OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Settembre 2024

Settembre 2024

I principali aggiornamenti in materia di TMT & Data Protection del mese.

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

Provvedimenti del Garante Privacy

- Dal Garante Privacy sanzione di 5 mln di euro a un fornitore di luce e gas [Link]
- Design ingannevole, indagine internazionale: ancora troppi ostacoli per gli utenti [Link]
- Giornalismo: Garante, no ai dettagli che violano la riservatezza dei minori [Link]
- D.lgs. resilienza dei soggetti critici, ok del Garante ma più tutela per la privacy [Link]

EDPB

- EDPB to work together with European Commission to develop guidance on interplay GDPR and DMA [Link]
- 95th Plenary meeting [Link]

AGCOM

- Agcom avvia il procedimento istruttorio di analisi dei mercati dei servizi di accesso alla rete fissa [Link]
- Rapporto annuale sull'applicazione del Regolamento (UE) 2019/1150 in materia di platform to business ("Report P2B 2024"), approvato dal Consiglio dell'Autorità il 24 luglio 2024 [Link]

Il ruolo cruciale delle autorità di protezione dei dati personali nell'ambito dell'AI Act: le raccomandazioni dell'EDPB

L'*European Data Protection Board* ("**EDPB**") con la Dichiarazione 3/2024 (la "**Dichiarazione**") ha espresso il proprio parere in merito al ruolo delle autorità di protezione dei dati personali ("**DPA**") nel nuovo quadro regolatorio previsto dal Regolamento (UE) 1689/2024 ("**AI Act**").

Richiamando il Parere Congiunto 5/2021 rilasciato dall'EDPB e dall'*European Data Protection Supervisor* ("**EDPS**"), l'EDPB sottolinea la necessità di attribuire un ruolo centrale alle DPA nella *governance* dell'AI Act, riconoscendo l'esperienza e le competenze dalle stesse maturate in materia di trattamento dei dati personali connessi ai sistemi di intelligenza artificiale ("**IA**").

L'EDPB, dopo aver chiarito il contesto e lo scopo della Dichiarazione, conclude con alcune raccomandazioni in merito al ruolo delle DPA nel contesto dell'AI Act.
Ma perché, a parere dell'EDPB, dovrebbe essere riconosciuto un ruolo cruciale alle DPA nella *governance* dell'AI Act?

Il sistema di governance dell'AI Act

Per comprendere appieno la Dichiarazione dell'EDPB, è fondamentale delineare brevemente il funzionamento del sistema di *governance* istituito dall'AI Act. In considerazione della complessità e della trasversalità dei sistemi di IA, il legislatore europeo ha previsto un articolato sistema di organi e uffici, sia a livello europeo che nazionale, a cui demandare le attività di *governance*.

Tali attività vengono descritte nel Capo VII dell'AI Act, la cui applicazione è prevista a partire dal **2 agosto 2025**. Nello specifico, a livello europeo l'AI Act individua i seguenti enti (artt. 64-69 dell'AI Act):

- l'**Ufficio per l'IA**, incaricato di sviluppare le competenze e le capacità dell'Unione nel settore dell'IA;
- il **Consiglio per l'IA**, che fornisce consulenza e assistenza alla Commissione europea (la "**Commissione**") e agli Stati membri al fine di agevolare l'applicazione coerente ed efficace dell'AI Act;
- il ***forum* consultivo**, il cui scopo è offrire consulenza e competenze tecniche al Consiglio per l'IA e alla Commissione, contribuendo alle loro funzioni; e
- il **gruppo di esperti scientifici indipendenti**, finalizzato a sostenere le attività di esecuzione dell'AI Act.

A livello nazionale, ciascuno Stato membro deve istituire o designare **almeno un'autorità di notifica** e **almeno un'autorità di vigilanza del mercato** (*Market surveillance authority(ies)* – "**MSA**") come autorità nazionali competenti. Inoltre, gli Stati membri devono designare una MSA che funge da **punto di contatto unico** per l'AI Act (art. 70, par. 2, dell'AI Act).

