LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 2 / 2025

Gianluigi CIACCI

Protezione dei dati personali e Intelligenza Artificiale

Protezione dei dati personali e Intelligenza Artificiale

Gianluigi CIACCI

Avvocato

Lo sviluppo di un'attenzione "diffusa" per l'IA, conseguenza anche del moltiplicarsi delle sue applicazioni nella quotidianità degli utenti (si pensi ad esempio agli assistenti virtuali nei cellulari o in *device* casalinghi, ed all'"esplosione" dei *chatbot* e dell'intelligenza artificiale generativa), oltre a portarla al di fuori della discussione tra esperti, ha fatto nascere un dibattito sulla necessità di trovare un equilibrio fra due opposte esigenze:

– non rallentare, o addirittura bloccare, il progresso del settore, e quindi le conseguenze positive dello stesso (e poi sì, anche l'enorme business da essa resa possibile direttamente, per il valore in sé dell'IA e, indirettamente, per la ricchezza prodotta dalle sue applicazioni);

– impedire che tale progresso avvenga in danno dei suoi utenti.

Dicotomia che raggiunge una forte criticità, da una parte, proprio nel momento in cui dal suo sviluppo dipendono enormi interessi economici ("aumentando la posta in gioco"); e, dall'altra, quando il danno agli utenti riguarda i loro dati personali: in questo secondo caso soprattutto a causa della presenza di una normativa forte, rappresentata dal Regolamento UE 27 aprile 2016, n. 679 (il c.d. GDPR), finalizzata proprio a prevenire, o comunque limitare, tale potenziale danno.

Rispetto alla quale si entra in contatto con un'anomalia "paradigmatica", soprattutto con riferimento al nostro Paese: principalmente creata dall'idea generalizzata che vede la relativa disciplina come assolutamente inutile, burocratica, anzi, addirittura dannosa per chi vuole oggi fare impresa ("se c'è la privacy non si può fare niente"), insomma qualcosa da cui difendersi. Conseguenza di tale anomalia è stata la forte carenza negli anni di una generalizzata "cultura" della protezione dei dati personali, la disattenzione politica al problema, lo scarso livello di adeguamento alla legge delle strutture dei vari titolari di trattamento, privati ed anche pubblici. Carenza che purtroppo ha portato ad un forte divario tra la sempre maggiore diffusione dell'uso delle tecnologie nella nostra quotidianità, in ogni momento della quale si realizza una costante interazione con esse (ed alla conseguente condivisione delle nostre informazioni, anche le più delicate: si pensi a come oggi vengono utilizzati i social network non solo da parte degli utenti giovani e giovanissimi, ma anche delle generazioni precedenti), e la regolamentazione, non necessariamente giuridica, delle stesse: spesso inadeguata, in linea di massima non conosciuta, in genere non applicata.

Infatti la disciplina in materia di protezione dei dati personali applicata ai sistemi di intelligenza artificiale incontra diversi problemi, che rendono il rispetto degli obblighi da essa dettati estremamente complesso per i titolari di trattamento che usano, in diverse realtà, tali sistemi [1].

[1] Il riferimento è non solo ai produttori di sistemi di intelligenza artificiale, ma anche agli utenti degli stessi: i primi certamente dovranno applicare quanto disposto dalla disciplina posta a tutela delle informazioni relative agli individui impiegate fin dalla fase di istruzione dei loro algoritmi, ma poi anche in quella successiva di completa operatività. Per quanto riguarda poi gli utenti, si devono prendere in considerazione coloro che usano le macchine intelligenti non già per le proprie specifiche esigenze (ad esempio per ricercare informazioni in una determinata banca dati su cui operano sistemi di ricerca assistita dall'I.A., o per fare i compiti di scuola con Chat GPT), ma per svolgere il loro lavoro in cui sottopongono a processi automatizzati attraverso gli innovativi algoritmi dati personali dei loro clienti (si pensi agli avvocati che oggi utilizzano applicativi di intelligenza artificiale per lavorare le pratiche dei propri assistiti: applicativi che per funzionare vengono

Tra questi, le difficoltà nell'applicazione dei principi generali di trasparenza, minimizzazione e limitazione della conservazione (art. 5, par. 1, rispettivamente lett. *a*, *c*, *e* del Regolamento UE 2016/679); la complessità nell'individuazione delle basi giuridiche per il trattamento dei dati personali (artt. 6 e 9 del Regolamento); i problemi nell'adempimento degli obblighi di informativa (artt. 13 e 14) e di quello di agevolare l'esercizio dei diritti (art. 12, par. 2); le difficoltà nella determinazione e regolamentazione dei soggetti coinvolti nel trattamento dei dati collegati alle "macchine intelligenti", il cosiddetto "organigramma privacy" (in particolare per le figure del titolare, dei contitolari, del responsabile del trattamento, e dei subresponsabili).

