OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Febbraio 2025

Febbraio 2025

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

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

EDPB

- Work Programme 2025-2026; [Link]
- Dichiarazione 1/2025 sulla garanzia dell'età; [Link]
- EDPB Document on Process guide for the selection and the handling of strategic cases. [Link]

AGCOM

- Definizione del punto terminale di rete (NTP) per i servizi di accesso alla rete Internet da postazione fissa; [Link]
- Broadband Map: dati aggiornati al quarto trimestre 2024 e nuove funzionalità software. [Link]

La pseudonimizzazione come strumento di tutela e conformità secondo le nuove Linee Guida dell'EDPB

Nel corso della riunione plenaria di gennaio 2025, il Comitato europeo per la protezione dei dati (*European Data Protection Board* – "**EDPB**") ha adottato **le Linee Guida 01/2025 sulla pseudonimizzazione** (le "**Linee Guida**"), con l'obiettivo di chiarire il ruolo e l'applicazione di questa tecnica ai fini della conformità al Regolamento (UE) 679/2016 (il "**GDPR**").

Il GDPR introduce per la prima volta il concetto di "pseudonimizzazione" all'articolo 4(5), riconoscendola come una misura di salvaguardia efficace per il lecito trattamento dei dati personali. Le Linee Guida approfondiscono la definizione e l'ambito di applicazione della pseudonimizzazione, nonché i benefici derivanti dal suo utilizzo.

I due punti chiave delle Linee Guida

L'EDP apporta due chiarimenti principali:

1. i **dati pseudonimizzati non sono dati anonimi**.

Sebbene la pseudonimizzazione riduca il legame diretto tra i dati e gli interessati, questi ultimi possono essere identificati qualora esistano informazioni aggiuntive, che ne consentano le reidentificazione, dovendo conseguentemente trovare applicazione anche le disposizioni del GDPR in merito all'esercizio dei diritti degli interessati[1];

2. la **pseudonimizzazione come strumento di mitigazione dei rischi**[2].

La pseudonimizzazione rappresenta una misura fondamentale per la protezione dei dati personali degli interessati, in quanto protegge i loro dati da accessi o utilizzi non autorizzati senza comprometterne l'utilità.

Essa favorisce il rispetto dei principi di ***privacy by design*** e ***by default***, di **minimizzazione** dei dati e **riservatezza**, oltre a garantire la **liceità**, la **correttezza**, la **limitazione delle finalità** e l'**accuratezza del trattamento**[3].

In tale ottica, **la pseudonimizzazione può facilitare l'utilizzo dell'interesse legittimo come base giuridica del trattamento**, purché siano rispettati tutti gli altri requisiti imposti dal GDPR. Essa, infatti, contribuisce alla valutazione della prevalenza dell'interesse legittimo del titolare rispetto agli interessi, ai diritti e alle libertà degli interessati.

L'EDPB, inoltre, sostiene che la pseudonimizzazione può costituire una "**misura supplementare**"per garantire la conformità agli

[1] Ad esempio, se l'interessato è in grado di fornire lo/gli pseudonimo/i sotto cui sono conservati i dati che lo riguardano, e una prova che tali pseudonimi si riferiscono a lui, il titolare è in grado di identificarlo e, dunque, dovrebbero applicarsi i diritti dell'interessato. Pertanto, al fine di garantire il pieno esercizio dei diritti degli interessati, il titolare dovrebbe indicare, nelle informazioni fornite agli interessati ai sensi dell'Art. 11(2) del GDPR, come questi possano ottenere gli pseudonimi a loro riferiti e come possano essere utilizzati per dimostrare la loro identità. In tale contesto, il titolare potrebbe dover fornire l'identità e i dettagli di contatto della fonte dei dati pseudonimizzati o del titolare responsabile della pseudonimizzazione.

[2] In particolare, la pseudonimizzazione è in grado di ridurre: (i) i rischi per la riservatezza; (ii) il rischio di function creep (ovvero il rischio che i dati personali vengano ulteriormente trattati in modo incompatibile con le finalità per le quali sono stati originariamente raccolti); (iii) i rischi per l'accuratezza dei dati, limitando la possibilità di attribuire erroneamente dati o oggetti a soggetti sbagliati.

