



FLAVIA ZORZI GIUSTINIANI*

LA LEGGE ITALIANA SULL'INTELLIGENZA ARTIFICIALE E LA SENTENZA DELLA CORTE DI GIUSTIZIA SULLA PSEUDONOMIZZAZIONE DEI DATI PERSONALI **

SOMMARIO: 1. La legge italiana sull'intelligenza artificiale. 2. La sentenza della Corte di Giustizia sulla pseudonomizzazione dei dati personali.

1. La legge italiana sull'intelligenza artificiale

Nel periodo in rassegna la maggior novità è costituita dall'adozione, da parte del Parlamento italiano, della Legge n. 132 del 23 settembre 2025, recante “Disposizioni e deleghe al Governo in materia di intelligenza artificiale”. Con tale atto, qualificabile come legge quadro, l'Italia è stata il primo Stato membro dell'Unione a dotarsi di una normativa organica dedicata all'intelligenza artificiale (di seguito IA). Il testo, composto da 28 articoli, intende da un lato dare attuazione agli obblighi previsti dal Regolamento UE 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (*AI Act*), e dall'altro, disciplinare l'utilizzo dell'IA nei settori rientranti nelle competenze normative nazionali. Come stabilito espressamente dall'art. 1 par. 2, la Legge deve essere interpretata ed applicata in modo conforme all'*AI Act*.

Trattandosi di una legge quadro, essa mira essenzialmente a fissare le basi per i successivi provvedimenti attuativi, che disciplineranno nel dettaglio la materia. Principio generale comune ai diversi ambiti regolati, che corrispondono ai settori considerati ad alto rischio dall'*AI Act*, è costituito dal ricorso meramente ausiliario allo strumento dell'IA, in linea con un approccio antropocentrico.

In ambito sanitario, il suddetto principio è ribadito e declinato sottolineando l'insostituibilità del medico. L'utilizzo dell'IA è consentito a certe condizioni come strumento di supporto, ai professionisti medici, per diagnosi e cure, e garantendo il diritto dei pazienti ad essere informati sull'*an* e il *quomodo* del ricorso a sistemi di IA nel proprio

* Professoressa associata di Diritto dell'Unione europea – Università degli Studi Link, Roma.

** Contributo sottoposto a *peer review*.

trattamento sanitario. Si prevede poi lo sviluppo, a cura dell'Agencia nazionale per i servizi sanitari regionali (AGENAS), di una specifica piattaforma nazionale sull'IA in materia sanitaria al fine di garantire sicurezza, minimizzazione dei dati e rispetto della dignità umana.

Nel settore della giustizia, si esclude anzitutto qualsiasi ruolo decisionale dell'IA nell'attività giurisdizionale¹. Viceversa, l'uso della stessa è consentito esclusivamente per compiti organizzativi o ausiliari, così da garantire la piena compatibilità con i principi della Costituzione italiana e la sindacabilità delle decisioni giudiziarie. Analogamente, in ambito amministrativo l'IA è concepita come meramente strumentale e di supporto ai funzionari, al fine di aumentare l'efficienza, ridurre i tempi procedurali e migliorare i servizi.

In tema di *copyright*, la legge interviene modificando la legge sul diritto d'autore (in particolare l'articolo 1 di quest'ultima) sancendo un principio fondamentale, ovvero che unicamente le opere frutto dell'ingegno umano, anche se ideate con l'ausilio di strumenti di IA, possono beneficiare della protezione del diritto d'autore². Sono dunque esclusi da ogni protezione i contenuti generati dall'IA senza alcun contributo creativo umano, con la conseguente necessità di dover provare, e valutare, detto contributo, richiedendo probabilmente l'intervento di professionisti e aprendo la strada a relativi contenziosi contrattuali. Al fine, tuttavia, di non comprimere lo sviluppo dell'IA, è previsto, in tema di addestramento dei modelli di IA, che le aziende sviluppatrici possano utilizzare per i propri algoritmi materiali reperiti in rete, a patto che l'accesso agli stessi sia legittimo e che l'estrazione di testo e dati avvenga per finalità di addestramento.

