OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Maggio 2026

Maggio 2026

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

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Deepfake: nuovo avvertimento del Garante privacy. L'Autorità chiede maggiori poteri di intervento; [Link]
- IA e lavoro: il Garante Privacy avverte una start-up italiana. Sotto la lente dell'Autorità il plug-in che può rilevare linguaggio, emozioni e livello di stress dei dipendenti; [Link]
- Data breach, il Garante privacy sanziona The European House Ambrosetti per 85mila euro; [Link]
- Garante privacy: online le Faq aggiornate sul Fascicolo sanitario elettronico. [Link]

AGCOM

- Osservatorio sulle comunicazioni n.1-2026; [Link]

ACN

- Il G7 vara le linee guida relative al Software Bill of Materials (SBOM) per l'intelligenza artificiale; [Link]

Dalla liceità del trattamento alla progettazione delle piattaforme: cosa cambia con le Linee Guida EDPB su DSA e GDPR

Il rapporto tra DSA e GDPR deve essere letto in un'ottica di complementarità: da un lato la disciplina sulla protezione dei dati personali, dall'altro nuove regole di trasparenza per le piattaforme *online*.

Le Linee Guida 03/2025 dell'EDPB (le "**Linee Guida**") mostrano però un quadro più articolato[1]. Il punto emerge con particolare evidenza in due ambiti centrali dell'economia digitale: la pubblicità comportamentale e i sistemi di raccomandazione.

Da un lato, il DSA impone nuove modalità di trasparenza immediata e accessibile sugli annunci pubblicitari; dall'altro, vieta in modo assoluto l'utilizzo di categorie particolari di dati per finalità di profilazione pubblicitaria, anche laddove il trattamento potrebbe teoricamente trovare una base di liceità ai sensi del GDPR.

Parallelamente, le Linee Guida chiariscono che i sistemi di raccomandazione non rappresentano soltanto strumenti di ottimizzazione della *user experience*, ma vere e proprie attività di trattamento che possono incidere significativamente sugli utenti e richiedono quindi precise scelte di *governance*, trasparenza e minimizzazione dei dati.

Più che introdurre obblighi autonomi e separati, il DSA sembra dunque spostare il baricentro della *compliance*: non è più sufficiente verificare se un trattamento sia astrattamente lecito ai sensi del GDPR, ma occorre valutare se l'intera architettura del servizio digitale sia compatibile con gli obiettivi di trasparenza, *accountability* e tutela dell'utente perseguiti dal regolamento sui servizi digitali.

Trasparenza della pubblicità e profilazione

L'art. 26 del DSA introduce specifici obblighi di trasparenza in materia di pubblicità, imponendo ai fornitori di piattaforme *online* di rendere immediatamente accessibili agli utenti una serie di informazioni relative agli annunci visualizzati[2]. Le informazioni devono essere presentate in tempo reale e direttamente accessibili dall'annuncio stesso.

Le Linee Guida chiariscono che tale obbligo può essere adempiuto anche successivamente all'effettivo trattamento dei dati personali utilizzati per la selezione dell'annuncio.

Ciò non esclude, tuttavia, l'applicazione delle regole del GDPR in materia di informativa privacy: le informazioni previste dagli artt. 13 e 14 del GDPR devono infatti essere fornite al momento della raccolta dei dati e, quindi, prima del trattamento.

Un chiarimento particolarmente rilevante riguarda però l'autonomia degli obblighi del DSA

[1] Le Linee Guida affrontano anche altri temi, tra cui con la moderazione dei contenuti online e il trattamento dei dati personali, all'articolo derubricato: "*Moderazione dei contenuti e trattamento dei dati personali: l'interazione tra gli obblighi del DSA e quelli del GDPR*

[2] In particolare, l'art. 26 DSA prevede che, per ogni singola pubblicità, le piattaforme online devono indicare: (i) se l'informazione costituisce una pubblicità; (ii) la persona fisica o giuridica per conto della quale viene presentata la pubblicità; (iii) la persona fisica che paga per la pubblicità; (iv) informazioni sui parametri utilizzati per determinare il destinatario al quale viene presentata la pubblicità e le eventuali opzioni per modificarli.

rispetto alla disciplina privacy. L'art. 26 del DSA si applica infatti anche a forme di pubblicità che non implicano profilazione e che possono persino non comportare alcun trattamento di dati personali.