[3] L'EDPB offre, in un apposito allegato alle Linee Guida, una lista di esempi in cui illustra concretamente come la pseudonimizzazione contribuisca al soddisfacimento di tali principi.

artt. 44-46(1) del GDPR **per i trasferimenti di dati verso paesi terzi**, proteggendo i dati dall'accesso sproporzionato delle autorità pubbliche straniere[4].

Il "dominio di pseudonimizzazione"

Uno degli aspetti più innovativi introdotti dalle Linee Guida è il concetto di "**dominio di pseudonimizzazione**", inteso come l'ambito operativo – all'interno dell'organizzazione del titolare – entro cui la pseudonimizzazione deve impedire l'attribuzione dei dati a soggetti determinati, prevenendone la reidentificazione. Si tratta, in pratica, di una valutazione del titolare, il quale – a seconda dell'obiettivo della pseudonimizzazione e della valutazione del rischio - può definire il dominio di pseudonimizzazione includendo, ad esempio, una sua singola unità organizzativa, un singolo destinatario esterno oppure tutti i destinatari autorizzati o previsti e legittimi.

Tuttavia, di fatto, ponendo tale scelta in seno alla discrezionalità del titolare, il rischio è quello di rimettere l'efficacia della pseudonimizzazione unicamente alla volontà soggettiva del titolare stesso, in assenza di criteri oggettivi.

Ad ogni modo, l'EDPB sottolinea la necessità di adottare misure adeguate affinché il dominio sia opportunamente protetto e separato dalle informazioni aggiuntive, evitando che queste ultime possano entrare nel dominio stesso o che i dati pseudonimizzati ne escano senza adeguate garanzie.

Il processo di pseudonimizzazione e le sue implicazioni tecniche

La pseudonimizzazione si realizza attraverso l'applicazione di una **trasformazione pseudonimizzante**[5], un processo che modifica i dati originali in modo tale che il risultato – i dati pseudonimizzati – non possa essere attribuito a un interessato senza l'ausilio di informazioni supplementari.

Nella maggior parte dei casi, questa operazione avviene mediante la sostituzione di dati identificativi con **pseudonimi**, ossia identificatori alternativi che permettono la riassociazione ai soggetti originari solo attraverso l'uso di informazioni aggiuntive adeguatamente protette.

Affinché la pseudonimizzazione sia efficace, i dati pseudonimizzati non devono contenere identificatori diretti (ad esempio, il codice fiscale o il numero di passaporto) né "quasi-identificatori", ossia attributi che, combinati, possono condurre all'identificazione dell'interessato[6].

Per questo motivo, tali identificatori devono essere eliminati o sostituiti nel corso del processo di pseudonimizzazione. Un aspetto cruciale della pseudonimizzazione è l'adozione di **dati segreti** per prevenire l'attribuzione non autorizzata dei dati pseudonimizzati.

Tali dati – definiti nelle Linee Guida come *"pseudonymisation secrets*" – comprendono chiavi crittografiche, tabelle di corrispondenza tra pseudonimi e dati reali e altre tecniche di protezione.

[4] L'EDPB richiama le proprie Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE.

[5] Tale processo di trasformazione avviene, generalmente, attraverso l'utilizzo di due diverse tecniche: gli algoritmi crittografici, che prendono la forma di parametri segreti o chiavi (come, ad esempio, i codici di autenticazione del messaggio o gli algoritmi di crittografia), e le tabelle di ricerca che associano gli identificatori con gli pseudonimi utilizzati per sostituirli.

[6] Si tratti di attributi in grado di rivelare informazioni su identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale dell'interessato. Costituiscono un esempio di "quasi-identificatori" i dati demografici, quali età, genere, lingue parlate, stato civile o familiare, professione, reddito. Analogamente, nel caso dei dipendenti altri dati rilevanti possono riguardare la funzione o il ruolo ricoperti, il numero di ore lavorative e la durata del servizio.

L'EDPB raccomanda di implementare misure tecniche e organizzative adeguate per garantirne la riservatezza e impedire usi impropri o non autorizzati[7].

