come pure aveva vietato un sistema di lettura biometrica che, montato su totem pubblicitari, registrava sesso, range di età, distanza dal monitor e tempo di permanenza dinanzi ad esso dei passanti che s’imbattevano o s’intrattenevano a guardare uno degli spot proiettati, in modo da calcolare la fascia d’età, il sesso, il grado di attenzione e persino la stima dell’espressione facciale mostrata da differenti target commerciali rispetto ai vari prodotti pubblicizzati[4].

Di fatto il Garante stava già consacrando il principio che di lì a poco sarebbe stato enunciato a chiare lettere dall’art. 22 del GDPR, ovvero il diritto dell’interessato a non essere soggetto ad una decisione basata unicamente su di un trattamento automatizzato, compresa la profilazione, che abbia il potere di produrre effetti giuridicamente rilevanti o, comunque, parimenti significativi sulla

sua sfera di vita (si pensi alla concessione di un mutuo, alla definizione di una polizza assicurativa, ad una diagnosi clinica).

Il Garante vigila sulla tutela dei diritti e delle libertà dei cittadini anche quando il titolare del trattamento che ricorre all'utilizzo dell'AI sia un soggetto pubblico. Si pensi ai pareri resi sul c.d. Redditometro, alle sperimentazioni di incrocio di banche dati tributarie a fini anti-evasione[5], alla sanzione comminata per l'utilizzo da parte dell'INPS di un software di data mining al fine di attribuire uno score di credibilità al certificato medico presentato dal lavoratore[6].

La pandemia ha senz'altro incrementato l'impegno dell'Autorità su questo fronte, con l'obiettivo di evitare una proliferazione senza criterio di sistemi di analisi intelligente dei dati sanitari dei cittadini adottati da parte di enti locali e nazionali senza un coordinamento centralizzato anche al fine della distribuzione delle risorse economiche[7].

Allo stesso modo, si è avuto un forte impulso allo studio degli impatti sul diritto alla protezione dei dati a seguito dell'impiego dell'intelligenza artificiale a scopi di medicina preventiva o d'iniziativa da parte delle amministrazioni sanitarie.

Importanti le prese di posizione quanto ai sistemi di intelligenza artificiale applicate alla Università in relazione agli esami a distanza[8] e al mondo del lavoro[9].

Si tratta di un percorso lungo e articolato che il Garante ha compiuto parallelamente alle istituzioni europee. Per molto tempo l'Europa ha mantenuto un atteggiamento "light" sul tema. La maggior parte dei documenti degli ultimi anni, di fatto atti di soft law – come le "Linee guida relative ai principi sull'intelligenza artificiale" dell'OCDE e la Raccomandazione del Consiglio d'Europa adottata il 14 maggio 2019 – hanno mantenuto il livello della discussione soprattutto sul piano dei principi. Nel 2021, però, dopo la Risoluzione del Parlamento europeo sull'intelligenza artificiale, con la presentazione del Regolamento sull'Intelligenza artificiale si è compiuto un passaggio decisivo. L'innovatività non sta solo nell'essere la prima normativa a livello sovraregionale a disciplinare in modo organico l'IA, ma nel sottendere una scelta importante sia in termini regolatori, sia politici che assiologici. La bozza di Regolamento, infatti, implica il tentativo di rimodulare il perimetro del tecnicamente possibile sulla base di quello che si ritiene giuridicamente ed eticamente accettabile.

In un'ottica guidata dai valori europei e dalla tutela dei diritti fondamentali, l'Artificial Intelligence Act identifica diversi livelli di rischio nell'utilizzo di tali tecnologie, prevedendo limiti all'implementazione di tecnologie algoritmiche nel settore pubblico e privato.

Il Regolamento è oggi ancora in piena costruzione. Nel dicembre scorso il Consiglio ha condiviso la sua controproposta che ha parzialmente alterato il contenuto della proposta originaria[10]. Si aspetta adesso il testo di compromesso che dovrebbe uscire non prima di qualche mese. Nondimeno alcune annotazioni possono fin d'ora essere fatte con riferimento al rapporto con la normativa privacy e con la generale governance del sistema.

Intelligenza artificiale e normativa sulla protezione dei dati personali

Sebbene il Regolamento sulla protezione dei dati personali (GDPR) si focalizzi sul trattamento dei dati e la bozza di Regolamento sull'IA riguardi la tecnologia per effettuare tale trattamento – e dunque siano formalmente complementari – entrambi gli atti normativi rischiano di condurre ad un eccesso di regolamentazione.

