OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Gennaio 2025

Gennaio 2025

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

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

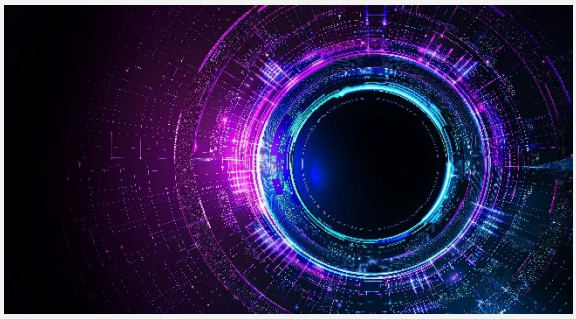
Provvedimenti del Garante Privacy

- Telemarketing, Garante privacy: sanzione di oltre 890mila euro a forniture luce e gas; [Link]
- Data breach, FSE Molise: le sanzioni del Garante privacy; [Link]
- Foto di un lifting sui social: il Garante sanziona un chirurgo; [Link]
- Pseudonimizzazione, in consultazione le linee guida dei Garanti privacy europei. [Link]

EDPB

- Guidelines 01/2025 on Pseudonymisation; [Link]
- Position paper on Interplay between data protection and competition law; [Link]
- Coordinated Enforcement Action, implementation of the right of access by controllers. [Link]

AI Act: upcoming deadlines and obligations



2025 shall be a pivotal year for artificial intelligence in Europe.

Starting from **February** and **August**, significant restrictions and obligations provided by the AI Act shall apply, directly impacting all companies that use or develop artificial intelligence systems.

Preparation and training in advance shall be key to seizing the opportunities presented by this technological revolution. The keywords here are **training**, **mapping of AI systems**, and **risk classification**. To facilitate this process, we have prepared a clear and concise summary of the key deadlines and obligations for 2025.

* * *

NIS2: Registrazione sulla piattaforma dell'ACN

Dal 1° dicembre 2024, le imprese a cui si applica il D. Lgs. 138/2024 ("**Decreto NIS2**"), che recepisce la Direttiva (UE) 2555/2022 ("**Direttiva NIS2**"), possono registrarsi sulla piattaforma digitale resa disponibile dall'Agenzia per la Cybersicurezza Nazionale ("**ACN**") per l'identificazione e l'elencazione dei soggetti essenziali e dei soggetti importanti.

L'obbligo di registrazione, che deve essere adempiuto entro il **28 febbraio 2025**, si applica ai:

- **soggetti essenziali**, rappresentati da quei soggetti che operano in settori altamente critici tra cui quello sanitario, energetico, finanziario, spaziale e delle infrastrutture digitali;
- **soggetti importanti**, definiti per esclusione come quei soggetti non rientranti tra i soggetti essenziali, ossia servizi postali, gestione dei rifiuti, prodotti chimici, ricerca, alimentari, industria manifatturiera, provider digitali (ad es. social network, motori di ricerca, *marketplace* online).

Sono già in ritardo, ove non abbiano provveduto già all'iscrizione, specifici soggetti che si dovevano registrare sulla piattaforma entro lo scorso **17 gennaio**, tra cui:

- i fornitori di servizi di sistema dei nomi di dominio;
- i gestori di registri dei nomi di dominio di primo livello;
- i fornitori di servizi di registrazione dei nomi di dominio;
- i fornitori di servizi di *cloud computing*;
- i fornitori di servizi di *data center*;
- i fornitori di reti di distribuzione dei contenuti;
- i fornitori di servizi gestiti;
- i fornitori di servizi di sicurezza gestiti;
- i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network che rientrano nell'ambito di applicazione del Decreto NIS2.

La mancata registrazione entro il 17 gennaio espone i soggetti interessati al rischio di sanzioni, come vedremo a breve.

A partire da quest'anno, i soggetti essenziali ed importanti, inoltre, dovranno registrarsi o aggiornare le informazioni contenute nella registrazione nel periodo intercorrente tra il **1° gennaio** e il **28 febbraio**.

Uno strumento fondamentale e utile per la registrazione è la "*Determinazione del Direttore generale dell'Agenzia per la cybersicurezza nazionale*" n. 38565 del 26 novembre 2024, nella quale sono stati definiti i termini, le modalità e i procedimenti di utilizzo e accesso alla piattaforma digitale.

Cosa occorre sapere?

Il portale, già attivo, richiede, per la registrazione, l'accesso tramite SPID o con credenziali.