In particolare, in Italia, lo schema di disegno di legge sull'IA approvato lo scorso 23 aprile dal Consiglio dei Ministri ("**DDL IA**" – per un maggior approfondimento sul tema, si veda il nostro precedente contributo, disponibile qui, in inglese), individua:

- l'**Agenzia per l'Italia digitale** ("**AgID**"), incaricata di promuovere l'innovazione e lo sviluppo dell'IA, definire le procedure, nonché 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;

- l'**Agenzia per la cybersicurezza nazionale** ("**ACN**"), responsabile della vigilanza dei sistemi di IA e della promozione e sviluppo dell'IA per quanto concerne i profili di cybersicurezza.

Per assicurare il coordinamento e la collaborazione con le altre pubbliche amministrazioni e autorità indipendenti, nonché tra AgID e ACN, il DDL IA prevede che venga istituito un **Comitato di coordinamento**, composto dai direttori generali delle due Agenzie e dal Capo del dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri.

Il DDL IA preserva inoltre i compiti, i poteri e le competenze del **Garante per la protezione dei dati personali**.
Infine, all'art. 22, il DDL AI affida al Governo il compito di designare le autorità nazionali competenti, tra cui la MSA, l'autorità di notifica e il punto di contatto con le istituzioni dell'Unione europea.

Contesto e scopo della Dichiarazione

L'EDPB chiarisce che l'AI Act e la disciplina comunitaria in materia di protezione dei dati personali – ovvero il Regolamento (UE) 679/2016 ("**GDPR**"), il Regolamento (UE) 1725/2018 ("**EUDPR**"), la Direttiva (UE) 680/2016 ("**LED**")[1] e la Direttiva 58/2002/CE ("**Direttiva ePrivacy**") (complessivamente intese come "**Normativa Privacy**") – devono essere considerati e interpretati come **strumenti complementari**, in grado di rafforzarsi reciprocamente. In particolare, l'AI Act mira a garantire la protezione dei diritti fondamentali alla privacy e alla protezione dei dati personali, conformemente agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

Il trattamento di dati personali coinvolge, infatti, l'intero ciclo di vita dei sistemi di IA, specialmente se si tratta di sistemi di IA ad alto rischio. L'EDPB sottolinea che il trattamento "*è chiaramente (e continuerà ad essere) un elemento centrale delle diverse tecnologie coperte della definizione di IA*", prevista dall'art. 3, par. 1, dell'AI Act. Per tale motivo, alcune DPA si sono già attivate e l'EDPB ha seguito da vicino l'*iter* legislativo dell'AI Act, vista la sua "*multiforme interazione*" con la Normativa Privacy.

Gli Stati membri possono designare qualsiasi ente come autorità di notifica e MSA per controllare l'applicazione e l'attuazione dell'AI Act. Tuttavia, l'EDPB suggerisce che la nomina della DPA come MSA garantirebbe un migliore coordinamento tra le diverse autorità di regolamentazione, rafforzerebbe la certezza del diritto per tutte le parti interessate e migliorerebbe la vigilanza e l'applicazione sia della legge sull'IA che della Normativa Privacy.

L'EDPB basa queste affermazioni su diversi elementi:

- le DPA, oltre che nelle tecnologie dell'IA, sono **esperte** in molti ambiti elencati dall'art. 70, par. 3, dell'AI Act, quali quello

[1] L'EUDPR prevede le regole applicabili al trattamento dei dati personali da parte delle istituzioni, degli organismi, degli uffici e delle agenzie dell'Unione europea in linea con gli standard di protezione dei dati prescritti dal GDPR. La LED riguarda invece la tutela dei dati personali usati dalla polizia e dalle autorità di giustizia penale.

dell'elaborazione dei dati e della sicurezza dei dati, nonché nella valutazione dei rischi per i diritti fondamentali posti dalle nuove tecnologie;

- le DPA sono pienamente **indipendenti** e soddisfano i requisiti di cui all'art. 70, par. 1, dell'AI Act, che prevede che le autorità nazionali competenti devono poter esercitare i loro poteri in modo indipendente, imparziale e senza pregiudizi;

- ai sensi dell'art. 74, par. 8, dell'AI Act, per i **sistemi di IA ad alto rischio** operanti nel settore della biometria e utilizzati per attività di contrasto, gestione delle frontiere, giustizia e democrazia, nonché per quelli operanti nei settori dell'attività di contrasto, della migrazione, asilo e gestione del controllo delle frontiere, nonché dell'amministrazione della giustizia di cui Allegato III dell'AI Act, gli Stati membri devono designare le DPA come MSA;

- qualora le istituzioni, gli organi e gli organismi dell'Unione rientrino nell'ambito di applicazione dell'AI Act, l'**EDPS** deve poter agire come autorità competente per la loro vigilanza (art. 70, par. 9 dell'AI Act);

- esiste uno **stretto legame tra la valutazione d'impatto sulla protezione dei dati**, prevista dall'art. 35 del GDPR e la **valutazione d'impatto sui diritti fondamentali**, prevista dall'art. 27 dell'AI Act.

