Camera dei deputati

Commissioni IX e X riunite

Disposizioni e deleghe al Governo in materia di intelligenza artificiale (C. 2316)

Audizione del Presidente del Garante per la protezione dei dati personali

Prof. Pasquale Stanzione

Il disegno di legge, nella versione già approvata dal Senato (AS 1146) il 20 marzo u.s., reca disposizioni di principio in materia di ricerca, sperimentazione, sviluppo, adozione, applicazione e utilizzo dei sistemi e modelli di intelligenza artificiale per finalità generali, volte a indirizzarne l'applicazione in una direzione antropocentrica, socialmente ed eticamente sostenibile (artt. 1, c. 1, e 3, c. 1). In particolare, muovendo dalla disciplina unionale in materia (Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024*; infra*: Ai Act), promuove un utilizzo "corretto, trasparente e responsabile" dell'intelligenza artificiale, garantendone la vigilanza rispetto ai rischi economici e sociali e all'impatto sui diritti fondamentali degli interessati.

Sul testo originario il Garante ha già formulato alcune prime considerazioni, in particolare attraverso l'audizione del 24 luglio 2024 presso le Commissioni riunte 8ª e 10ª del Senato e il parere reso alla Presidenza del Consiglio dei Ministri in data 2 agosto 2024. Il mancato recepimento dei rilievi sinora formulati rende opportuno svolgere una riflessione complessiva, che tiene conto anche delle modifiche apportate nell'ambito della prima lettura.

CAPO I – Articoli 1 e 3

Il Capo I reca disposizioni in materia di **princìpi** e finalità del provvedimento, focalizzandosi su quelli di carattere generale, sui princìpi in materia di informazione e riservatezza dei dati personali, di sviluppo economico, nonché su quelli di sicurezza e difesa nazionale.

In proposito, il Garante ha già sottolineato (e qui ribadisce) l'opportunità di introdurre un articolo specifico e ad applicazione trasversale – sopprimendo, di riflesso, i commi 2 e 3 dell'articolo 4 – recante un vincolo generale di conformità dei trattamenti alla disciplina in materia di protezione dei dati personali, così da assorbire − salvo eventuali istituti espressamente richiamati con rinvio mobile − i singoli riferimenti alle disposizioni rilevanti in materia.

Potrebbe quindi risultare opportuno, anche per garantire una maggiore coerenza del sistema, prevedere – se non in un articolo specifico, quantomeno al comma 2 dell'articolo 1 – un richiamo all'osservanza generale della disciplina in materia di protezione dei dati personali (analogo richiamo, inoltre, potrebbe essere stabilito con riferimento all'articolo 3, comma 1, del testo, il cui riferimento alla protezione dei dati personali, peraltro, andrebbe più correttamente inserito nell'ambito dei diritti fondamentali di cui si impone il rispetto e non, invece, tra i "principi" di cui si esige l'osservanza).

Per quanto attiene al comma 2 dell'articolo 3 – che prevede che lo sviluppo di sistemi e di modelli di intelligenza artificiale debba avvenire su dati e tramite processi di cui deve essere garantita e

Piazza Venezia, 11 - 00187 Roma
Tel. +39 06 69677.1
sali@gpdp.it
www.gpdp.it

vigilata la correttezza, l'attendibilità, la sicurezza, la qualità, l 'appropriatezza e la trasparenza, secondo il principio di proporzionalità in relazione ai settori nei quali sono utilizzati – potrebbe essere opportuno, per completezza, richiamare anche i principi di integrità e riservatezza di cui all'articolo 5, par. 1, lett. f) del Regolamento (UE) 2016/679, *infra*: GDPR.

Articolo 4

Fermo quanto osservato s*upra*, all'articolo 4 – relativo ai "*Principi in materia di informazione e di riservatezza dei dati personali*" – potrebbe operarsi, al comma 2, un richiamo integrale ai principi di cui all'articolo 5 del GDPR, e non solo a quelli di liceità correttezza e trasparenza attualmente previsti (l'AI Act, in tal senso, richiama anche i princìpi di determinazione delle finalità, esattezza e limitazione della conservazione, sia pure in riferimento ai dati biometrici a scopo di identificazione: considerando n. 94).