Prima di procedere con la procedura di registrazione, è opportuno risolvere alcune questioni preliminari, tra cui:

- individuare il soggetto che rivestirà il ruolo di **punto di contatto** con l'ACN e, nel caso in cui tale figura sia un delegato dal rappresentante legale del soggetto essenziale o importante, non già munito di procura generale, predisporre specifica **delega di autorizzazione** ad accedere alla piattaforma e ai servizi dell'ACN per conto del soggetto stesso;
- individuare il **ruolo privacy** di tale figura e porre in essere gli adempimenti previsti dalla normativa in materia di protezione dei dati personali (ad es. nomina della figura prescelta a punto di contatto quale autorizzato al trattamento dei dati, ai sensi dell'art. 29 del GDPR).

Il punto di contatto, infatti, dovrà effettuare la registrazione per conto del soggetto e curare l'attuazione delle disposizioni del Decreto NIS2 accedendo al portale ACN (tra cui, ad esempio, in caso di inserimento nell'elenco dell'ACN, la comunicazione dello spazio di indirizzamento IP pubblico e i nomi di dominio in uso o nella disponibilità del soggetto, nonché la predisposizione e il caricamento sulla piattaforma dell'elenco degli Stati membri in cui vengono forniti i servizi che rientrano nell'ambito di applicazione del Decreto NIS2), nonché interloquire con l'ACN, ove necessario.

La mancata registrazione, comunicazione o aggiornamento delle informazioni potrebbe dar luogo a pesanti sanzioni amministrative pecuniarie:

- per i soggetti essenziali fino a un **massimo dello 0,1%** del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo modalità specifiche;
- per i soggetti importanti fino a un **massimo dello 0,7%** del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo modalità specifiche.

In caso di mancata o tardiva registrazione potrebbe essere altresì contestata la mancata osservanza degli obblighi imposti agli **organi di amministrazione** e agli **organi direttivi** e si applicherebbe la sanzione prevista per la violazione più grave, aumentata fino al triplo.

Gli organi amministrativi e direttivi non sono soltanto responsabili in caso di mancata, tardiva o erronea registrazione sulla piattaforma ACN, ma anche delle altre violazioni del Decreto NIS2, tra cui la loro mancata formazione in materia di sicurezza informatica, nonché l'assenza di promozione della formazione ai dipendenti in

merito alle misure di gestione dei rischi per la sicurezza informatica.

* * *

Protezione dei dati personali nell'IA: il Parere dell'EDPB su anonimizzazione, interesse legittimo e conseguenze di un trattamento illecito

Il Comitato Europeo per la Protezione dei Dati (*European Data Protection Board* – "**EDPB**") ha recentemente adottato l'Opinion 28/2024 relativa all'uso dei dati personali nello sviluppo e nella gestione di modelli di intelligenza artificiale (il "**Parere**").

Il Parere rappresenta un passaggio cruciale nella tutela della protezione dei dati, un ambito che sta diventando sempre più complesso e fondamentale in un contesto tecnologico in rapida evoluzione.

L'intelligenza artificiale, infatti, si caratterizza per l'uso pervasivo di tecniche di raccolta, trattamento e analisi di dati, che sollevano nuove sfide in termini di *privacy* e sicurezza.

Il Parere è stato redatto a seguito della richiesta dell'autorità per la protezione dei dati personali irlandese, al fine di garantire un'armonizzazione normativa a livello europeo su alcune questioni fondamentali relative alla tutela dei dati personali nell'era dell'IA.

Tali questioni riguardano: (i) quando e come un modello di IA può essere considerato "anonimo"; (ii) l'utilizzo dell'interesse legittimo come base giuridica per il trattamento dei dati durante le fasi di sviluppo e utilizzo dei modelli di IA e (iii) cosa accade se un modello di IA viene sviluppato utilizzando dati personali trattati illecitamente.

Ma cosa prevede, in concreto, il Parere dell'EDPB?

1. **Modelli di IA "anonimi"**

L'EDPB osserva che un modello di IA addestrato con dati personali non può, in ogni caso, essere considerato anonimo senza una valutazione specifica.

In effetti, quando un modello di IA è costruito utilizzando dati personali è possibile che esso generi inferenze (ossia previsioni o conclusioni) su individui non inclusi nei dati di addestramento o che produca direttamente dati personali riferibili a tali soggetti.