Le raccomandazioni dell'EDPB

1. Designazione delle DPA come MSA per sistemi di IA ad alto rischio

L'EDPB raccomanda agli Stati membri di considerare la nomina delle DPA come MSA anche per i sistemi di IA ad alto rischio operanti nei settori elencati nell'Allegato III dell'AI Act, diversi da quelli specificati nell'art. 74, par. 8, dell'AI Act. Tali settori includono infrastrutture critiche, istruzione e formazione professionale, occupazione, gestione dei lavoratori e accesso al lavoro autonomo, accesso a servizi privati essenziali e a prestazioni e sevizi pubblici essenziali.

Questa raccomandazione è particolarmente rilevante nei casi in cui tali sistemi siano in grado di impattare sui diritti e sulle libertà degli interessati in relazione al trattamento dei dati personali, escludendo quei settori dove l'AI Act prevede come obbligatoria la nomina di un'autorità specifica (ad esempio, per il settore finanziario, dove la MSA è l'autorità nazionale pertinente responsabile della vigilanza finanziaria di tali enti – art. 74, par. 6, dell'AI Act).

2. Designazione delle DPA come punto di contatto unico

Secondo l'EDPB, le DPA, in qualità di MSA, dovrebbero essere designate quale punto di contatto unico per il pubblico e per le controparti degli altri Stati membri e dell'Unione. Questo consentirebbe di avere un approccio unificato, coerente ed efficace nei diversi settori di applicazione dell'IA.

3. Dotazione di risorse umane e finanziarie aggiuntive

La designazione delle DPA come MSA implica l'assegnazione di nuovi poteri e funzioni, che richiedono l'assegnazione di risorse umane e finanziarie aggiuntive. L'EDPB sottolinea l'importanza di fornire alle DPA le risorse

necessarie per svolgere efficacemente i nuovi compiti assegnati.

4. Cooperazione tra tutte le autorità coinvolte e procedure chiare

Da ultimo, l'EDPB insiste sulla necessità di promuovere e stabilire un'adeguata ed efficace cooperazione tra tutte le autorità coinvolte nel rispetto del **principio di leale cooperazione**, sancito dall'art. 4, par. 3, del Trattato dell'Unione europea, come richiamato dalla Corte di Giustizia dell'Unione europea [2], adottando a tal fine procedure chiare.
Tale cooperazione non riguarda solo le DPA, ma dovrebbe avvenire anche tra le DPA e la Commissione e l'Ufficio dell'IA.

Le considerazioni finora svolte, secondo l'EDPB, si applicano in maniera analoga anche ai **modelli di IA ad uso generale** (*general purpose AI models* – "**GPAI**"), i quali potrebbero essere addestrati su dati personali e i cui *output* sono in grado di influire sui diritti alla privacy e alla protezione dei dati personali. L'EDPB sottolinea infatti come nell'AI Act non è stabilita una chiara coordinazione tra l'Ufficio dell'IA e le DPA e/o l'EDPB. Al contrario, un coordinamento è in questi casi indispensabile ogni qual volta un modello o sistema GPAI comporti il trattamento di dati personali, ricadendo automaticamente sotto la supervisione delle DPA e dell'EDPS (quando rientra nell'ambito dell'EUDPR).

Conclusioni

La Dichiarazione dell'EDPB pone in evidenza la necessità di attribuire un ruolo centrale alle DPA all'interno del nuovo quadro regolatorio previsto dall'AI Act. Riconoscendo l'esperienza e le competenze acquisite dalle DPA in materia di trattamento dei dati personali, l'EDPB ritiene che tali autorità siano le più indicate per garantire una supervisione efficace e coordinata dei sistemi di IA, specialmente se si tratta di sistemi ad alto rischio.