La trasparenza pubblicitaria richiesta dal DSA non rappresenta quindi una mera estensione degli obblighi informativi previsti dal GDPR, ma un obbligo autonomo che riguarda il funzionamento stesso dell'ambiente digitale.

L'obiettivo non è soltanto rendere lecito il trattamento dei dati, ma consentire agli utenti di comprendere immediatamente perché stanno visualizzando un determinato contenuto pubblicitario e secondo quali criteri esso viene selezionato.

Nella pratica, ciò implica che le piattaforme *online* non possano più limitarsi a inserire informazioni generiche nelle *privacy policy* o nei *cookie banner*, ma debbano progettare interfacce che rendano effettivamente comprensibili i criteri di *targeting* utilizzati e le logiche di selezione degli annunci.

Le piattaforme *online*, al fine di mostrare pubblicità mirata, ricorrono frequentemente ad attività di profilazione che possono rientrare nell'ambito di applicazione dell'art. 22 del GDPR, trattandosi di processi automatizzati volti a valutare aspetti personali degli utenti.

Le Linee Guida precisano tuttavia che non ogni forma di *advertising* personalizzato produce necessariamente effetti giuridici o analogamente significativi ai sensi dell'art. 22 GDPR (si pensi, ad esempio, alla pubblicità generica).

La valutazione richiede un'analisi concreta delle caratteristiche del trattamento, considerando elementi quali il grado di intrusività della profilazione, il tracciamento *cross-device*, le aspettative ragionevoli dell'utente, le modalità di erogazione dell'annuncio o l'eventuale sfruttamento di vulnerabilità individuali.

Nei casi in cui trovi applicazione l'art. 22 GDPR, gli interessati hanno diritto a non essere sottoposti a decisioni unicamente automatizzate che producano effetti giuridici o incidano in modo analogo sulla loro persona, salvo che il trattamento sia necessario per l'esecuzione di un contratto, autorizzato dal diritto dell'Unione o degli Stati membri oppure fondato sul consenso esplicito dell'interessato.

In tali ipotesi, il GDPR richiede che gli utenti siano adeguatamente informati circa la logica utilizzata, l'importanza e le conseguenze previste del trattamento automatizzato, garantendo inoltre la possibilità di ottenere un intervento umano e contestare la decisione. Ne deriva che parte degli obblighi informativi previsti dal DSA si sovrappongono a quelli già imposti dal GDPR.

Tuttavia, il DSA introduce un elemento ulteriore: non si limita a richiedere trasparenza sul trattamento, ma impone che i principali parametri utilizzati per determinare la visualizzazione dell'annuncio siano facilmente accessibili e concretamente comprensibili direttamente nell'interfaccia della piattaforma.

Le Linee Guida sembrano così confermare una trasformazione più ampia dell'approccio europeo alla regolazione delle piattaforme digitali: la *compliance* non riguarda più soltanto la liceità del trattamento dei dati personali, ma anche la trasparenza delle logiche che governano la personalizzazione dei contenuti e delle inserzioni pubblicitarie.

Resta in ogni caso fermo che, indipendentemente dal fatto che il trattamento integri una forma di profilazione o sia finalizzato alla diffusione di pubblicità personalizzata, le piattaforme *online*

devono sempre individuare una valida base giuridica ai sensi del GDPR.

Divieto di profilazione basata su categorie particolari di dati

L'art. 26 DSA vieta la presentazione di annunci basati su tecniche di profilazione che utilizzano categorie particolari di dati personali ai sensi dell'art. 9 GDPR.

La disposizione assume particolare rilievo se letta congiuntamente all'art. 22 GDPR, il quale limita l'adozione di decisioni automatizzate fondate su categorie particolari di dati, salvo specifiche eccezioni, quali il consenso esplicito dell'interessato o rilevanti motivi di interesse pubblico.

Le Linee Guida evidenziano però come il DSA introduca, sotto questo profilo, una disciplina più restrittiva rispetto al GDPR. Mentre quest'ultimo consente in astratto il trattamento di categorie particolari di dati in presenza delle condizioni previste dagli artt. 6 e 9 GDPR, il DSA vieta in modo assoluto la presentazione di pubblicità basata sulla profilazione effettuata mediante tali dati. Si tratta di un passaggio particolarmente significativo.

Alcune pratiche di *advertising* comportamentale non vengono più valutate soltanto in termini di liceità del trattamento, ma considerate incompatibili, in sé, con il modello di tutela delineato dal DSA.