In tal caso, il modello incorpora informazioni relative a persone fisiche identificate o identificabili, comportando il trattamento di dati personali e risultando, pertanto, non anonimo. Si pensi, ad esempio, a un modello di IA generativa addestrato con registrazioni vocali di un individuo per replicarne la voce.

Allo stesso modo, anche se i modelli non sono progettati per produrre informazioni relative a persone identificate o identificabili, i dati personali utilizzati per l'addestramento potrebbero restare "assorbiti" nei parametri del modello sotto forma di rappresentazioni matematiche.

Queste rappresentazioni potrebbero poi essere estratte o dedotte, sia direttamente che indirettamente. Pertanto, qualora fosse possibile ottenere dati personali tramite mezzi ragionevolmente prevedibili, il modello non potrà essere considerato anonimo.

Ci si chiede, quindi, quali circostanze debbano essere prese in considerazione per definire un modello di IA "anonimo".

L'EDPB suggerisce che le autorità di vigilanza e i titolari del trattamento dovrebbero rispettivamente verificare e provare che: (i) **non sia possibile estrarre dati personali dai dati di addestramento attraverso il modello**; e (ii) **qualsiasi *output* prodotto dal modello non sia riconducibile ai soggetti i cui dati personali sono stati utilizzati per l'addestramento**.

A tal fine, l'EDPB precisa che questa valutazione dovrebbe considerare tre aspetti fondamentali:

a. **riferimenti alle linee guida esistenti**, in particolare il Parere 05/2014 del WB29 sulle Tecniche di Anonimizzazione. Tale parere stabilisce che i dati possano essere considerati anonimi solo se non è possibile identificarli, correlarli o trarne inferenze. Inoltre, qualora non siano soddisfatti questi criteri, è necessario eseguire una **valutazione approfondita dei rischi di identificazione** [1]. L'EDPB ritiene che, a causa del rischio di estrazione e inferenza, i modelli di IA richiedono una valutazione accurata dei suddetti rischi;

b. **mezzi ragionevolmente prevedibili**. La valutazione deve tenere conto di tutti i mezzi che potrebbero essere impiegati dal titolare del trattamento o da terzi per identificare gli interessati. La determinazione di questi mezzi deve basarsi su **fattori oggettivi**, come indicato nel Considerando 26 del Regolamento (UE) 679/2016 ("**GDPR**"), e includere:

- le caratteristiche dei dati di addestramento, del modello di IA e della procedura di addestramento (ad es., l'unicità dei record, la precisione delle informazioni, l'aggregazione, ecc..);
- il contesto in cui il modello di IA viene rilasciato e/o utilizzato (ad es., eventuali limitazioni nell'accesso);
- ulteriori informazioni che potrebbero consentire l'identificazione;
- i costi e i tempi necessari per ottenere tali informazioni (nel caso in cui non siano già disponibili);
- la tecnologia disponibile al momento del trattamento e i suoi sviluppi futuri;

c. **valutazione del rischio di identificazione**. Le Autorità di Controllo per la protezione dei dati personali (*Data Protection Authorities* – "**DPA**") dovrebbero esaminare se i titolari del trattamento abbiano valutato adeguatamente il rischio di identificazione, sia da parte loro che da parte di soggetti esterni, inclusi i terzi non autorizzati che potrebbero accedere al modello di IA.

In sintesi, l'EDPB sottolinea che per considerare anonimo un modello di IA, è necessario che (i) non vi sia alcuna possibilità di estrazione diretta di dati personali (compresa quella probabilistica) relativi agli individui il cui dato è stato utilizzato per l'addestramento, e (ii) che la probabilità di ottenere tali informazioni, sia intenzionalmente che accidentalmente, sia irrilevante per l'interessato.

Le DPA dovrebbero, quindi, prendere in considerazione la necessità di una valutazione approfondita dei rischi di identificazione, che deve includere tutti i "mezzi ragionevolmente prevedibili" che potrebbero essere impiegati dal

[1] WP29 Parere 05/2014, p. 26.

titolare del trattamento o da terzi, inclusi il riutilizzo o la divulgazione non intenzionale del modello.

Inoltre, l'EDPB elenca una serie di elementi per **valutare la probabilità residua di identificazione** che le DPA potrebbero prendere in considerazione, tra cui:

- la progettazione del modello di IA, comprendente quattro aspetti chiave: le fonti di dati utilizzate per l'addestramento, la preparazione e la minimizzazione dei dati, le scelte metodologiche adottate nell'addestramento e le misure adottate per gestire gli *output* del modello;
- l'analisi del modello, che implica la valutazione da parte del titolare del trattamento dell'efficacia delle misure adottate per ridurre il rischio di identificazione, anche attraverso *audit* documentali;
- i *test* del modello di IA e la sua resistenza agli attacchi;
- la documentazione necessaria, come previsto dagli articoli 5, 24, 25, 30 e 35 del GDPR.