Per risolvere tali difficoltà applicative, e quindi utilizzate per superare il contrasto tra lo sviluppo delle macchine intelligenti e la necessità di tutelare i diritti fondamentali dell'individuo, in modo da evitare che tale sviluppo si realizzi a suo danno, ci si deve muovere dall'analisi del contesto normativo che oggi regolamenta l'intelligenza artificiale e le sue applicazioni, attraverso la conoscenza approfondita della disciplina in materia di protezione dei dati personali, per poi arrivare a "tracciare" la strada da seguire: analisi volta stabilire se nella normativa di settore venga meno presa in considerazione tale disciplina, e con quale incidenza.

Non potendo nel presente scritto procedere ad un completo esame delle fonti sull'intelligenza artificiale, si riporta quale esempi da una parte il recente Regolamento UE 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (il c.d. A.I. Act, quindi la normativa di riferimento per quanto riguarda l'innovativa tecnologia che sta sempre più entrando nella nostra quotidianità); dall'altra, il disegno di legge italiano del 20 maggio 2024 n.1146, intitolato "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", che è stato approvato dal Senato in data 20 marzo 2025 ed ora è in esame alla Camera.

Per quanto riguarda la fonte europea, la stretta connessione con la disciplina che tutela le informazioni relative agli individui si manifesta sia a livello di sistema normativo, sia per i numerosi richiami al GDPR che si possono riscontrare nel suo testo. Dal primo punto di vista, viene evidenziata la scelta del legislatore europeo di riproporre la struttura del Regolamento 2016/679 per disciplinare l'intelligenza artificiale e le sua applicazioni, costituiscono esempi di tale connessione la presenza anche nell'AI Act:

– del criterio della localizzazione dei destinatari dell'offerta produttiva quale parametro di applicazione territoriale della normativa (c.d. *target*, art. 2, par. 1, lett. *a* e c [2]);

– dell'approccio fondato sul rischio (modulato secondo una piramide di gravità ascendente), con la correlata valutazione d'impatto (si vedano a tale proposito il Considerando 96 e l'art. 27, intitolato proprio "*valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio*");

– delle certificazioni e dei codici di condotta in funzione co-regolativa (art. 95);

– della modulazione del trattamento sanzionatorio secondo il fatturato, così da esercitare maggiore deterrenza (artt. 99-101);

"alimentati" con tutte le informazioni di tali pratiche, sicuramente riservate, e spesso anche di natura sensibile): dati che dovranno dunque essere protetti, rispettando la normativa di settore.

[2] Secondo tale norma il Regolamento si applica: *a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo;* (...) *c) ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione*.

– della presenza di una comunicazione obbligatoria degli "incidenti" potenzialmente pregiudizievoli (art. 73);

– della creazione di un'Autorità di controllo interna ai singoli Paesi (art. 70);

– del coordinamento tra le autorità nazionali nell'ambito di un Comitato europeo per l'IA (art. 65).

Tutti aspetti che, come si è visto, dimostrano che questa fonte, fondamentale per la realtà delle macchine intelligenti, nel replicare la "costruzione" e le caratteristiche del Regolamento 2016/679, ribadiscono efficacia e importanza della relativa disciplina, e ne valorizzano la centralità anche in tale settore.

Dal secondo punto di vista, invece, quello che evidenzia i numerosi richiami al GDPR che si possono riscontrare nel testo del Regolamento UE 2024/1689, nell'ambito del presente scritto ci si limita a riportare quanto previsto dal suo Considerando 10 e dall'art. 2, par. 7.

Nel primo riferimento viene infatti specificato che l'A.I. Act "*non mira a pregiudicare l'applicazione del vigente diritto dell'Unione che disciplina il trattamento dei dati personali, inclusi i compiti e i poteri delle autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti*" [3]; mentre la seconda norma, nell'indicare relativamente l'ambito di applicazione di tale fonte, specifica che "*il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti*" nel Regolamento 2024/1689, che quindi "lascia impregiudicato" il GDPR.