L'integrazione delle DPA nel sistema di *governance* dell'AI Act rappresenta non solo una scelta logica ma anche una misura essenziale per assicurare la protezione dei diritti fondamentali alla privacy e alla protezione dei dati personali. In un contesto in cui l'IA gioca un ruolo sempre più pervasivo, il riconoscimento delle DPA come pilastri della vigilanza e dell'applicazione normativa non solo rafforza la protezione dei dati personali, ma assicura anche un'applicazione coerente ed efficace delle norme europee. L'EDPB invita dunque gli Stati membri e le istituzioni dell'Unione a considerare attentamente queste raccomandazioni per realizzare un sistema di *governance* dell'IA che sia al contempo robusto, coordinato e rispettoso dei diritti fondamentali.

* * *

Dark patterns e privacy: il rapporto Sweep 2024 del GPEN rivela le strategie ingannevoli delle piattaforme digitali

*Il Global Privacy Enforcement Network ("**GPEN**") ha pubblicato il rapporto dello Sweep 2024 ("**Sweep**") incentrato sui Deceptive Design Patterns ("**DDPs**"), noti anche come "dark patterns" (o modelli di progettazione ingannevoli), riscontrati nei siti web e nelle app mobile.*

[2] CGUE, sentenza del 4 luglio 2023, Meta Platforms e altri.

L'obiettivo è quello di analizzare come le scelte di design delle piattaforme digitali siano in grado di influenzare, manipolare o costringere gli utenti a prendere decisioni contrarie ai loro interessi, specialmente con riferimento alla loro privacy.

Ma cos'è il GPEN e cosa è emerso durante lo Sweep?

Il GPEN – creato nel 2010 prendendo spunto da una raccomandazione[3] dell'Organizzazione per la cooperazione e lo sviluppo economico ("**OCSE**") – rappresenta una rete informale di Autorità di controllo e di altre parti interessate, per discutere gli aspetti pratici della cooperazione in materia di applicazione delle normative sulla protezione dei dati.
Il GPEN coordina il c.d. Privacy Sweep, ovvero un'indagine conoscitiva che, per l'anno 2024, si è incentrata sui ***dark patterns***.

Con la definizione di "*dark pattern*" vengono indicate quelle interfacce e quei percorsi di navigazione progettati per influenzare l'utente affinché intraprenda azioni inconsapevoli o non desiderate – e potenzialmente dannose dal punto della privacy del singolo – ma favorevoli all'interesse della piattaforma o del gestore del servizio.

Detti anche "modelli di progettazione ingannevoli", i *dark pattern* mirano dunque a influenzare il nostro comportamento e possono ostacolare la capacità di proteggere efficacemente i nostri dati personali[4].

Lo Sweep, svoltosi dal 29 gennaio al 2 febbraio 2024, ha visto la partecipazione di 26 Autorità di controllo, tra cui l'Autorità Garante per la protezione dei dati personali ("**Garante Privacy**"). Per la prima volta, lo Sweep di quest'anno si è svolto in collaborazione con l'*International Consumer Protection and Enforcement Network*, evidenziando l'importanza dei DDPs sia sotto il profilo della tutela dei dati personali che di quella dei consumatori, questioni fondamentali nell'ambito dell'economia digitale.

La metodologia seguita

L'obiettivo perseguito dallo Sweep è stato quello di chiedere ai partecipanti (cd. "*Sweepers*") di replicare l'esperienza degli utenti/consumatori, interagendo con siti *web* e app *mobile* al fine di valutare le modalità con cui questi gestiscono le scelte sulla privacy, acquisiscono il consenso informato degli utenti/consumatori e gestiscono le procedure di *log-out* e cancellazione degli *account*.

L'analisi dei siti *web* e delle app è stata condotta sulla base di un questionario strutturato su cinque indicatori chiave, ritenuti rilevanti sia dalla normativa privacy che dalla normativa consumeristica, e derivanti dalla tassonomia dei *dark patterns* dell'OCSE[5]:

1. linguaggio complesso e confuso (*complex and confusing language*): DDP che connota la presenza di informative privacy eccessivamente lunghe o che utilizzano un linguaggio troppo tecnico o complicato per l'utente medio. In tali circostanze, gli utenti tendono a non leggere o a non comprendere pienamente il contenuto dell'informativa, rischiando così di adottare decisioni potenzialmente non conformi alle loro reali preferenze in materia di privacy.