2. **L'interesse legittimo come base giuridica nelle fasi di sviluppo e utilizzo dei modelli di IA**

L'EDPB, richiamando le proprie linee guida sul legittimo interesse[2], prende in considerazione le tre fasi richieste dalla valutazione del legittimo interesse (*Legitimate Interest Assessment* – "**LIA**") nel contesto dello sviluppo e della diffusione dei modelli di IA:

a. il **perseguimento di un interesse legittimo da parte del titolare del trattamento o di una terza parte**

L'EDPB sottolinea che un interesse può essere considerato legittimo se è **lecito**, **specifico** e **non speculativo**.
Nel contesto dei modelli di IA, esempi di interessi legittimi possono comprendere lo sviluppo di IA conversazionale, come *chatbot* o assistenti virtuali; l'implementazione di soluzioni di IA per rilevare contenuti o comportamenti fraudolenti; o il miglioramento della sicurezza informatica, come il rafforzamento della capacità di rilevamento di minacce;

b. la **necessità del trattamento per perseguire l'interesse legittimo** (***necessity test***)

Il *necessity test* implica due valutazioni principali: (i) il trattamento deve essere necessario per perseguire lo scopo perseguito; e (ii) non devono esistere alternative meno invasive per raggiungere lo stesso obiettivo.

In concreto, nel contesto dei modelli di IA, questo significa che il titolare deve considerare se il trattamento dei dati personali è **indispensabile** per ottenere il risultato desiderato, o se esistono **metodi alternativi**, che comportano una minore invasività nei diritti degli interessati, per raggiungere lo stesso scopo.

Pertanto, se l'obiettivo può essere conseguito tramite un modello di IA che non comporta il trattamento di dati personali, allora quest'ultimo non dovrebbe essere considerato necessario.
Il *necessity test* può comunque essere soddisfatto se vengono adottate **misure tecniche e organizzative appropriate** [3], come l'uso di pseudonimizzazione, la minimizzazione dei dati (ad es., riducendo al minimo la quantità di dati personali utilizzati per l'addestramento), e l'adozione di strategie di filtraggio per escludere dati personali non rilevanti.

[2] Linee Guida 1/2024 sul trattamento di dati personali basato sull'Articolo 6(1)(f) del GDPR

[3] L'EDPB identifica le misure di sicurezza nella Sezione 3.2.2 del Parere.

Sebbene queste misure non garantiscano l'anonimizzazione totale, contribuiscono comunque a ridurre la probabilità di identificare gli interessati;

c. la **prevalenza degli interessi, diritti e libertà degli interessati** (***balancing test***)

L'ultima condizione che deve essere soddisfatta per il trattamento basato sull'interesse legittimo è il *balancing test*, ossia la verifica che gli interessi, i diritti fondamentali e le libertà degli interessati non prevalgano sull'interesse legittimo del titolare. In questo contesto, l'EDPB individua una serie di diritti e interessi degli interessati che devono essere presi in considerazione. Questi includono, nella fase di sviluppo del modello di IA, il diritto all'autodeterminazione e al controllo sui propri dati personali.

Nella fase di utilizzo del modello, gli interessi degli interessati possono riguardare la gestione dei propri dati personali, ma anche interessi finanziari, benefici personali e socio-economici, come l'accesso migliorato ai servizi sanitari o l'esercizio di diritti fondamentali come l'accesso all'istruzione.
Il trattamento dei dati personali durante lo sviluppo e l'uso dei modelli di IA può comportare rischi significativi per i diritti tutelati dalla Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto alla vita privata (art. 7) e il diritto alla protezione dei dati personali (art. 8)[4].

Tali rischi possono emergere tanto nella fase di sviluppo (ad es., attraverso il *web scraping*) quanto in quella di utilizzo (ad es., nel caso in cui un cyberattacco porti alla rivelazione di dati sensibili contenuti nel *dataset* di addestramento).

Il trattamento di dati personali durante lo sviluppo e l'utilizzo dei modello di IA può avere impatti sia positivi[5] che negativi sugli interessati.