Inoltre, si ribadisce l'opportunità, già sottolineata, di integrare il comma 4, relativo alla legittimazione del minore, con il riferimento a misure idonee a garantire sistemi adeguati di verifica dell'età, in analogia con l'articolo 13-bis, comma 3, d.l. n. 123 del 2023, convertito, con modificazioni, dalla l. n. 159 del 2023. La previsione di adeguati sistemi di *age-verification* è quantomai necessaria in considerazione della presumibile vulnerabilità dei soggetti minori e della potenziale pervasività dei sistemi in questione.

Articolo 6

L'articolo 6 sottrae, all'ambito applicativo della legge, le attività di ricerca, sviluppo, sperimentazione, uso di sistemi di intelligenza artificiale a fini di sicurezza nazionale, da parte degli Organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124 e dall'Agenzia per la cybersicurezza nazionale.

In particolare il comma 1 specifica il novero di soggetti per i quali vale l'esclusione, tra cui rientrano ora anche le Forze di polizia per le attività *"dirette a prevenire e contrastare, ai fini della sicurezza nazionale, i reati di cui all'articolo 9, comma 1, lettera b) e lettera b-ter) della legge n. 146 del 2006*" (di ratifica ed esecuzione a Convenzione e Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale).

Di contro, la norma ribadisce l'applicabilità del regime normativo speciale previsto dall'articolo **58** del d.lgs. 196 del 2003 e s.m.i. (cui, per l'Agenzia, rinvia l'articolo 13 del decreto legge 14 giugno 2021, n. 82) ai trattamenti svolti dagli Organismi e sottesi a tali utilizzi. Tuttavia, in ragione dell'estensione dell'esimente operata in prima lettura, sarebbe opportuno precisare che ai trattamenti svolti dalle forze di polizia in relazione a sistemi di i.a. funzionali alla sicurezza nazionale si applica, parimenti, il regime di cui al comma 2 del citato art. 58.

Articolo 8

L'articolo 8 ("*Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario"),* seppur modificato rispetto al testo originario sottoposto all'attenzione del Garante, presenta ancora taluni profili di criticità e necessiterebbe, pertanto, di alcune modifiche.

Al di là dell'assenza, al comma 1 degli elementi di cui agli articoli 6, par. 3, del GDPR e 2-sexies del d.lgs. 196 del 2003 e dell'indeterminatezza della disposizione[1], sarebbe opportuno integrare il comma 2, che autorizza sempre il trattamento secondario dei dati, anche particolari, in forma pseudonimizzata, salvo che "*la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute*". Nel rispetto del principio di autodeterminazione informativa del paziente, esso andrebbe integrato con la previsione del rilascio, per tale eventualità, di un esplicito consenso da parte degli interessati (cfr. anche i documenti internazionali in materia di ricerca in campo medico, biomedico ed epidemiologico e il divieto di trattamento dei dati personali raccolti a fini di ricerca per scopi diversi: art. 105 del d.lgs. 196 del 2003).

Riguardo al comma 3, il riferimento, introdotto in prima lettura, alla possibilità di trattamento per fini di anonimizzazione, pseudonimizzazione e sintetizzazione, volto allo studio e alla ricerca sui gesti atletici, sui movimenti e sulle prestazioni nell'attività sportiva in tutte le sue forme andrebbe circondato da maggiori garanzie (anche ad esempio per quanto riguarda i minori). .

Con riferimento al comma 5, la previsione dell'obbligo di comunicazione al Garante dei trattamenti di cui ai commi 1 e 2 della disposizione potrebbe ingenerare aspettative di legittimità dei trattamenti medesimi qualora l'Autorità non adotti un provvedimento di blocco (da intendersi, verosimilmente, come limitazione ex art. 58, par. 2, lett. f) del GDPR) nei successivi 30 giorni. La disposizione, pertanto, andrebbe modificata - come già rilevato nel parere sul ddl- chiarendo che l'avvenuta comunicazione, o la decorrenza del termine di 30 giorni in assenza di misure inibitorie non consuma i poteri (di controllo ed, eventualmente, sanzionatori) dell'Autorità.

Restano impregiudicate, infine, le esigenze di modifica/integrazione già indicate dal Garante nel parere del 2 agosto 2024, con riguardo, tra l'altro, a: i requisiti di determinatezza di cui agli articoli 6, par. 3, lett. b), 9, par. 2, lett. g) del GDPR e 2-sexies del d.lgs. 196 del 2003; le garanzie di cui all'articolo 89 del GDPR; la sostituzione della locuzione "dati privi di elementi identificativi diretti" con quella di "dati pseudonimizzati"; la soppressione del riferimento alla possibilità di assolvere l'obbligo di informativa in forma generale.