Riflessioni finali

La pseudonimizzazione emerge dalle Linee Guida dell'EDPB come uno strumento di grande rilevanza nella protezione dei dati personali, in grado di contribuire significativamente alla conformità normativa e alla tutela degli interessati.

Tuttavia, l'EDPB sottolinea che essa, pur essendo una misura efficace, non rappresenta una soluzione assoluta e deve essere integrata con altre garanzie adeguate per assicurare una protezione complessiva dei dati personali degli interessati.

Di conseguenza, i titolari del trattamento dovranno valutare attentamente l'insieme delle misure adottate per verificare la loro idoneità nel soddisfare i requisiti di protezione previsti dal GDPR.

* * *

Commissione europea: un supporto per l'interpretazione del concetto di sistema di AI

A partire dallo scorso 2 febbraio 2025 sono divenute ufficialmente applicabili le prime disposizioni del Regolamento (UE) 1689/2024 (noto come "**AI Act**"), tra cui gli articoli relativi a definizioni, alfabetizzazione e pratiche di AI vietate.

Per le aziende, ciò comporta una serie di obblighi che richiedono, tra gli altri, un'accurata **mappatura e classificazione dei sistemi di AI** in base alle categorie di rischio previste dalla normativa.

Tuttavia, prima di affrontare la classificazione del rischio, è imprescindibile comprendere **cosa si intenda per** "**sistema di AI**". La definizione contenuta nell'AI Act è chiara e precisa, ma altrettanto fondamentale è l'interpretazione pratica e concreta che ne può scaturire.

Un sistema di AI è definito come un "*sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che,*

[7] L'EDPB sottolinea come misure tecniche appropriate possono includere la segmentazione della rete, l'archiviazione sicura delle chiavi segrete in moduli di sicurezza hardware, l'autenticazione sicura per l'accesso alle API (Application Programming Interface) e la limitazione della velocità e la registrazione dell'esecuzione sia della trasformazione pseudonimizzante sia, in particolare, della sua applicazione inversa, ove disponibile. Quanto, invece, alle misure organizzative, esse includono l'impiego di personale selezionato e specificamente autorizzato per il funzionamento dei sistemi utilizzati per l'esecuzione della trasformazione pseudonimizzante e per l'archiviazione degli pseudonymization secrets. I titolari dovranno altresì garantire che tutti coloro incaricati sia di interagire con gli interessati sia di accedere ai dati pseudonimizzati (ad esempio, per garantire i diritti degli interessati), ricevano una formazione adeguata.

per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali" (art. 3, n. 1), dell'AI Act).

Ma cosa significa in concreto? La risposta a questa domanda viene fornita dalla Commissione europea (la "**Commissione**"), che ha recentemente adottato delle Linee Guida sulla definizione di un sistema di AI (le "**Linee Guida**"), con l'obiettivo di consentire a fornitori, *deployer* e a tutti gli *stakeholders* di determinare se un software possa essere considerato un vero e proprio "sistema di AI".

I sette requisiti fondamentali per definire un sistema di AI

La Commissione ha suddiviso la definizione di sistema di AI in sette elementi chiave, che devono essere considerati per ogni applicazione pratica:

1. **sistema automatizzato**: un sistema che operi su base computazionale, basato su componenti sia hardware che software;
2. **autonomia**: il sistema deve operare con un certo grado di indipendenza, pur ammettendo l'intervento umano, quando necessario;
3. **adattabilità**: la capacità di autoapprendimento, anche se non obbligatoria, può essere un elemento distintivo del sistema, permettendogli di modificarsi durante l'utilizzo;
4. **obiettivi del sistema**: il fine ultimo dei compiti da eseguire e dei risultati da ottenere, che possono essere sia espliciti che impliciti[8];
5. **inferenza**: la capacità del sistema, riferita alla sua fase di sviluppo, di elaborare input per generare output, utilizzando tecniche come il *machine learning* [9] o approcci basati sulla logica e sulla conoscenza[10];
6. **output**: i risultati generati dal sistema, che includono previsioni, contenuti, raccomandazioni o decisioni;
7. **influenza sugli ambienti**: l'impatto che il sistema può avere su ambienti fisici (come oggetti o macchinari, quali ad esempio, un braccio robotico) o virtuali (come spazi digitali, flussi di dati ed ecosistemi software).