[3] Raccomandazione del 12 giugno 2007 sulla cooperazione transfrontaliera nell'attuazione di normative in materia di privacy.
[4] Il 24 febbraio 2023, il Comitato europeo per la protezione dati (EDPB) ha pubblicato le linee guida su come riconoscere ed evitare questi sistemi. Il documento offre raccomandazioni pratiche a gestori dei social media, a designer e utenti su come comportarsi di fronte a queste interfacce che si pongono in violazione del Regolamento europeo in materia di protezione dati. Cfr. Linee Guida 3/2022, "*Dark patterns in social media platform interfaces: how to recognize and avoid them*".
[5] "*Dark commercial Patterns*", OECD Digital economy papers, Ottobre 2022, n. 336.

2. Interferenza dell'interfaccia (*interface interference*): uso di elementi di *design* e metodi di presentazione che alterano la percezione e il processo decisionale degli utenti in merito alle opzioni sulla privacy. Rientrano in questa categoria diverse tipologie di DDPs, quali:

- **falsa gerarchia** (*false hierarchy*): vengono messi in risalto alcuni elementi oscurandone altri, incanalando così gli utenti verso opzioni meno tutelanti per la loro privacy (ad esempio, quando nella *cookie policy* l'opzione "*accetta tutti i cookie*" presenta un colore diverso, più acceso, risultando, dunque, in evidenza);

- **preselezione** (*preselection*): vengono preselezionate di *default* opzioni più invasive per la privacy;

- ***confirm-shaming***: viene utilizzato un linguaggio emotivo in modo da far propendere gli utenti verso le opzioni preferite dalla piattaforma (ad esempio: "*sei sicuro di voler cancellare il tuo account? Sarebbe un peccato vederti andar via!*").

3. Fastidio (*nagging*): tecnica con cui i siti *web* e le app invitano ripetutamente gli utenti a compiere un'azione specifica (ad esempio, rivedere i propri dati sulla privacy o accedere al proprio *account*) a favore degli scopi dell'organizzazione. Tali richieste ripetute e assillanti interrompono l'esperienza dell'utente e possono incoraggiarlo a cedere alle richieste pur di evitare il "fastidio" di ulteriori sollecitazioni.

4. Ostruzione (*obstruction*): consiste nell'inserire ulteriori passaggi (c.d. *click fatigue*) tra gli utenti e i loro obiettivi, dissuadendoli o rendendoli meno motivati a compiere le scelte legate alla privacy (ad esempio, con riguardo alle preferenze sui *cookie*) che invece avrebbero intrapreso. Tale tecnica può essere molto efficace perché sfrutta il tempo, l'attenzione e/o la disponibilità limitata degli utenti a navigare su siti *web* e app.

5. Azione forzata (*forced action*): questo tipo di DDPs costringe gli utenti – o li inganna facendo credere che sia necessario – a fornire più dati personali del necessario (ad esempio, quando nella cookie policy è presente solo la voce "*accettare*" o "*accetta tutti i cookie*").

I risultati e le raccomandazioni del GPEN

Gli *Sweepers* hanno rilevato la presenza di DDPs nella maggior parte dei siti *web* e app esaminate, con il 97% dei casi contenenti almeno un *dark pattern*. Il DDP più frequentemente riscontrato è stato il "*complex and confusing language*". Infatti, l'89% delle informative privacy risultava eccessivamente lunga o caratterizzata da un linguaggio tecnico e complesso, ostacolando così l'effettiva comprensione da parte degli utenti.

Le Autorità di controllo hanno inoltre evidenziato la presenza di "*interface interference*" nel 43% dei casi e di "*obstruction*" nel 39%. Ad esempio, l'opzione per la cancellazione degli *account* era spesso difficilmente individuabile o richiedeva numerosi passaggi (*click*), mentre nel 55% dei casi non era prevista un'opzione diretta per la cancellazione dell'*account*.

Meno comuni, ma comunque presenti, sono stati i DDPs delle azioni fastidiose (pari al 14%) e forzate (pari al 21%).
In termini generali, il GPEN ha osservato che la maggior parte dei siti *web* e delle app risulta progettata per incentivare gli utenti a maturare decisioni in materia di privacy che non favoriscono i propri interessi, ma – al contrario – quelli delle piattaforme stesse.