Anche il DDL n.1146 (iniziativa legislativa italiana mirata a regolamentare l'impiego dell'intelligenza artificiale in vari settori di rilevanza strategica, comprese le P.A.) riporta diversi richiami al Regolamento 2016/679: in particolare, si rivelano di estrema importanza gli artt. 3, sui principi generali, e 4, intitolato "*Principi in materia di informazione e di riservatezza dei dati personali*". I due commi della prima delle due norme testualmente dispone:

> "1. *La ricerca, la sperimentazione, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi e di modelli di intelligenza artificiale avvengono nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei princìpi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.*".
>
> "3. *I sistemi e i modelli di intelligenza artificiale devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della spiegabilità e dei princìpi di cui al comma 1.*".

Mentre l'art. 4 (in particolare i suoi commi 2, 3 e 4) dispone

> "2. *L'utilizzo di sistemi di intelligenza artificiale garantisce il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti, in conformità con il diritto dell'Unione europea in materia di dati personali e di tutela della riservatezza.*

[3] Per poi proseguire affermando che il Regolamento "*lascia impregiudicati gli obblighi dei fornitori e dei deployer dei sistemi di IA nel loro ruolo di titolari del trattamento o responsabili del trattamento derivanti dal diritto dell'Unione o nazionale in materia di protezione dei dati personali, nella misura in cui la progettazione, lo sviluppo o l'uso di sistemi di IA comportino il trattamento di dati personali. È inoltre opportuno chiarire che gli interessati continuano a godere di tutti i diritti e le garanzie loro conferiti da tale diritto dell'Unione, compresi i diritti connessi al processo decisionale esclusivamente automatizzato relativo alle persone fisiche, compresa la profilazione*".

3. *Le informazioni e le comunicazioni relative al trattamento dei dati connesse all'utilizzo di sistemi di intelligenza artificiale avvengono con linguaggio chiaro e semplice, in modo da garantire all'utente la piena conoscibilità e la facoltà di opporsi ai trattamenti non corretti dei propri dati personali.*

4. *L'accesso alle tecnologie di intelligenza artificiale dei minori di anni quattordici richiede il consenso di chi esercita la responsabilità genitoriale. Il minore degli anni diciotto, che abbia compiuto quattordici anni, può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, purché le informazioni e le comunicazioni di cui al comma 3 siano facilmente accessibili e comprensibili.*".

Un testo che non lascia quindi dubbi sul fatto che, anche nella realtà di trattamento dei dati personali attraverso sistemi di intelligenza artificiale, non è ammissibile il mancato rispetto dei due diritti fondamentali dell'individuo, quelli di riservatezza e di protezione dei dati personali.

Così, rispetto alle norme dettate per le macchine intelligenti, ed in particolare a quelle contenute nelle due fonti di riferimento per l'intelligenza artificiale sopra richiamate, la loro analisi dimostra come siano sempre presenti richiami, più o meno specifici, alla tutela delle informazioni relative agli individui: riferimenti che ribadiscono e sottolineano l'importanza del rispetto dei diritti fondamentali dell'individuo, in particolare quello alla protezione dei suoi dati personali, anche nella realtà delle applicazioni dell'intelligenza artificiale. Situazione che pone il contrasto indicato all'inizio di questo breve scritto [4] non tanto e non solo nella dicotomia "applico/non applico", ma anche nella più ampia scelta tra "rispetto/non rispetto" la legge: e allora non si può certo ritenere ammissibile la rinuncia alla legalità, e nella specie a tale protezione.

Provando allora ad immaginare le possibili soluzioni a tale contrasto, le "cose da fare", indichiamo tre differenti ambiti.

Innanzitutto, dal punta di vista dei "*player*" del settore, cioè da un lato i produttori/fornitori di sistemi di intelligenza artificiale, dall'altro gli utilizzatori di tali sistemi a scopo professionale (comunque tutti "titolari del trattamento" se questi vengono applicati ad informazioni relative agli individui, direttamente o indirettamente identificabili), questi devono essere portati ad adeguarsi obbligatoriamente e in maniera corretta ed effettiva al sistema della protezione dei dati personali introdotto dal Regolamento 2016/679, ognuno nell'ambito della propria attività di trattamento di tali dati.

Con riferimento poi agli utenti delle macchine intelligenti, occorre sviluppare il più possibile una tutela "dal basso", cioè posta in essere dagli stessi interessati che, in maniera più o meno consapevole, cedono i loro dati ai *player* citati: tutela che deve partire dalla loro corretta ed efficace informazione e formazione, in generale sulla realtà digitale in cui vivono, ma anche in particolare su quella del trattamento dei dati personali, sugli utilizzi che se ne fanno nei sistemi di intelligenza artificiale, e quindi sulle modalità della loro tutela. Portandoli in questo modo a realizzare che non possono più essere solo passivi fruitori della sempre più pervasiva innovazione tecnologica, né d'altro canto "tecno-entusiasti" senza alcun senso critico: ma che devono diventare "tecno-consapevoli", capaci così di gestire tale innovazione, e dunque di proteggere i propri diritti fondamentali, non ultimo per evitare di essere gestiti da essa.