Articolo 9

L'articolo, introdotto in prima lettura, demanda a un decreto del Ministro della salute, sentito anche il Garante, la disciplina del trattamento dei dati personali, anche particolari, con il "massimo delle modalità semplificate consentite dal Regolamento", per finalità di ricerca e sperimentazione anche tramite sistemi di intelligenza artificiale e *machine learning*, inclusi la costituzione e l'utilizzo

[1] In ordine all'individuazione dei trattamenti, alle fonti dei dati particolari, all'assenza di distinzione tra ricerca scientifica volta alla realizzazione di sistemi di intelligenza artificiale e quella volta alla creazione di modelli di base, alla mancata precisazione del carattere qualificato dei ricercatori operanti, alla formulazione non chiara del comma 3 in ordine alla pseudonimizzazione.

di spazi speciali di sperimentazione a fini di ricerca, anche mediante l'uso secondario dei dati personali.

In ragione della natura non regolamentare dell'atto cui si rinvia, è opportuno circoscrivere meglio l'ambito applicativo della norma con l'indicazione, in particolare, dell'ambito di applicazione soggettivo e oggettivo (sistemi informativi). E' inoltre opportuno integrare l'oggetto dell'atto con riguardo a caratteristiche essenziali del trattamento, quali le operazioni e alle modalità di trattamento, al periodo di conservazione dei dati.

Articolo 10

L'articolo 10 reca disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale, rinviando a uno o più decreti del Ministro della salute, di concerto con altri enti, la disciplina delle soluzioni di IA aventi funzione di supporto alle finalità del FSE (diagnosi, cura e riabilitazione; prevenzione; profilassi internazionale; studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria). Tale/i decreto/i dovra(nno) anche individuare i soggetti che, nell'esercizio delle proprie funzioni, accedono alle soluzioni di IA e le relative modalità.

In ragione della rilevanza degli atti, ne andrebbe prevista la sottoposizione a parere del Garante. Andrebbe inoltre chiarito – al fine, eventualmente, di coordinarne il testo con la disciplina dell'Ecosistema dati sanitari − se le soluzioni di IA previste dalla disposizione a supporto del FSE elaborino, come l'EDS, i dati ivi contenuti. Tale circostanza renderebbe opportuno riflettere sulla possibilità di demandare allo stesso EDS la funzione di elaborazione dei dati del FSE anche attraverso l'IA, per rendere più coerente il quadro regolatorio in materia di sistemi di sanità digitale.

Per quanto attiene alla prevista istituzione di una piattaforma di IA per finalità di cura (la cui progettazione, realizzazione, messa in servizio e titolarità è attribuita all'Agenzia nazionale per la sanità digitale-AGENAS) ne andrebbe chiarito il rapporto con la Piattaforma nazionale di intelligenza artificiale di cui all'art. 12, c.15-undecies, lett., g) del dl 179 del 2012, parimenti affidata ad Agenas. Anche in tal caso, per garantire coerenza con l'attuale configurazione dei sistemi di sanità digitale ed evitare duplicazioni di banche dati, sarebbe auspicabile che le funzioni di tale piattaforma siano ricondotte a quelle già previste per l'EDS specificando che potranno essere assolte anche attraverso soluzioni di intelligenza artificiale al momento non previste in EDS.

Suscita perplessità, inoltre, l'attribuzione della titolarità dei trattamenti effettuati attraverso la piattaforma a un ente strumentale quale AGENAS anziché al Dicastero cui il trattamento è complessivamente imputabile e che dispone dei correlati poteri provvedimentali e, *lato sensu*, decisori.

Articolo 11

Per quanto attiene al settore del lavoro, l'articolo 11 individua, al comma 1, le finalità per le quali i sistemi di IA possono essere utilizzati in tale ambito (miglioramento delle condizioni di lavoro; tutela dell'integrità psicofisica dei lavoratori; accrescimento della qualità delle prestazioni professionali e della produttività delle persone). Al fine di allinearne il testo alle previsioni dell'AI ACT (considerando n. 44; art. 5(1)f), potrebbe risultare opportuno prevedere anche i casi in cui tale tecnologia non possa essere, invece, utilizzata, perché vietata (ad esempio, per la rilevazione dello stato emotivo delle persone in situazioni relative al luogo di lavoro).