Il futuro Regolamento sull'IA, infatti, non solo si applicherà come un'ulteriore legge di protezione sull'uso e sulla condivisione dei dati, ma avrà anche, necessariamente, una vasta area di potenziale sovrapposizione con il GDPR.

La sovrapposizione deriva, da un lato, dalla definizione estremamente ampia di IA, che comprende persino gli approcci statistici e, dall'altro lato, dal fatto che i cosiddetti sistemi di IA ad alto rischio sono definiti nella bozza per aree in cui per la stragrande maggioranza sono i dati personali ad essere trattati. Si pensi all'identificazione biometrica, all'istruzione, alla sanità, alle prestazioni assistenziali, all'immigrazione, ecc. Solo nel settore delle infrastrutture il Regolamento IA potrebbe avere un'applicazione del tutto autonoma. Negli altri settori vi sarebbe, di fatto, una coregolamentazione e, probabilmente, saranno le normative in materia di protezione dei dati personali a prevalere in quanto competenti per materia. La bozza di Regolamento AI riguarda poi in larga parte oggetti e i principi già enucleati nel GDPR (sebbene l'approccio al rischio diverga perché l'uno responsabilizza il titolare del trattamento ponendo al centro i diritti dell'interessato, l'altro invece introduce un meccanismo di compliance a standard predefiniti dall'alto). Entrambe le leggi si concentrano sulle finalità del trattamento dei dati personali, sull'utilizzo del sistema di IA, sull'approccio by design; entrambi richiedono che gli indirizzi del Regolamento identifichino i rischi per i diritti fondamentali. Tuttavia la proposta di Regolamento si propone esplicitamente di avere un approccio «umano-centrico» e di plasmare IA che siano affidabili e sicure per gli individui.

Naturalmente ci sono anche differenze, come ad esempio: a) il fatto che il GDPR è a portata generale (e quindi intersettoriale) e non è pensato per un ambito specifico; b) o il fatto che il Regolamento sull'IA si rivolge soprattutto agli sviluppatori e meno agli utilizzatori. Tutto sommato, però, non è affatto scorretto affermare che la regolamentazione prevista appare o simile (certe volte addirittura identica), con il rischio di una superfetazione di norme, o complementare. Un esempio del primo tipo si ha per quelle previsioni della bozza del Regolamento che riguardano i modi con cui cercare di contenere le imprevedibilità delle risposte degli algoritmi e, quindi, di limitare i cc.dd. risk managment attraverso una valutazione d'impatto (la c.d. Data Protection Impact Assessment), esattamente come è previsto all'art. 35 del GDPR. Un esempio di complementarietà si evince dal fatto che la bozza di Regolamento, sebbene sia orientato alla tutela degli individui, non prevede per questi ultimi la possibilità di intervenire come invece avviene ai sensi dell'art. 22 del GDPR, previsione chiave nella disciplina dell'automatizzazione.

Ecco, sia queste similitudini che queste differenze sollevano interrogativi riguardo al coordinamento tra il regime giuridico dei dati personali e dell'intelligenza artificiale. Pertanto, non è tanto l'individuazione dei principi e delle regole di condotta da applicare alla IA ad essere problematica, ma la loro concreta applicazione. È necessario capire come questa normativa andrà a recepire tali principi e tali regole, cioè come queste ultime si inverino concretamente sia nella vita digitale che analogica regolata dall'IA. Per capirci, un interrogativo è che ruolo debbano avere, ad esempio, in caso di dubbio interpretativo, le norme "fundamental-rights oriented" del GDPR[11]. Peraltro, il principio contenuto del GDPR che maggiormente sembra interpretare l'esigenza di integrare il rispetto dei diritti fondamentali nello sviluppo tecnologico è probabilmente quello della privacy by design enunciato nell'articolo 25 che può esser declinato, nel caso dell'intelligenza artificiale, come la necessità di proteggere i dati personali fin dal momento in cui un sistema di AI (una app, un software, una macchina intelligente…) viene progettato.