Pertanto, al fine di mitigare l'impatto negativo dei *dark pattern*, il GPEN ha evidenziato diverse

azioni che le organizzazioni potrebbero attuare, anche in un'ottica di *accountability*, quali per esempio:

- semplificare le informative privacy per renderle più comprensibili agli utenti;
- progettare interfacce *web* e applicative che rispettino le scelte degli utenti;
- evitare il fenomeno della c.d. *click fatigue*;
- fornire opzioni semplici, chiare e immediate che permettano agli utenti di esprimere le proprie preferenze in materia di privacy.

Considerato quanto sopra, il GPEN ha evidenziato con chiarezza la pervasività dei *dark patterns* nelle piattaforme digitali e il loro impatto negativo sui diritti degli utenti, in particolare sulla loro capacità di prendere decisioni informate in materia di privacy. Con il 97% dei siti *web* e delle app esaminati che presentano almeno un DDP, emerge un quadro preoccupante in cui le scelte progettuali vengono spesso utilizzate per manipolare gli utenti, favorendo gli interessi delle piattaforme a discapito della tutela dei dati personali.

L'analisi condotta dal GPEN non solo sottolinea la necessità di interventi correttivi, ma offre anche raccomandazioni concrete per le organizzazioni per consentire loro di rispettare le scelte degli utenti e volte a evitare pratiche di progettazione ingannevoli.

In tale ottica – si comprende dalla lettura dello Sweep – si può ricorrere a tecniche di *legal design*, che, adottando una visione umano-centrica, garantiscono che le informazioni siano facilmente comprensibili, fruibili e accessibili a tutti.

Ma la normativa privacy non è l'unica ad attenzionare il tema dei *dark patterns*. Infatti, gli obblighi di trasparenza verso gli utenti e il divieto di utilizzo dei *dark patterns* trovano un'apposita disciplina anche nel D.Lgs. 206/2005 ("**Codice del Consumo**"), in base al quale i DDPs potrebbero configurarsi come omissioni ingannevoli (art. 22, co. 2, del Codice del Consumo) in quanto comportano l'occultamento o la presentazione ambigua di informazioni rilevanti.

Pertanto, come precisato anche dal GPEN, solo implementando pratiche di design orientate alla tutela della privacy, le organizzazioni potranno offrire agli utenti esperienze prive di indebite influenze, manipolazioni o coercizioni, rafforzando al contempo la fiducia dei consumatori e garantendo la conformità normativa alle disposizioni del GDPR e del Codice del Consumo.

* * *

Il parere del Garante Privacy sul DDL IA: modifiche essenziali per la conformità con il GDPR e l'AI Act

Nell'ambito dell'*iter* di approvazione dello schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale ("**DDL IA**"), adottato dal Consiglio dei Ministri il 23 aprile 2024, l'Autorità garante per la protezione dei dati personali (il "**Garante Privacy**"), ha espresso il proprio parere con provvedimento n. 477 del 2

agosto 2024, (il "**Parere**") ai sensi dell'art. 36, par. 4 del Regolamento (UE) 679/2016 ("**GDPR**").

Il DDL IA definisce norme e principi di natura programmatica, settoriale e promozionale, destinati a regolare la ricerca, la sperimentazione, lo sviluppo, l'adozione e l'applicazione di sistemi e modelli di IA (per un maggior approfondimento circa il contenuto del DDL IA si rimanda ad un nostro precedente contributo, disponibile qui, in inglese). Le norme intervengono in cinque ambiti: la strategia nazionale, le autorità nazionali, le azioni di promozione, la tutela del diritto d'autore, le sanzioni penali. Si prevede, inoltre, una delega al governo per adeguare l'ordinamento nazionale al Regolamento (UE) 1689/2024 ("**AI Act**").

Il Garante Privacy ha espresso un **parere favorevole** sul DDL IA, **condizionandolo** tuttavia all'introduzione di specifiche modifiche e integrazioni e all'osservazione relativa all'opportunità di riconoscere una **partecipazione più attiva del Garante** stesso all'interno del nuovo quadro normativo.

Ma in cosa consistono le raccomandazioni del Garante Privacy?

Di seguito, si riassumono le principali critiche mostrate dal Garante Privacy nei diversi settori trattati dal DDL IA.