La conseguenza pratica è rilevante per i fornitori di piattaforme *online* e per gli operatori dell'*adtech ecosystem*. Anche laddove un soggetto ritenga di poter fondare il trattamento su una valida base giuridica e su una delle deroghe previste dall'art. 9, par. 2 GDPR, la pubblicità basata su categorie particolari di dati resta comunque vietata dal DSA.

Emblematico è l'esempio richiamato dall'EDPB relativo all'utilizzo di dati di localizzazione per inferire convinzioni religiose dell'utente o delle abitudini di acquisto per indirizzare messaggi pubblicitari personalizzati: anche in assenza di una raccolta esplicita del dato "sensibile", l'inferenza algoritmica di categorie particolari di dati può ricadere nel divieto previsto dal DSA.

I sistemi di raccomandazione

Le Linee Guida dedicano particolare attenzione anche ai sistemi di raccomandazione, definiti dal DSA come sistemi automatizzati o semi-automatizzati utilizzati dalle piattaforme *online* per suggerire, classificare o dare priorità ai contenuti visualizzati dagli utenti.

Questi sistemi costituiscono oggi uno degli strumenti principali attraverso cui le piattaforme organizzano l'esperienza digitale degli utenti, influenzando la visibilità dei contenuti, le interazioni *online* e, in alcuni casi, persino le scelte economiche o professionali degli interessati.

Le raccomandazioni possono basarsi su criteri molto diversi. In alcuni casi, il sistema opera senza trattare dati personali dell'utente, come avviene, ad esempio, quando un *e-commerce* mostra genericamente i prodotti più venduti.

In altri casi, invece, gli algoritmi elaborano dati comportamentali, cronologia di navigazione, preferenze o interazioni pregresse per prevedere quali contenuti siano maggiormente idonei a catturare l'attenzione dell'utente.

È soprattutto in quest'ultima ipotesi che emergono i principali profili di rischio evidenziati dall'EDPB: trattamento su larga scala di dati personali, opacità delle inferenze algoritmiche, utilizzo di categorie particolari di dati, possibile coinvolgimento di soggetti vulnerabili e adozione

di decisioni automatizzate suscettibili di incidere significativamente sugli interessati.

Le Linee Guida sembrano così recepire una consapevolezza ormai centrale nel dibattito europeo sulla regolazione digitale: i sistemi di raccomandazione non rappresentano strumenti neutrali di organizzazione dei contenuti, ma meccanismi in grado di orientare il comportamento degli utenti e influenzarne le decisioni.

Quando i sistemi di raccomandazione comportano il trattamento di dati personali, le piattaforme *online* agiscono in qualità di titolari del trattamento e devono pertanto rispettare i principi del GDPR, tra cui liceità, correttezza, trasparenza, limitazione della finalità e accuratezza dei dati.

In tale contesto, l'EDPB valorizza gli obblighi di trasparenza previsti dall'art. 27 DSA. Le piattaforme devono indicare nei propri termini e condizioni, in linguaggio chiaro e comprensibile, i principali parametri utilizzati dai sistemi di raccomandazione e le ragioni per cui determinati contenuti vengono suggeriti, prioritizzati o presentati con una certa prominenza. L'obiettivo perseguito dal DSA non sembra però limitarsi alla sola trasparenza documentale.

Le piattaforme devono infatti consentire agli utenti di modificare direttamente dall'interfaccia *online* le opzioni relative ai sistemi di raccomandazione, introducendo così forme di controllo effettivo sulla personalizzazione dei contenuti.

Ulteriori obblighi sono previsti per VLOPs e VLOSEs[3], le piattaforme e i motori di ricerca di dimensioni molto grandi che svolgono un ruolo sistemico nel mercato digitale. Tali soggetti devono offrire almeno un'opzione di sistema di raccomandazione non basata sulla profilazione.

Sul punto, le Linee Guida precisano che VLOPs e VLOSEs non possono progettare le interfacce in modo da orientare gli utenti verso sistemi di raccomandazione basati sulla profilazione. Le modalità di presentazione delle opzioni devono quindi rispettare i principi di *privacy by design*, *privacy by defaul*t e minimizzazione dei dati.