Questi impatti devono essere valutati considerando: (i) la natura dei dati trattati, (ii) il contesto del trattamento (inclusi i rischi legati al modo in cui è stato sviluppato e utilizzato il modello e alle misure di sicurezza adottate), e (iii) le ulteriori conseguenze, da valutare in base al caso concreto, inclusa la probabilità che tali conseguenze si materializzino e le misure di sicurezza adottate[6].

Le **ragionevoli aspettative degli interessati**, come stabilito nel Considerando 47 del GDPR, rivestono un ruolo fondamentale nel *balancing test*, soprattutto in considerazione della complessità intrinseca delle tecnologie di IA.

Gli interessati potrebbero non essere pienamente consapevoli dei potenziali utilizzi dei loro dati da parte di un modello di IA, rendendo cruciale la trasparenza e l'informazione adeguata. L'EDPB osserva, tuttavia, che la mera *compliance* agli obblighi di trasparenza del GDPR non è di per sé sufficiente a costituire una "ragionevole aspettativa" da parte degli interessati, la quale deve invece essere valutata in base a fattori concreti, come la pubblica disponibilità dei dati, la loro fonte e le specifiche capacità del modello di IA.

Nel caso in cui gli interessi, i diritti e le libertà degli interessati sembrino prevalere sul legittimo interesse del titolare, quest'ultimo potrebbe considerare di introdurre **misure di mitigazione** per ridurre al minimo l'impatto del trattamento sugli interessati. L'EDPB offre un elenco non

[4] L'EDPB sottolinea come, in realtà, a seconda del caso specifico, possono venire in rilievo anche altri rischi per i diritti fondamentali, tra cui la libertà di espressione (art. 11 della Carta), il diritto a svolgere un'attività lavorativa (art. 15 della Carta), il diritto alla non discriminazione (art. 21 della Carta).
[5] Si pensi ad esempio alle ipotesi in cui il modello di IA venga utilizzato per identificare contenuti dannosi online oppure ai casi in cui faciliti l'accesso a determinati servizi essenziali, come l'accesso all'informazione o all'istruzione.
[6] Ad esempio, nel caso dell'IA generativa, le misure potrebbero riguardare i controlli volti a limitare il più possibile il loro utilizzo per pratiche dannose, come la creazione di *deepfakes*.

esaustivo di misure di mitigazione applicabili, distinguendo tra quelle da adottare durante la fase di sviluppo del modello di IA e quelle da applicare durante l'uso, oltre a specifiche misure riguardanti il *web scraping*.

Nella fase di sviluppo, vengono individuate sia **misure tecniche**, come la pseudonimizzazione o la sostituzione di nomi e indirizzi e-mail con nomi e indirizzi e-mail fittizi, sia **misure volte a facilitare l'esercizio dei diritti degli interessati**, come la predisposizione di un diritto di "*opt-out*" incondizionato, fornendo agli interessati un diritto discrezionale di opporsi al trattamento ancor prima che il trattamento abbia luogo, sia **misure di trasparenza**, come la pubblicazione di informazioni pubbliche e facilmente accessibili che vadano oltre le informazioni richieste dagli artt. 13 e 14 del GDPR (ad es., fornendo dettagli aggiuntivi sui criteri di raccolta e sui *dataset* utilizzati), oppure la previsione di forme alternative per informare gli interessati (ad es., la pubblicazione di FAQ).

Per quanto riguarda il ***web scraping***, l'EDPB suggerisce l'esclusione di dati che comportano rischi per particolari persone o gruppi di persone dai *dataset*, l'imposizione di limiti alla raccolta e l'introduzione di meccanismi di *opt-out* per consentire agli interessati di opporsi, anche in via preventiva, alla raccolta dei loro dati su determinati siti o piattaforme *online*.

Prendendo invece in considerazione la fase di utilizzo del modello di IA, le misure tecniche potrebbero mirare a prevenire la memorizzazione, riproduzione e generazione di dati personali (ad es., i filtri per gli *output*), mentre misure volte a facilitare l'esercizio di diritti degli interessati potrebbero riguardare, ad esempio, la previsione di tecniche post-addestramento volte a rimuovere i dati personali.

Infine, l'EDPB suggerisce che le DPA, nella fase di utilizzo del modello, considerino se il titolare abbia pubblicato il risultato del *balancing test* e se abbia coinvolto, quando applicabile, il DPO nella valutazione.