1. Protezione dei dati personali

- **Coordinamento normativo**. La natura programmatica di molte disposizioni del DDL IA potrebbe porre il rischio di sovrapposizione con alcune norme dell'AI Act. Pertanto, con riguardo alla protezione dei dati personali, il Garante Privacy raccomanda di introdurre nel Capo I ("*principi e finalità*") del DDL IA un articolo specifico e ad applicazione trasversale che imponga un **vincolo generale di conformità al GDPR e al Codice Privacy** (D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018).

- **Privacy come diritto fondamentale**. Il Garante Privacy suggerisce di modificare l'art. 3, comma 1 del DDL IA, sostituendo il riferimento al "*principio di protezione dei dati personali*" con quello, più corretto, ai diritti fondamentali (art. 8 della Carta di Nizza).

- **Legittimazione del minore**. Il Garante Privacy rileva che dovrà essere riformulato l'art. 4, comma 4, del DDL IA facendo riferimento non alla soglia di età attualmente prevista per l'accesso dei minori alle tecnologie di IA (attualmente fissata a quattordici anni), ma piuttosto all'art. 2-*quinquies* del Codice Privacy. Tale rinvio mobile permetterebbe al DDL IA di essere costantemente allineato alla normativa vigente. Il Garante Privacy, inoltre, suggerisce di integrare la disposizione in esame prevedendo misure idonee a garantire sistemi efficaci di verifica dell'età, in modo da prevenire la facile elusione della soglia anagrafica prevista per il consenso.

2. Settore sanitario

- **Maggiori garanzie**. Il Garante Privacy ritiene insufficiente il generico richiamo alla protezione dei dati previsto dall'art. 7 del DDL IA e invita a un **richiamo diretto all'art. 10 dell'AI Act**. Quest'ultimo prevede, infatti, garanzie essenziali, non assorbite dall'art. 7 del DDL IA, quali, ad esempio, la preferenza circa l'uso di dati sintetici o anonimi, particolari limitazioni per l'uso di dati sanitari (divieto di trasmissione, trasferimento o

comunicazione), nonché la limitazione della conservazione.
Il richiamo all'art. 10 dell'AI Act dovrà essere aggiunto anche all'art. 9 del DDL IA (*Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale*).

- **Coordinamento normativo**. Il Garante Privacy ritiene che l'art. 8 del DDL IA, dedicato alla legittimazione del trattamento di dati personali per fini di ricerca nell'ambito dell'IA[6], necessita di modifiche per essere conforme da un lato, ai **requisiti di determinatezza** di cui agli artt. 6, par. 3, lett. b) e 9, par. 2, lett. g) del GDPR e 2-*sexies* del Codice Privacy, relativi alla necessità di prevedere una base giuridica chiara e specifica per il trattamento dei dati personali; dall'altro, con riferimento all'uso secondario dei dati, alle **garanzie di cui all'art. 89 del GDPR**, quali, ad esempio, la predisposizione di misure tecniche e organizzative al fine di garantire il rispetto del principio di minimizzazione dei dati. Il Garante Privacy ha altresì evidenziato la necessità di eliminare il riferimento alla **possibilità di assolvere l'obbligo di informativa in forma generale**, mediante pubblicazione sul sito *web* del titolare, considerandola non compatibile con l'uso secondario dei dati. Infine, la previsione della previa comunicazione al Garante Privacy del trattamento con un meccanismo di silenzio-assenso dovrebbe essere chiarita specificando che la decorrenza dei trenta giorni non fa venir meno i poteri di controllo (ed eventualmente sanzionatori) del Garante Privacy.

3. Settore giuslavoristico

- **Esigenze di tutela e non discriminazione**. Il Garante Privacy suggerisce di integrare l'art. 10 del DDL IA **richiamando gli artt. 22, par. 3 e 88 del GDPR e gli artt. 113 e 114 del Codice Privacy**, in modo da assicurare il rispetto delle garanzie necessarie per il ricorso all'IA nel settore giuslavoristico, ove sono particolarmente rilevanti le esigenze di tutela e non discriminazione, non solo nella fase successiva all'instaurazione del rapporto di lavoro, ma **anche in fase pre-assuntiva**, a fini di selezione del personale.