Le Linee Guida sottolineano inoltre che le informazioni raccolte in relazione alle preferenze espresse dagli utenti sui sistemi di raccomandazione possono essere trattate esclusivamente per adempiere agli obblighi previsti dal DSA. Tali dati devono essere conservati solo per il tempo strettamente necessario, evitando la creazione di storici relativi alle scelte effettuate dagli utenti.

Conclusioni

Le Linee Guida confermano che, nel contesto delle piattaforme *online*, la *compliance* non può più essere affrontata separando artificialmente protezione dei dati, *governance* algoritmica e trasparenza dei servizi digitali.

La logica sottesa al DSA appare infatti diversa rispetto all'impostazione tradizionale del GDPR. Quest'ultimo si concentra prevalentemente sulle condizioni di liceità del trattamento; il DSA, invece, interviene anche sulle modalità con cui le piattaforme progettano l'esperienza digitale degli utenti, imponendo vincoli specifici alla pubblicità comportamentale, alla personalizzazione dei contenuti e all'utilizzo dei sistemi di raccomandazione.

Per i fornitori di piattaforme *online*, ciò implica un cambiamento organizzativo significativo. Gli

[3] Per maggiori approfondimenti sul tema, rinviamo al nostro precedente contributo "*DSA: European Commission designated 19 Very Large Online Platforms and Search Engines*".

obblighi di trasparenza non possono essere gestiti esclusivamente attraverso informative privacy o aggiornamenti documentali, ma richiedono interventi sull'interfaccia utente, sulla configurazione dei sistemi di *targeting*, sulla *governance* degli algoritmi e sulla gestione delle preferenze degli utenti.

In questa prospettiva, le Linee Guida sembrano anticipare un approccio regolatorio sempre più orientato non solo alla legittimità del trattamento dei dati, ma alla responsabilizzazione delle piattaforme rispetto agli effetti concreti che determinati modelli di personalizzazione e profilazione possono produrre sugli utenti.

* * *

Cessazione del rapporto di lavoro: come gestire correttamente e-mail e documenti aziendali

Molte imprese ritengono che, una volta cessato il rapporto di lavoro, la posta elettronica aziendale e i documenti presenti sui dispositivi assegnati all'*ex* dipendente rientrino nella piena disponibilità dell'organizzazione.

Il provvedimento del Garante Privacy del 12 marzo 2026 (Provv. 165 del 12 marzo 2026 – doc. web. 1023328) mostra come questa convinzione possa essere fuorviante e, in alcuni casi, esporre l'azienda a rilevanti rischi sanzionatori.

Il caso trae origine dalla richiesta di un *ex* dipendente di accedere ai contenuti della propria casella di posta elettronica aziendale e ai *file* presenti sul *computer* assegnatogli durante il rapporto di lavoro.

La società aveva invece selezionato e limitato i contenuti da fornire, distinguendo tra comunicazioni ritenute "personali" e comunicazioni "di lavoro", oltre ad aver effettuato operazioni di anonimizzazione per tutelare informazioni considerate riservate.

Il Garante ha ritenuto tale approccio non conforme alla normativa, irrogando una sanzione amministrativa di 50.000 euro nei confronti della società coinvolta.

La vicenda offre però spunti che vanno ben oltre il singolo caso. La decisione affronta infatti una questione destinata a interessare trasversalmente imprese di ogni settore: fino a che punto un *ex* dipendente può accedere ai dati contenuti negli strumenti di lavoro utilizzati durante il rapporto? E quali limiti può legittimamente opporre il datore di lavoro?

Il punto di partenza: i dati non "appartengono" all'organizzazione

Uno degli aspetti più rilevanti del provvedimento è il superamento di una visione ancora diffusa nella pratica aziendale, secondo cui i contenuti delle e-mail aziendali sarebbero nella disponibilità esclusiva del datore di lavoro.

Il Garante ribadisce invece che ciò che conta non è il "contesto" lavorativo in cui il dato è generato, ma la sua riconducibilità a una persona fisica identificata o identificabile. In altri termini, anche le comunicazioni avvenute su strumenti aziendali possono costituire dati personali del lavoratore e rientrare pienamente nel perimetro del diritto di accesso.

Questa impostazione si collega a una visione più ampia della protezione dei dati personali, in cui la linea tra dimensione professionale e dimensione privata non è rigida. Anche nel contesto lavorativo, infatti, possono svilupparsi relazioni e contenuti che rientrano nella nozione di "vita privata" e "corrispondenza", tutelati anche a livello europeo (art. 8 della CEDU)[4].