I sistemi esclusi dalla definizione di AI

Non tutti i sistemi rientrano nella definizione di AI. Le Linee Guida della Commissione precisano quali sistemi, pur essendo automatici, non siano considerabili come sistemi di AI.

Tra questi vi sono:

- sistemi di **ottimizzazione matematica** (come la regressione lineare o logistica) che, pur essendo in grado di effettuare inferenze, non vanno oltre la soglia di "semplice elaborazione dei dati". Si pensi, ad esempio, a un sistema di telecomunicazioni satellitari destinato a

[8] Gli obiettivi sono "espliciti" se chiaramente definiti e codificati dallo sviluppatore del sistema; si dicono invece "impliciti" se sono deducibili indirettamente dal sistema.

[9] Questa categoria include un'ampia varietà di approcci che permettono a un sistema di "apprendere", tra cui l'apprendimento supervisionato (dove il sistema di AI apprende da un insieme di dati già etichettato, in cui ogni input è associato all'output corretto), l'apprendimento non supervisionato (in cui il sistema non ha accesso a risposte predefinite e cerca modelli, strutture o relazioni nei dati), l'apprendimento auto-supervisionato (in cui il sistema apprende da dati non etichettati in modo supervisionato, utilizzando i dati stessi per creare le proprie etichette o obiettivi) e l'apprendimento per rinforzo (in cui il sistema apprende dai dati raccolti dalla propria esperienza, provando e sbagliando).

[10] In questo caso, invece di apprendere dai dati, i sistemi di AI apprendono dalla conoscenza, che include regole, fatti e relazioni codificate da esperti umani. Sulla base di questa conoscenza, i sistemi possono "ragionare" attraverso motori deduttivi o induttivi o mediante operazioni come ordinamento, ricerca, confronto e concatenazione.

ottimizzare l'allocazione della larghezza di banda e la gestione delle risorse;

- sistemi di **elaborazione dati di base**, che eseguono compiti basati su input manuali o regole fisse, senza alcuna capacità di apprendimento, ragionamento o modellizzazione. Ne costituiscono un esempio i gestionali usati per ordinare o filtrare i dati in base a criteri specifici, i software di fogli di calcolo standard o per il calcolo di medie statistiche, oppure i software per la visualizzazione di report di vendita o per l'analisi statistica di sondaggi o rilevazioni d'opinione;
- sistemi basati su **euristiche classiche**, ossia tecniche di risoluzione dei problemi – comunemente utilizzate in programmazione – che si basano su modelli basati sull'esperienza per trovare soluzioni approssimative in modo efficiente. Ne costituisce un esempio un programma di scacchi che utilizza un algoritmo per valutare le posizioni sulla scacchiera;
- sistemi di **previsioni semplici**, come quelli impiegati nelle previsioni finanziarie di base (in grado, ad esempio, di prevedere i prezzi futuri delle azioni), oppure nelle stime dalla temperatura.

L'applicabilità prime disposizioni dell'AI Act rappresenta un passo decisivo nella regolamentazione dell'AI in Europa. La comprensione chiara del concetto di "sistema di AI" e dei requisiti necessari per la sua classificazione è essenziale per ogni azienda che intenda operare in conformità con l'AI Act.

In tale contesto, le Linee Guida della Commissione, seppur non vincolanti, costituisco un documento di grande rilevanza, in grado di aiutare le aziende a orientarsi nell'ambito della mappatura e classificazione dei propri sistemi di AI, accompagnandole nel loro processo di adeguamento normativo.

Le Linee Guida sono destinate a evolversi nel tempo e, ove necessario, verranno aggiornate, anche e soprattutto alla luce delle esperienze pratiche e dei dubbi che potranno sorgere.

Decreto NIS 2 e clausola di salvaguardia: deroghe all'applicabilità della normativa

Il Decreto NIS 2[11] (D.Lgs. 138/2024), che ha dato attuazione in Italia alla Direttiva (UE) 2555/2022 ("**NIS 2**") si arricchisce di un elemento di rilievo cruciale con l'adozione del **D.P.C.M. 221/2024**, pubblicato in Gazzetta Ufficiale lo scorso 10 febbraio (il "**DPCM**").