Il Considerando 78 GDPR è a tal fine esplicativo quando afferma, tra le altre cose, che «lo sviluppo, la progettazione, la selezione e l'utilizzo di applicazioni (…) dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati» e ovviamente dei suoi presupposti e precipitati. Ciò significa inserire una componente valoriale all'interno della progettazione tecnica e questo rende l'articolo 25 un precetto di tenore quasi costituzionale. Costituzionale sia in senso stretto, poiché rappresenta un requisito fondante della costruzione e del funzionamento dei processi algoritmici nella realtà sociale digitale, sia costituzionale in senso ampio perché inserisce a pieno titolo i diritti costituzionali nella dimensione digitale.

Il turno adesso è del Parlamento europeo, che dovrebbe ascoltare anche la società civile, sensibile al discorso sui diritti: sia il Comitato che il Garante europeo per la Protezione dei dati personali (EDPB/EDPS) hanno già tracciato la via nel loro parere congiunto (18 giugno 2021); in

termini analoghi si è espresso anche il Garante nei confronti del Parlamento nazionale nella precedente legislatura[12]. La proposta è quella di accogliere con favore l'approccio basato sul rischio, ma di accertarsi che la natura e il grado rischio per i diritti fondamentali sia uniformato ai parametri del GDPR e del Regolamento 2018/1725.

3. Governance del sistema.

Le contraddizioni tra metodo algoritmico e disciplina del GDPR investono, poi, anche il profilo della gestione. E qui ci si collega al tema che riguarda la supervisione sul Regolamento sull'IA. Se, infatti, l'IA è destinata ad avere, ed in larga parte ha già oggi, un sempre maggiore spazio sulla governance sia dell'infosfera che della biosfera, la domanda che dobbiamo porci è: come può essere concepita la governance di questa governance? Come verificare e regolare il suo buon funzionamento? In altre parole, chi deve controllare il gestore? Possono/devono essere le Autorità di protezione dei dati a contribuire a quest'opera (anche considerato che hanno una storia di diritti e "digitale" alle spalle piuttosto consolidata) o ci sono proposte migliori sul tappeto?

La rassegna meramente esemplificativa dei casi affrontati dal Garante privacy dimostra come i problemi di natura contenutistica legati all'intelligenza artificiale (potenziali bias nell'impostazione degli strumenti normativi che utilizzano l'IA, deviazioni, abusi) si risolvono in massimo grado attraverso un'attenta pratica regolatoria che tiene in considerazione i grandi vantaggi offerti dall'utilizzo degli algoritmi, ma allo stesso tempo li legge alla luce dei principi del nostro ordinamento giuridico.

Ora, né il primo draft della Commissione, né il secondo del Consiglio definiscono in maniera chiara la competente autorità a livello nazionale, ma rimettono ad ogni Stato membro la decisione di costituire una o più autorità nazionali di controllo.

La questione dell'Autorità che deve assumersi l'onere di gestire le prospettive applicative in tema di responsabilità da intelligenza artificiale resta un punto molto delicato. L'AI è, per sua natura, intra e infrasettoriale tanto che una prima ipotesi avanzata è stata, appunto, lo "spacchettamento" della competenza tra varie Autorità. Ovvio che una tale scelta, pur ragionevole, potrebbe rischiare di condurre ad una diversificazione delle risposte, portando a regole e gradi di supervisione diversi da settore a settore. Anche un sistema di scambio di informazioni tra Autorità coinvolte potrebbe rischiare, se non ben pianificato, di non essere adeguato allo scopo. Altra proposta emersa dal dibattito parlamentare è stata quella della creazione di una specifica Autorità dei diritti digitali. Ma questa stessa ipotesi sembra essere stata finora esclusa considerato che si sta, comunque, parlando di diritti fondamentali – cioè non di un tema nuovo – sia pur nella loro estensione digitale.

Per concludere

Sempre più negli ultimi anni gli interventi nel campo dell'IA sono stati caratterizzati da un approccio proattivo, volto ad estrarre da questa tecnologia gli effetti positivi per i cittadini e le imprese e mitigarne quelli dannosi. È proprio l'uso che faremo dell'intelligenza artificiale che ne determinerà la sua connotazione in senso positivo o negativo ed è per questo motivo che una sua efficace regolamentazione assume un'importanza fondamentale. Resta sempre da verificare quale sarà il testo definitivo del Regolamento e come verrà declinato l'aspetto della governance con riferimento all'Autorità competente. Quel che è certo è che non si potrà prescindere né dai principi del GDPR – considerato che la stessa intelligenza artificiale si nutre di dati e, in particolare, proprio quelli di natura personale – né da un ruolo centrale delle Autorità garanti per la protezione dei dati a livello nazionale nelle decisioni strategiche complessive e nelle regolazioni settoriali. Ciò sia per il contributo di expertise che esse potrebbero offrire ai titolari del trattamento pubblici e privati, sia perché ciò consentirebbe di assicurare, pur evitando di apporre superflui ostacoli all'innovazione, la giustiziabilità dei propri diritti e interessi sulla base di ormai consolidate prassi.