Appare poi necessario richiamare esplicitamente le garanzie previste dagli articoli 22, par. 3, e 88 del GDPR – queste ultime espressamente dedicate ai rapporti di lavoro −, nonché gli articoli 113 e 114 del d.lgs. 196 del 2003 per i trattamenti di dati personali funzionali ai sistemi di IA utilizzati in tale specifico contesto.

Inoltre, il richiamo all'articolo 1-bis del d.lgs. 26 maggio 1997, n. 152 e s.m.i. dovrebbe essere concepito come non esaustivo, dal momento che si riferisce ai soli trattamenti interamente automatizzati.

Come già rilevato, sarebbe inoltre auspicabile chiarire che le garanzie introdotte dalla disposizione si applicano anche alla fase preassuntiva, in ragione dell'ampio uso che potrebbe essere fatto dei sistemi di IA a fini di selezione del personale.

Articolo 16

L'articolo 16 (Delega al Governo in materia di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale), introdotto al Senato, reca la delega al Governo all'adozione di uno o più decreti legislativi per definire la disciplina organica relativa all'utilizzo dei dati, algoritmi e metodi matematici per l'addestramento di sistemi di IA.

In particolare, in linea con i principi e criteri direttivi di cui al comma 3, dell'articolo 16, il legislatore delegato è chiamato, in primo luogo, a individuare le ipotesi per le quali appare necessario dettare il regime giuridico dell'utilizzo dei dati, algoritmi e metodi matematici per l'addestramento dei sistemi di IA, nonché i diritti e gli obblighi gravanti sulla parte che intenda procedere al suddetto utilizzo (lett. a).

Al riguardo, sarebbe opportuno – come già rilevato per l'articolo 4 del disegno di legge – prevedere che il trattamento dei dati osservi adeguate garanzie, nel rispetto della disciplina nazionale ed europea.

CAPO III - Articolo 19

L'articolo 19 (*Strategia nazionale per l'intelligenza artificiale*) demanda la predisposizione e l'aggiornamento della strategia nazionale per l'IA – che deve tener conto dei princìpi del diritto internazionale umanitario, al fine di sviluppare e promuovere sistemi di IA che tutelino i diritti umani − alla struttura della Presidenza del Consiglio dei Ministri competente per l'innovazione tecnologica e la transizione digitale, sentiti, per i profili di competenza, il Ministro per il made in Italy, il Ministro della difesa e il Ministro dell'università e della ricerca, d'intesa con le Autorità nazionali per l'IA.

Il coordinamento e il monitoraggio dell'attuazione della strategia nazionale per l'intelligenza artificiale sono demandati alla stessa Presidenza del Consiglio dei Ministri, che si avvale della collaborazione dell'AgID e dell'ACN, sentite Banca d'Italia, CONSOB e IVASS in qualità di autorità di vigilanza del mercato.

La disposizione, pur se modificata in prima lettura, non tiene conto della proposta di prevedere il parere (anche) del Garante sulla Strategia nazionale per l'IA. La previa consultazione dell'Autorità ai sensi dell'articolo 57, p.1, lett. c), del Regolamento potrebbe, infatti, evitare possibili contrasti tra le misure e politiche delineate con la disciplina di protezione dei dati, garantendone la complessiva coerenza con il quadro normativo di riferimento.

Articolo 20

L'articolo 20 (Autorità nazionali per l'intelligenza artificiale) designa quali Autorità nazionali per l'IA l'Agenzia per l'Italia digitale (AgID) e l'Agenzia per la cybersicurezza nazionale (ACN), con il compito di promuovere l'innovazione e lo sviluppo dell'IA, definire le procedure e a esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di IA, secondo quanto previsto dalla normativa nazionale e dell'Unione europea (comma 1).

Le due Autorità vengono altresì designate, rispettivamente, quale autorità di notifica e quale autorità di vigilanza del mercato e punto di contatto unico con le istituzioni dell'Unione europea ai sensi dell'articolo 70 del regolamento (UE) 2024/1689 (comma 2), mentre il coordinamento delle Autorità nazionali per l'IA con gli altri soggetti pubblici (ivi comprese le autorità indipendenti), viene affidato a un apposito Comitato, cui partecipano, per le questioni di rispettiva competenza, i rappresentanti di vertice della Banca d'Italia, della CONSOB e dell'IVASS.