4. Ruolo del Garante Privacy nel contesto del DDL IA

- **Partecipazione più attiva del Garante Privacy** sia nella definizione della **strategia nazionale per l'IA** (art. 17 del DDL IA) in modo da evitare che le misure e le politiche delineate contrastino con la disciplina di protezione dei dati personali, sia nei lavori del **Comitato di coordinamento** (art. 18 del DDL IA[7]), con

[6] L'attuale formulazione dell'articolo prevede che il soggetto pubblico e privato senza scopo di lucro possano trattare dati personali se il trattamento è necessario per motivi di interesse pubblico (art. 9, lett. g) del GDPR) oppure se sono autorizzati all'utilizzo secondario di dati privi di identificati diretti (i.e. pseudonimizzati), previo parere favorevole del comitato etico e comunicazione al Garante Privacy della titolarità, del rispetto dei principi di *privacy by design* e *by default*, delle misure di sicurezza implementate, della valutazione d'impatto effettuata, nonché dell'elenco dei responsabili ex art. 28 del GDPR. Il Garante Privacy avrà poi un termine di 30 giorni per adottare eventuali misure inibitorie del trattamento.

[7] L'art. 18 del DDL IA individua l'Agenzia per l'Italia digitale e l'Agenzia per la cybersicurezza nazionale quali autorità nazionali competenti per l'IA. La norma, inoltre, al comma 2, istituisce il Comitato di coordinamento al fine di assicurare il coordinamento e la collaborazione tra le diverse autorità competenti.

obbligo per le altre autorità di consultare il Garante Privacy in caso di questioni relative alla protezione dei dati personali.

5. Delega legislativa per l'adeguamento dell'ordinamento interno all'AI Act

- **Adeguamento del DDL IA all'AI Act**. Il Garante Privacy ritiene che il comma 2 dell'art. 22 del DDL IA debba essere integrato con la previsione di criteri direttivi specifici riguardanti la disciplina dell'autorizzazione dei sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per finalità di polizia (art. 5, par. 3 e 5, dell'AI Ac [8]), suggerendo la designazione del **Garante Privacy quale autorità competente all'effettuazione di tale vaglio autorizzativo**, in virtù delle sue competenze consolidate nella regolamentazione dei processi decisionali algoritmici basati su dati personali.
  Inoltre, il Garante Privacy ha sottolineato l'importanza di **designare il Garante stesso quale autorità competente per i sistemi di IA ad alto rischio** operanti nel settore della biometria, soprattutto se utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia, oppure utilizzati dalle autorità di contrasto (art. 74, par. 8 dell'AI Act che richiama l'allegato III, punti 1 e 6 dell'AI Act).
- **Adeguato coinvolgimento del Garante Privacy**. Il Garante Privacy ha richiesto che sia previsto un suo coinvolgimento adeguato **nella realizzazione degli spazi di sperimentazione normativa** di cui all'art. 57 dell'AI Act e che lo stesso sia incluso tra le **autorità competenti alla tutela dei diritti fondamentali**, secondo quanto previsto dall'art. 77 dell'AI Act.

Il Parere del Garante Privacy sul DDL IA evidenzia l'importanza di un coordinamento sistematico tra le disposizioni in materia di IA e la normativa sulla protezione dei dati personali. Tra le principali raccomandazioni emergono l'integrazione di un articolo trasversale sulla protezione dei dati personali, la riformulazione delle norme relative all'IA in ambito sanitario e lavorativo, e un maggiore coinvolgimento del Garante nelle procedure decisionali e strategiche.

L'attuazione di queste modifiche è cruciale per evitare sovrapposizioni normative, assicurare la protezione dei diritti fondamentali e garantire che l'adozione dell'IA in Italia avvenga in modo etico e responsabile, nel rispetto dei diritti degli interessati.

[8] Tale disposizione demanda a ciascuno Stato membro la decisione sulla possibilità di autorizzare, pur nel rispetto dei limiti ivi previsti (ad esempio, per la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse), in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico per finalità di polizia. A tal fine, ai sensi dell'art. 5, par. 3 dell'AI Act, il legislatore nazionale deve altresì individuare, nell'autorità giudiziaria o in un'autorità amministrativa indipendente, l'organo competente a rilasciare l'autorizzazione all'utilizzo di tale tipologia di sistemi.

Per maggiori informazioni e approfondimenti

Carlo Impalà
Partner e Responsabile Osservatorio TMT&DP

Carloo.Impala@MorriRossetti.it

Morri Rossetti

Osservatorio TMT&DP

OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-dataprotection.it