Il diritto di accesso non può essere "filtrato" dall'impresa

Il secondo messaggio chiave del provvedimento riguarda i limiti all'intervento del datore di lavoro sui contenuti richiesti dall'interessato. Nel caso esaminato, la società aveva proceduto a una selezione preventiva delle e-mail, fornendo solo quelle ritenute "personali" e omettendo quelle di natura lavorativa. Inoltre, aveva anonimizzato i contenuti per proteggere informazioni riservate.

Il Garante considera entrambe le attività non conformi. Il diritto di accesso, infatti, comprende l'insieme dei dati personali riferibili all'interessato e non può essere ridotto attraverso una valutazione unilaterale del titolare del trattamento su ciò che è rilevante o meno per il lavoratore.

Le eventuali limitazioni sono possibili solo in presenza di condizioni rigorose, come richieste manifestamente infondate o eccessive, oppure quando sia dimostrato un concreto e attuale pregiudizio ai diritti di terzi, inclusi segreti industriali o diritti di proprietà intellettuale.

In questo punto il provvedimento si allinea alle Linee guida dell'EDPB sul diritto di accesso, che chiariscono come non sia sufficiente un rischio generico o ipotetico di lesione di diritti altrui. È necessario, al contrario, un rischio effettivo e dimostrabile.

Nel caso concreto, il Garante ha rilevato inoltre che i dati di terzi erano già conosciuti dal lavoratore e che la società non aveva dimostrato in modo adeguato l'esistenza di segreti aziendali che potessero essere compromessi dall'accesso.

Correttezza e trasparenza: informative carenti e periodi di conservazione sproporzionati

Accanto al tema del diritto di accesso, il provvedimento affronta un aspetto altrettanto rilevante per le imprese: la gestione della conservazione delle e-mail e dei *log*.

Il Garante ha ritenuto non proporzionati i tempi di conservazione stabiliti dalla società, evidenziando criticità sia sul piano dei *backup* delle e-mail (cinque anni) sia su quello dei *log* di navigazione (dodici mesi).

Il punto centrale non è solo la durata, ma il modello organizzativo sottostante. L'Autorità chiarisce innanzitutto che l'attività di conservazione della posta elettronica aziendale mediante *backup* costituisce un'operazione di trattamento dei dati personali. Dunque, ritenere che la conservazione delle e-mail *offline* non sia un trattamento, è un'interpretazione errata che non tiene conto della più ampia definizione di trattamento prevista dal GDPR.

[4] Corte EDU pronunce Niemietz c. Allemagne, 16/12/1992 (ric. n. 13710/88), spec. par. 29; Copland v. UK, 03/04/2007 (ric. n. 62617/00), spec. par. 41; Bărbulescu v. Romania [GC], 05/09/2017 (ric. n. 61496/08), spec. par. 70-73; Antović and Mirković v. Montenegro, 28/11/2017 (ric. n. 70838/13), spec. par. 41-42; Garante Privacy, Linee guida per la posta elettronica e Internet, dove si legge che "*il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati – riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente […]*"; Garante Privacy, provv.ti: n. 8 del 16/01/2025, doc web n. 10110927; n. 732 del 27/11/2024, doc web n. 10101221; n. 353 del 29/09/2021, doc web n. 9719914.

In secondo luogo, il Garante ribadisce[5] che la posta elettronica aziendale non è uno strumento idoneo a fungere da sistema di archiviazione documentale: affidare ai sistemi di e-mail la conservazione sistematica delle informazioni aziendali comporta inevitabilmente un trattamento esteso e potenzialmente invasivo dei dati personali dei lavoratori.

Ne deriva un'indicazione chiara: le imprese devono dotarsi di sistemi di gestione documentale progettati per finalità di archiviazione, evitando di utilizzare la posta elettronica come archivio.

Quanto ai *log*, il principio è analogo. La loro conservazione è legittima solo se proporzionata alle finalità dichiarate, come la sicurezza informatica o la gestione degli incidenti.

Periodi eccessivamente lunghi devono essere giustificati da esigenze concrete e non generiche (*cfr*. Documento di indirizzo sul trattamento dei metadati – per maggiori approfondimenti rinviamo al nostro contributo "*Posta elettronica e metadati: il nuovo documento di indirizzo del Garante Privacy*").