**Il presente scritto costituisce una rielaborazione dell'intervento tenuto il 20 gennaio 2023 alla Camera dei Deputati, Sala del Cenacolo, Palazzo Valdina, in occasione della presentazione dell'interessante e articolato volume di F. Lazzini, Etica e Intelligenza artificiale, Torino, Giappichelli, 2022.*

[1] Sui più recenti contributi si veda A. Simoncini, A. Adinolfi (a cura di), Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche, Napoli, ESI, 2022; sia, altresì, consentito rinviare anchea G. Cerrina Feroni, C. Fontana, E. Raffiotta (a cura di), AI Anthology, Bologna, Il Mulino, 2022. Specificamente sui due profili, cfr., rispettivamente, A. Pajno, M. Bassini, G. De Gregorio, M. Macchia, F. Paolo Patti, O, Pollicino, S. Quattrocolo, D. Simeoli, P. Sirena, AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista, in Rivista di Biodiritto/ Bio Law Journal, n. 3, 2019, G. D'Acquisto, On conflicts between ethical and logical principles in artificial intelligence, in AI & Society, vol. 35, n. 4, 2020, 895-900.

[2] A. D'Aloia, Ripensare il diritto nel tempo dell'intelligenza artificiale, in A. Pajno, F. Donati e A. Perrucci(a cura di), Intelligenza artificiale e diritto: una rivoluzione?, vol I (Diritti fondamentali, dati personali e regolazione), 2022,79-110, spec. 103.

[3] Cfr. caso "Metavaluate" (Ordinanza di ingiunzione – 26 luglio 2018; doc. web. n. 9052099).

[4] Provv. Doc. web. N. 7496252 del 21 dicembre 2017 "Istallazione di apparati promozionali del tipo 'digital signage' (definiti anche Totem) presso una stazione ferroviaria", con il quale il Garante ha riconosciuto lecito il trattamento nella misura in cui fossero stati rispettati alcuni specifici requisiti, in particolare sotto l'aspetto dell'informativa, del consenso e degli obblighi di sicurezza (artt. 12, 23 e 32 del Codice nella versione del tempo).

[5] Nel 2013 il Garante privacy ha affrontato il tema del c.d."Redditometro", strumento di controllo che si fondava sul trattamento automatizzato di dati personali presenti nell'anagrafe tributaria. L'Autorità ha espresso parere favorevole sulla richiesta dell'Agenzia delle Entrate, definendo però le garanzie necessarie per il rispetto dei diritti degli interessati. Sempre in ambito fiscale è poi da segnalare la sperimentazione di procedure per l'individuazione di profili di evasione attraverso l'analisi dei dati finalizzata. In tale occasione, il Garante ha individuato le misure di sicurezza e organizzative idonee per fare in modo che il controllo tramite algoritmo fosse conforme alla protezione dei dati personali ma, al contempo, efficace.

[6] Cfr. provv. 14 marzo 2019, n. 58, doc. web. n. 9106329 e, precdentemente, provv. 20 luglio 2017, n. 321, doc. web. n. 6843736).

[7] Con riferimento al parere del 5 marzo 2020 al Consiglio di Stato in merito ai criteri di ripartizione del Fondo Sanitario Nazionale che prevedevano il trattamento di dati personali, anche sulla salute, di tutti i cittadini assistiti dal Servizio sanitario nazionale, così da rimodulare il sistema di distribuzione delle risorse economiche sulla base dello stato di salute di ogni singolo assistito, il Garante ha rilevato che il progetto ministeriale risultasse privo di una base normativa necessaria per raggiungere gli obiettivi prefissati e che invece l'uso di algoritmi avrebbe suddiviso tutta la popolazione in gruppi per omogeneità patologiche e reddituali (cfr. provv. 15 dicembre 2022, n. 416, doc. web n. 9845156). Nello specifico, secondo il Garante, «la profilazione dell'utente del servizio sanitario, sia questo regionale o nazionale, determinando un trattamento automatizzato di dati personali volto ad analizzare e prevedere l'evoluzione della situazione sanitaria del singolo assistito e l'eventuale correlazione con altri elementi di rischio clinico (nel caso di specie l'infezione da Sars Cov-2), può essere effettuata solo nel rispetto di requisiti specifici e garanzie adeguate per i diritti e le libertà degli interessati».