In ambito lavorativo, si introduce l'obbligo di informare i lavoratori circa l'utilizzo di strumenti di IA e si vietano *tout court* le discriminazioni algoritmiche, mentre è incoraggiato il ricorso all'IA per il miglioramento delle condizioni di lavoro e della sicurezza. Viene poi istituito, presso il Ministero del lavoro, un Osservatorio nazionale sull'IA nel lavoro al fine di monitorare evoluzione ed impatto dell'IA sull'occupazione e altresì promuovere nuove tutele per i lavoratori. Relativamente alle professioni regolamentate, il ricorso all'IA è permesso soltanto come attività strumentale e di supporto all'attività professionale, in modo tale che risulti la prevalenza del lavoro intellettuale svolto dal professionista con riguardo alla singola prestazione d'opera³.

Tra i punti più delicati, e criticati, vi è quello relativo alla *governance* dell'IA. Il sistema delineato dalla legge 132 assegna un ruolo centrale, di coordinamento, alla Presidenza del Consiglio e in particolare al Dipartimento per la trasformazione digitale, nonché a cascata al Comitato interministeriale di coordinamento sugli enti che operano nell'IA, di cui è prevista l'istituzione. Vengono altresì designate quali Autorità nazionali per l'IA due agenzie governative, l'Agencia per la Cybersicurezza Nazionale (ACN) e l'Agencia per l'Italia

¹ Cfr. Part. 15 della legge, che stabilisce che "ogni decisione sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti" è sempre riservata al magistrato. In termini analoghi, per la pubblica amministrazione l'IA potrà essere utilizzata soltanto come supporto e mai in sostituzione della valutazione o della responsabilità umana (cfr. art. 14).

² Cfr. l'art. 25 della legge 132. Il mancato rispetto di queste disposizioni potrà comportare specifiche sanzioni (come previsto dall'art. 26, comma 3 della Legge).

³ Cfr. l'art. 13 della legge 132.

Digitale (AgiD), ferme restando le competenze specifiche di Banca d'Italia, Consob e Ivass, e il necessario coordinamento con le Autorità preesistenti come il Garante per la protezione dei dati personali e l'Autorità Garante per le garanzie nelle comunicazioni⁴. Nello specifico, AgiD dovrà promuovere l'innovazione tecnologica e lo sviluppo dell'IA, con compiti di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità; ACN invece avrà compiti di vigilanza ed ispezione e potrà irrogare sanzioni ai trasgressori dell'impianto normativo. Le due agenzie dovranno inoltre istituire e cogestire spazi di sperimentazione finalizzati alla realizzazione di sistemi di IA (*sandbox*) conformi alla normativa nazionale ed europea. A ciò si accompagna la previsione dell'adozione di una Strategia nazionale per l'IA, che sarà concepita ed aggiornata su base biennale dal Dipartimento per la Trasformazione Digitale con l'ausilio di AgiD e ACN al fine di coordinare le politiche pubbliche in materia di IA. Sullo stato di attuazione della Strategia si prevede, a fini di trasparenza e per garantirne una concreta efficacia, un monitoraggio annuale da parte del Parlamento.

Un'altra novità di rilievo riguarda la previsione del reato di *deepfake*, con l'introduzione nel codice penale dell'art. 612-quater, che punisce chi diffonde, senza consenso, immagini, video o voci falsificati tramite AI e idonei a trarre in inganno (i *deepfake*, per l'appunto). La procedibilità, salvo aggravanti, è a querela, e il nuovo reato è punito con la reclusione da uno a cinque anni "se dal fatto deriva un danno ingiusto". Come è stato osservato, tuttavia, la norma presenta diverse criticità, a partire dalla estrema genericità della condotta e dalle particolari difficoltà nell'accertamento del dolo e delle aggravanti tecnologiche in assenza di adeguati e specifici sistemi tecnici di accertamento⁵. Altro limite è poi costituito dalla necessità, per la parte offesa, di fornire prova del danno subito.