Infine, si ritiene necessario potenziare il più possibile anche la tutela "dall'alto", sia a livello

[4] Quello tra l'esigenza di non rallentare o impedire il progresso dell'I.A., e quindi le conseguenze positive dello stesso, ma al contempo impedire che tale progresso avvenga in danno dei suoi utenti.

normativo, realizzando discipline che non si limitino solo a semplici richiami o ad affermazioni generali di principio, ma che individuino regole certe ed efficaci; sia rispetto alle Autorità di controllo (nel nostro Paese il Garante per la protezione dei dati personali), in particolare potenziandole e rendendole maggiormente operative. Dando quindi a queste ultime la possibilità di fornire un concreto ausilio per la realizzazione di quanto appena riportato: e dunque di condurre all'adeguamento alla disciplina normativa, in maniera qualitativamente migliore, i citati "*player*" del settore e, allo stesso tempo, di rendere consapevoli il maggior numero possibile di interessati.

Soluzioni sicuramente ambiziose, e allo stesso tempo di difficile realizzazione, e comunque non in tempi brevi. Ma occorre capire innanzitutto che, a fronte della repentina evoluzione delle macchine intelligenti, sempre più potenti ed invasive della nostra sfera privata, non si può non fare qualcosa per giungere alla soluzione del contrasto tra sviluppo dell'intelligenza artificiale e protezione dei dati: tra l'altro accorciando il più possibile i tempi per conseguire il relativo risultato. E questo avendo ben chiaro che il problema in realtà si pone su un livello più alto di quanto possa sembrare: in particolare quello tra la limitazione, o addirittura la rinuncia a un diritto fondamentale dell'individuo per l'importanza (economica) del settore, il cui sviluppo può comunque avere indubbi vantaggi per tutti noi, ed in ogni caso è oramai impossibile fermare.

Per questo motivo la soluzione sembra essere fondamentalmente quella di un "salto culturale", giuridico e tecnologico, finalizzato a portare al 100% di successo il sistema di protezione dei dati personali, quale contrappeso e limite rispetto agli innovativi (e di moda) sistemi di intelligenza artificiale: sfruttando in questo modo le utilità che possono apportare alla nostra vita, senza doverne subire necessariamente gli aspetti negativi. Salto culturale che deve portare innanzitutto ad un utilizzo sempre più consapevole delle tecnologie dell'informazione e comunicazione, in generale e nelle specifiche applicazioni di intelligenza artificiale; inoltre, e soprattutto, a valorizzare la disciplina in materia di protezione dei dati personali, a partire dalla sua effettiva, e seria, conoscenza, al di là di preconcetti o "scomodità" legate alla sua applicazione; infine, a promuovere e realizzare un uso "equilibrato" delle macchine intelligenti, non ultimo evidenziando la necessità e l'importanza della supervisione "umana" sul loro funzionamento e sui risultati realizzati tramite esse.

A tale proposito si può richiamare, in conclusione, quanto riportato da Guido Scorza, uno dei membri dell'attuale collegio del Garante per le protezione dei dati personali, in un breve scritto [5] a commento del provvedimento dell'Autorità nei confronti di Open AI per le violazioni della normativa in materia di protezione dei dati personali collegate all'uso di Chat GPT: "(...) *le ragioni del business e del progresso debbano sempre essere bilanciate con quelle dei diritti e delle libertà perché non si può definire innovazione una qualsiasi forma di progresso tecnologico ma solo quel progresso tecnologico capace di accrescere il benessere collettivo, per quanto possibile in un mondo che è rimane segnato da profonde differenze e iniquità, in maniera orizzontale, condivisa, universale almeno in termini di ambizione. Insomma, non esiste innovazione lontano dai diritti e dalle libertà fondamentali*".

[5] Si veda G. SCORZA, *Garante: "Chatgpt ha violato la nostra privacy", che succede ora?*, in *Agenda Digitale*, 20 dicembre 2024, https://www.agendadigitale.eu/sicurezza/privacy/garante-chatgpt-ha-violato-la-nostra-privacy-che-succede-ora/ visitato il 3 aprile 2025