3. **Conseguenze di un trattamento il lecito nello sviluppo di un modello di IA**

Con riguardo agli impatti che potrebbero derivare da un trattamento illecito nello sviluppo di un modello di IA, l'EDPB ipotizza tre scenari:

a. **scenario 1: il trattamento illecito e l'utilizzo successivo da parte dello stesso titolare**

Un titolare del trattamento tratta illecitamente dati personali per sviluppare un modello di IA, conserva tali dati e successivamente continua a trattarli. In questo caso, si rendono necessari:

- **interventi delle DPA**: il potere delle DPA di imporre misure correttive sul trattamento inziale avrebbe, in linea di principio, un impatto sul trattamento successivo. Si pensi, ad esempio, al caso in cui una DPA imponga a un titolare di cancellare i dati personali trattati illecitamente: il titolare, in virtù delle misure correttive applicate dalla DPA, non potrebbe trattare tali dati in futuro;
- **analisi dell'impatto**: le DPA devono esaminare come l'illiceità del trattamento inziale influisca sui successivi trattamenti, considerando le peculiarità del caso concreto.

b. **scenario 2: il trattamento illecito e il coinvolgimento di un altro titolare**

Un titolare del trattamento tratta illecitamente dati personali per sviluppare il modello, i quali vengono conservati nel modello e successivamente trattati da un altro titolare.
Le osservazioni principali dell'EDPB includono:

- **ruoli e responsabilità**: occorre chiarire, dal punto di vista privacy, i ruoli dei

diversi attori coinvolti, valutando possibili situazioni di contitolarità;

- **liceità dei trattamenti**: le DPA dovrebbero verificare che entrambi i trattamenti, quello del primo titolare e quello del secondo, rispettino le disposizioni del GDPR;
- **dichiarazione di conformità**: nel caso di sistemi di IA ad alto rischio, la dichiarazione di conformità richiesta dal Regolamento (UE) 1689/2024 ("**AI Act**")[7], anche se non costituisce presunzione di conformità al GDPR, può comunque essere pressa in considerazione dalle DPA;

c. **scenario 3: il trattamento illecito con successiva anonimizzazione**

In questa ipotesi, i dati personali trattati illecitamente per sviluppare il modello vengono anonimizzati prima di ulteriori utilizzi del modello (i.e. sia che il medesimo o un altro titolare avviino un ulteriore trattamento).

Sotto quest'ultimo profilo, le osservazioni dell'EDPB riguardano:

- **interventi delle DPA**: compete alle DPA intervenire sia con riguardo al trattamento legato all'anonimizzazione del modello, sia al trattamento svolto durante la fase di sviluppo, potendo, dunque, imporre misure correttive anche su questo trattamento inziale;
- **non applicazione del GDPR**: se si è in grado di dimostrare che il modello di IA non comporta il trattamento di dati personali (operando solo con dati anonimi), il GDPR non si applica. Tuttavia, l'EDPB sottolinea che una semplice dichiarazione di aver reso il modello di IA anonimo non è di per sé sufficiente per non applicare il GDPR, ma le DPA dovranno valutarlo caso per caso;
- **trattamenti successivi**: qualora i titolari del trattamento utilizzino successivamente dati personali, questi trattamenti saranno soggetti al GDPR, indipendentemente dall'illiceità della fase iniziale.

Considerazioni finali

Con questo Parere, l'EDPB conferma il ruolo cruciale del GDPR come pilastro normativo nel contesto delle nuove tecnologie, dimostrando la capacità di questa normativa di adattarsi alle rapide evoluzioni - normative e tecnologiche - che caratterizzano lo scenario attuale.

L'obiettivo perseguito è chiaro: cercare di raggiungere il delicato equilibrio tra innovazione e responsabilità. Come affermato anche dal presidente dell'EDPB, occorre garantire che lo sviluppo tecnologico avvenga in modo etico, sicuro e a beneficio di tutti.

Il Parere rappresenta un ulteriore passo in avanti verso una regolamentazione sempre più coerente e responsabile dell'IA, confermando l'impegno a garantire la protezione dei dati personali nel pieno rispetto del GDPR.

Una prospettiva, dunque, che oltre a tutelare i diritti degli interessati, favorisce un'innovazione responsabile, costruendo un futuro tecnologico sostenibile e inclusivo.

[7] Ai sensi dell'Art. 47 dell'AI Act, un fornitore di un sistema di IA ad alto rischio deve rendere una dichiarazione di conformità del sistema ai requisiti previsti dagli artt. 8-15 dell'AI Act. Tale dichiarazione deve contenere diversi elementi, tra cui, anche la dichiarazione che il sistema rispetti le disposizioni del GDPR.

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