In ambito lavorativo, si introduce l'obbligo di informare i lavoratori circa l'utilizzo di strumenti di IA e si vietano *tout court* le discriminazioni algoritmiche, mentre è incoraggiato il ricorso all'IA per il miglioramento delle condizioni di lavoro e della sicurezza. Viene poi istituito, presso il Ministero del lavoro, un Osservatorio nazionale sull'IA nel lavoro al fine di monitorare evoluzione ed impatto dell'IA sull'occupazione e altresì promuovere nuove tutele per i lavoratori. Una critica condivisa dai tre sindacati confederali è l'assenza di qualsiasi riferimento al controllo a distanza dei lavoratori e la mancata previsione di una

⁴ La mancata indipendenza delle due agenzie è stata peraltro oggetto di critiche (cfr. *Una legge sull'IA che non ci protegge: più potere al governo e meno diritti*, in *Hermes*, 18 settembre 2025, disponibile al link <https://hermescenter.org/iniziative/una-legge-sullia-che-non-ci-protette-piu-potere-al-governo-e-meno-diritti/>).

⁵ "Il rischio vero, allora, per le tecnologie è quello di un diritto penale proclamatorio inefficace, incerto e sproporzionato e, alla fine, senza neppure un'attenzione reale agli strumenti di accertamento effettivo dei reati presentati come soluzione ai mille problemi e ai mille rischi che ogni giorno la tecnologia pone" (sic G. CORASANITI, *Entra in vigore la legge 132/2025: l'Italia detta le nuove regole per l'AI*, in *Consiglio nazionale degli ingegneri*, 10 ottobre 2025, disponibile al link https://www.cni.it/images/Rassegna_stamp/2025/37_02.pdf).

consultazione preventiva con le sigle sindacali riguardo all'integrazione di sistemi di IA nelle aziende per l'organizzazione del lavoro⁶.

Tra le criticità maggiori vi è, infine, il mancato stanziamento di finanziamenti per le misure previste, con la conseguenza che il tutto dovrà essere finanziato con risorse già esistenti⁷ e con il rischio concreto di complicare ulteriormente l'attuazione⁸. Per dare una valutazione completa della Legge e della sua efficacia, bisognerà comunque attendere l'emanazione dei numerosi decreti attuativi previsti.

2. La sentenza della Corte di Giustizia sulla pseudonomizzazione dei dati personali

Una seconda novità da segnalare è la sentenza resa dalla Corte di Giustizia dell'Unione europea (CGUE) il 4 settembre scorso nella causa C-413/23 P. Il caso trae origine dal piano di risoluzione del Banco Popular Español SA del 7 giugno 2017, in cui il Comitato di Risoluzione Unico (*Single Resolution Board - SRB*)⁹ incaricava la società di revisione Deloitte di valutare commenti e osservazioni sull'operazione bancaria proposta provenienti da azionisti e creditori, previamente pseudonomizzati.

A seguito del reclamo di alcuni azionisti e creditori, il Garante europeo di protezione dei dati (*European Data Protection Supervisor - EDPS*) accertò che i commenti e le osservazioni condivisi, benché pseudonomizzati, potevano comunque qualificarsi come “dati personali” e che pertanto l'SRB avrebbe dovuto informare gli interessati dell'avvenuto trasferimento ai sensi dell'art. 15 del Regolamento UE 2018/1725 sulla tutela della privacy da parte delle istituzioni, degli organi e degli organismi dell'Unione. Il Tribunale dell'Unione, accogliendo parzialmente il ricorso dell'SRB, interpretava invece l'obbligo di informazione in senso restrittivo e sanciva che, non potendo Deloitte re-identificare i soggetti, i dati non fossero personali dal suo punto di vista. La controversia veniva quindi portata, su ricorso dell'EDPS, innanzi alla CGUE.