Con tale provvedimento il legislatore approfondisce e definisce i criteri di applicazione della c.d. **clausola di salvaguardia** (art. 3, commi 4 e 12, del Decreto NIS 2), ossia il meccanismo che consente, in determinati casi, l'**esenzione dagli obblighi imposti dalla normativa NIS 2.**
L'importanza del DPCM è cruciale: entro il prossimo **28 febbraio** tutte le aziende e pubbliche amministrazioni coinvolte dovranno obbligatoriamente registrarsi sulla piattaforma

[11] Per un maggior approfondimento sul Decreto NIS 2, si rinvia a un nostro precedente contributo, disponibile qui

predisposta dall'Agenzia per la Cybersicurezza Nazionale ("**ACN**")[12].

Ma qual è la *ratio* della clausola di salvaguardia? Essa mira a coniugare la **tutela della cybersicurezza** con il principio di **proporzionalità**, evitando che realtà indipendenti, ma formalmente collegate a gruppi societari di grandi dimensioni, siano gravate da obblighi più stringenti di quelli effettivamente giustificati dalla loro struttura operativa

Chi può beneficiare della clausola di salvaguardia?

Non tutti i soggetti, pubblici o privati, possono accedere a questa esenzione. È necessario **dimostrare congiuntamente** di possedere una **totale indipendenza** rispetto al gruppo di appartenenza, sia in termini di sistemi informativi e di rete, sia rispetto all'attività e ai servizi disciplinati dalla normativa.

In concreto, affinché un'impresa possa beneficiare dell'esenzione, devono ricorrere entrambe le seguenti condizioni:

a. i suoi sistemi informativi e di rete non devono contribuire in alcun modo al funzionamento dei sistemi informativi e di rete NIS delle altre imprese del gruppo;
b. le sue attività e i servizi non devono contribuire in alcun modo allo svolgimento delle attività e all'erogazione dei servizi NIS da parte di altre imprese del gruppo.

Tuttavia, il DPCM introduce anche alcune **eccezioni**. Non potranno, infatti, avvalersi della clausola di salvaguardia quelle imprese che rientrano **automaticamente nel perimetro applicativo del Decreto NIS 2**, ossia quelle imprese collegate a un soggetto importante o essenziale che soddisfino almeno uno dei criteri stabiliti dall'art. 3, comma 10, del Decreto NIS 2.

In particolare, l'esenzione è preclusa alle imprese che:

- adottano decisioni o esercitano un'influenza dominante sulle scelte riguardanti le misure di gestione del rischio per la sicurezza informatica del soggetto essenziale o importante;
- detengono o gestiscono sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto essenziale o importante;
- svolgono operazioni di sicurezza informatica per conto del soggetto essenziale o importante;
- forniscono servizi TIC o di sicurezza, inclusi quelli gestiti, al soggetto essenziale o importante.

Come richiedere l'esenzione?

Le imprese che ritengono di soddisfare i criteri sopra esposti devono presentare la propria richiesta di esenzione **registrandosi sulla piattaforma digitale messa a disposizione dell'ACN.** L'Agenzia, valutando caso per caso, fornirà un **esplicito riscontro** e, laddove accerti la sussistenza dei requisiti, riconoscerà l'applicabilità della clausola di salvaguardia.

In tale procedura, si impone un vincolo di veridicità: i dati e le informazioni fornite in sede di registrazione devono corrispondere al vero, pena l'applicazione delle sanzioni penali previste dalla normativa vigente[13].

[12] Per un maggior approfondimento sugli obblighi di iscrizione alla piattaforma messa a disposizione dell'ACN, si rinvia a un nostro precedente contributo, disponibile qui.

[13] Il DPCM richiama, infatti, l'applicabilità dell'art. 76 del D.P.R. 445/2000.

Per maggiori informazioni e approfondimenti

Carlo Impalà

Partner e Responsabile Osservatorio TMT&DP

Carloo.Impala@MorriRossetti.it

Morri Rossetti & Franzosi **Osservatorio TMT&DP**

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti & Franzosi

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-dataprotection.it