[8] Provv. 16 settembre 2021, n. 317, doc. web n. 9703988 (Proctoring Bocconi).

[9] Sul tema del lavoro a domicilio, si pensi ai casi che hanno riguardato nel 2021 Deliveroo Italia cui il Garante ha irrogato il pagamento di una sanzione di 2 milioni e 500 mila euro per aver trattato in modo illecito i dati personali di circa 8000 rider nell'ambito dell'utilizzo dell'intelligenza artificiale per l'assegnazione dei turni.

[10] Si fa riferimento al testo del Consiglio del 25 novembre 2022. Sono state proposte molte modifiche, in particolare, volte a garantire una chiara definizione di un sistema di IA; ad estendere agli attori privati il divieto di utilizzare l'IA per il punteggio sociale; ad estendere il divieto di uso di sistemi di IA che sfruttano le vulnerabilità di un gruppo specifico di persone, anche alle persone vulnerabili a causa della loro situazione sociale o economica. Per quanto riguarda il divieto di utilizzare sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico da parte delle autorità, il testo chiarisce le situazioni nelle quali tale uso è strettamente necessario e nelle quali le autorità dovrebbero pertanto essere eccezionalmente autorizzate a utilizzare tali sistemi. Per quanto riguarda la classificazione dei sistemi di IA come ad alto rischio, il testo inserisce un livello orizzontale in aggiunta alla classificazione ad alto rischio, al fine di garantire che non siano inclusi i sistemi di IA che non presentano il rischio di causare gravi violazioni dei diritti fondamentali o altri rischi significativi. Si escludono le finalità militari, di difesa e di sicurezza nazionale dall'ambito di applicazione della normativa sull'IA. Analogamente, è stato chiarito che la normativa sull'IA non dovrebbe applicarsi ai sistemi di IA e ai loro output utilizzati esclusivamente a fini di ricerca e sviluppo e agli obblighi delle persone che utilizzano l'IA per scopi non professionali, che non rientrerebbero nell'ambito di applicazione della normativa sull'IA, fatta eccezione per gli obblighi di trasparenza. Tra le altre indicazioni, si propone di modificare le disposizioni relative al comitato per l'IA, con l'obiettivo di garantire che abbia una maggiore autonomia e di rafforzare il suo ruolo nell'architettura di governance della normativa sull'IA. Al fine di garantire il coinvolgimento dei portatori di interessi in relazione a tutte le questioni relative all'attuazione della normativa sull'IA, compresa la preparazione degli atti di esecuzione e delegati, è stato aggiunto l'obbligo per il comitato di istituire un sottogruppo permanente che funga da piattaforma per un'ampia gamma di portatori di interessi. Si propone di aumentare la trasparenza per quanto riguarda l'uso dei sistemi di IA ad alto rischio. In particolare, alcune disposizioni sono state aggiornate per indicare che alcuni utenti di un sistema di IA ad alto rischio che sono entità pubbliche saranno anche tenuti a registrarsi nella banca dati dell'UE per i sistemi di IA ad alto rischio. Inoltre, una nuova disposizione pone l'accento sull'obbligo per gli utenti di un sistema di riconoscimento delle emozioni di informare le persone fisiche quando sono esposte a tale sistema.

Il testo chiarisce inoltre che una persona fisica o giuridica può presentare un reclamo alla pertinente autorità di vigilanza del mercato riguardo alla non conformità alla normativa sull'IA e può aspettarsi che tale reclamo sia trattato in linea con le procedure specifiche di tale autorità.

[11] Tra le molte opere che si interrogano sulla portata dei diritti e delle libertà fondamentali nel digititale, v. G. Sartor, L'informatica giuridica e le tecnologie dell'informazione, Giappichelli, Torino 2022.

[12] Si veda l'audizione del Garante Garante per la protezione dei dati personali sul ddl di delegazione europea 2021 davanti alla XIV Commissione del Senato della Repubblica (8 marzo 2022).