La Corte di Lussemburgo, nella sua sentenza qui in commento, si è soffermata anzitutto sulla definizione di dato personale di cui all'art. 3 par. 1 del Regolamento (UE) 2018/1725 e, rilevando l'estrema similarità con quella dell'art. 4 par. 1 del Regolamento 2016/679 (*General Data Protection Regulation - GDPR*), ha ritenuto che ciò richieda

⁶ Come riportato da C. MORELLI, *Pro e contro della legge sull'intelligenza artificiale, l'analisi*, in *Wired*, 24 settembre 2025, disponibile al link <https://www.wired.it/article/legge-italiana-intelligenza-artificiale-tra-innovazione-e-occasioni-mancate/>.

⁷ Al riguardo l'art. 23 si limita a prevedere investimenti *futuri* in materia di *cybersecurity* e calcolo quantistico.

⁸ Cfr. l'art. 27 della Legge, che esclude “nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni pubbliche interessate provvedono all'adempimento delle disposizioni della presente legge con le risorse umane, strumentali e finanziarie *disponibili a legislazione vigente*” (corsivo nostro).

⁹ L'SRB è un'agenzia europea istituita dal Regolamento (UE) n. 2014/806 del Parlamento europeo e del Consiglio del 15 luglio 2014 al fine di avviare e, in seguito, gestire i procedimenti di risoluzione delle crisi degli enti creditizi, anche attraverso l'utilizzo delle risorse finanziarie del Fondo di risoluzione unico, creato dal medesimo regolamento.

un'interpretazione uniforme delle due disposizioni. Il fatto che le opinioni o i punti di vista personali siano, per loro natura, fortemente collegati a colui che li esprime in quanto espressione diretta dell'individualità di quest'ultimo, è sufficiente per ritenere che riguardino tale individuo. Detti dati, indipendentemente da una verifica caso per caso del loro contenuto, finalità o conseguenze, come richiesto invece dal Tribunale, devono pertanto qualificarsi quali dati personali. I titolari del trattamento dovranno dunque rispettare gli obblighi posti al riguardo dal GDPR come dal Regolamento 2018/1725.

Nondimeno, ha aggiunto la Corte, la natura dei dati pseudonimizzati è relativa. Per pseudonimizzazione l'art. 3 par. 6 del Regolamento 2018/1725 intende un'attività di trattamento grazie alla quale i dati non possono essere ricondotti ad una persona fisica senza l'uso di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e siano protette da misure tecniche e organizzative appropriate¹⁰. Ne consegue che mentre per il titolare i dati pseudonimizzati restano sempre personali, per il destinatario – nel caso di specie, Deloitte – la natura è relativa e dipende dalla sua concreta capacità di re-identificare gli interessati. L'SRB avrebbe quindi dovuto informare i diretti interessati del trasferimento dei loro dati, anche se gli stessi erano pseudonimizzati, indicando Deloitte come destinatario già nell'informativa iniziale. Un siffatto obbligo di informazione è idoneo a garantire un trattamento corretto e trasparente nonché rafforza il diritto dell'interessato alla prevedibilità del trattamento.

Così statuendo la Corte è riuscita a coniugare la protezione dei dati con le esigenze di flessibilità discendenti dalla loro circolazione. In altri termini, la riferita connotazione mista di uno stesso dato personale, aumentando la fiducia verso la pseudonimizzazione, è funzionale ad una sua più ampia circolazione.

¹⁰ La pseudonimizzazione, a seconda delle circostanze del caso di specie, è dunque idonea ad impedire l'identificazione dell'interessato da parte di persone diverse dal titolare del trattamento, cosicché per queste l'interessato non possa essere identificato.