L'articolo non tiene conto delle indicazioni dell'Autorità relativamente alla necessità di chiarirvi– per esigenze di conformità al quadro normativo unionale – il ruolo del Garante stesso quale autorità indipendente, ai sensi degli artt. 8 CDFUE e 16 TFUE, per la protezione dei dati personali: diritto, appunto, fondamentale, le cui istanze di tutela si sovrappongono pressoché costantemente con l'applicazione dei sistemi di IA.

Come già previsto dal parere, dunque, sarebbe opportuno perfezionare l'articolo, estendendo più esplicitamente al comma 4, la clausola di salvaguardia delle funzioni del Garante anche alle norme del disegno di legge che abbiano implicazioni in termini di protezione dei dati e prevedendo, al comma 3, la partecipazione del Garante al Comitato di coordinamento, per realizzare pienamente quella leale cooperazione tra autorità competenti prevista dall'AI Act. Declinando in maniera più articolata le implicazioni di tale cooperazione, è inoltre opportuno integrare l'articolo prevedendo, infine, che l'AgID e l'ACN trasmettano al Garante gli atti dei procedimenti in relazione ai quali emergano profili suscettibili di rilevare in termini di protezione dati, richiedendo altresì il parere dell'Autorità rispetto a fattispecie, al loro esame, che coinvolgano aspetti di protezione dei dati. Il Garante trasmetterà, per parte sua, elementi informativi in ordine a profili di competenza dell'AgID o dell'ACN suscettibili di emergere nella trattazione dei propri procedimenti.

Articolo 24

L'articolo 24 (Deleghe al Governo in materia di intelligenza artificiale) conferisce al Governo una delega legislativa (da esercitarsi previo parere del Garante) per l'adeguamento della normativa interna al regolamento (UE) 2024/1689. La disposizione, modificata in Senato, prevede ora tra i princìpi e criteri direttivi: 1) l'attribuzione all'AgID e all'ACN di tutti i poteri di vigilanza, ispettivi e sanzionatori previsti dall'AI ACT; 2) modifiche alla normativa vigente, inclusa quella in materia di servizi bancari, finanziari, assicurativi e di pagamento, per il corretto e integrale adeguamento all'AI ACT; 3) rinvio alla disciplina secondaria adottata dall'AgID e dall'ACN nell'ambito e per le finalità specificamente previste dall'AI ACT e dalla normativa attuativa; 4) attribuzione alle medesime autorità del potere di imporre le sanzioni e le altre misure amministrative previste dall'articolo 99 del regolamento (UE) 2024/1689.

Un'ulteriore delega concerne poi l'adozione di decreti legislativi volti ad adeguare e specificare la disciplina dei casi di realizzazione e di impiego illeciti di sistemi di intelligenza artificiale (comma 3) rispetto ai quali – allineando la disposizione al primo comma – sarebbe opportuno prevedere il parere del Garante.

Sarebbe opportuno, inoltre, integrare l'articolo con la previsione, al comma 2, di criteri direttivi specifici (già suggeriti dal Garante) relativi: a) alla disciplina dell'autorizzazione di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per finalità di polizia, indicando l'autorità competente all'effettuazione di tale vaglio autorizzativo ai sensi dell'articolo 5, par. 3, dell'AI ACT; b) alla designazione del Garante quale autorità competente ai fini di cui all'articolo 74, par. 8, dell'AI ACT, con la relativa disciplina delle procedure di coordinamento con le Autorità designate ai sensi dell'articolo 18 del disegno di legge; c) all'adeguato coinvolgimento del Garante nella realizzazione degli spazi di sperimentazione normativa.

Si segnala, inoltre, l'opportunità di integrare i criteri di delega, introdotti in prima lettura, relativi all'uso dell'i.a. nelle indagini preliminari (" *nel rispetto delle garanzie inerenti al diritto di difesa e ai dati personali dei terzi, nonché dei principi di proporzionalità, non discriminazione e trasparenza*") e per l'attività di polizia, così da rendere maggiormente determinato l'esercizio delle relative deleghe legislative.

Piazza Venezia, 11 - 00187 Roma
Tel. +39 06 696771
sali@gpdp.it
www.gpdp.it