Profili giuslavoristici

Il provvedimento si inserisce anche nel perimetro della disciplina dei controlli a distanza del lavoratore (art. 4 dello Statuto dei lavoratori).

Sistemi come *backup* massivi delle e-mail o conservazione estesa dei *log* possono infatti, anche indirettamente, consentire un controllo sull'attività lavorativa.

Questo implica che non basta una valutazione in chiave "privacy": è necessario considerare anche le garanzie giuslavoristiche, come la sussistenza di esigenze tassative[6], la necessità di stipulare accordi sindacali o ottenere autorizzazioni amministrative, quando le modalità di trattamento lo richiedano.

Conclusioni: implicazioni per le imprese

Il recente provvedimento del Garante consente di svolgere alcune importanti riflessioni, soprattutto a livello organizzativo. Le imprese devono, infatti, strutturare correttamente i propri processi di gestione dei dati. In concreto, questo significa ripensare tre aspetti spesso dati per scontati:

- la configurazione delle caselle e-mail aziendali, che devono essere gestite come strumenti di lavoro e non come semplici archivi;
- il diritto di accesso, che copre tutti i dati personali del lavoratore, anche dopo la cessazione del rapporto di lavoro;
- i tempi e le modalità di conservazione, che devono essere coerenti con il principio di minimizzazione e con una reale esigenza organizzativa.

In tale ottica e al fine di evitare spiacevoli conseguenze sanzionatorie, sarà necessario rivedere (o definire) policy chiare sull'uso degli strumenti aziendali e sull'esercizio dei diritti degli interessati, evitando di prevedere filtri/dinieghi arbitrari, mantenere aggiornate le informative e riesaminare i periodi di conservazione. Ogni scelta organizzativa – dalla configurazione delle caselle e-mail ai tempi di conservazione – deve essere, infatti, valutata alla luce dei principi del GDPR e progettata *ex ante*.

[5] Sul punto si vedano anche v. provv. n. 732 del 27 novembre 2024, doc web n. 10101221, n. 263 del 22/06/2023, doc. web n. 9920814, provv. n. 53 del 01/02/2018, doc. web n. 8159221 e provv. n. 214 del 29/10/2020 doc. web 9518890.

[6] L'art. 4 dello Statuto dei Lavoratori prevede infatti che gli strumenti dai quali possa derivare la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

NIS2: come impostare la categorizzazione delle attività e dei servizi alla luce della Determinazione ACN 155238/2026

Come preannunciato la scorsa settimana, l'Agenzia per la Cybersicurezza Nazionale ("**ACN**") ha pubblicato nei giorni scorsi la nuova Determinazione 155238/2026 (la "**Determinazione 155238**").

La Determinazione 155238 introduce il modello ufficiale per l'elencazione e la categorizzazione delle attività e dei servizi dei soggetti NIS (c.d. **elenco categorizzato**), definendo criteri, modalità operative e livelli di impatto. A supporto di questo nuovo adempimento, l'ACN ha altresì pubblicato specifiche Linee Guida, volte a chiarire il funzionamento del modello di categorizzazione adottato (le "**Linee Guida**").

Nel linguaggio del Decreto NIS2 (D.Lgs. 138/2024), la "categorizzazione" consiste nell'attribuzione a ciascuna attività o servizio di un livello di rilevanza (alto, medio, basso o minimo) in funzione dell'impatto che una sua compromissione potrebbe avere sulla continuità operativa e sulla capacità del soggetto di erogare servizi NIS.

Attraverso tale classificazione, i soggetti NIS sono chiamati a individuare e classificare le proprie priorità operative, distinguendo le attività e i servizi in base alla loro effettiva criticità, in coerenza con un approccio c.d. *all-hazards* (multi-rischio), che considera non solo le minacce digitali ma anche il contesto operativo complessivo.

La categorizzazione rappresenta dunque lo strumento attraverso cui il legislatore e l'autorità di settore calibrano, in modo proporzionato, gli obblighi di sicurezza. In termini operativi, equivale a rispondere a una domanda chiave per il *business*: "*quali attività sono davvero critiche e con quale priorità devono essere protette?*".

Il contesto di riferimento

Nell'ambito degli adempimenti previsti dal Decreto NIS2, i soggetti "essenziali" e "importanti", a partire dalla ricezione della comunicazione di inclusione nell'elenco dei soggetti NIS, sono tenuti – dal **1° maggio al 30 giugno di ogni anno** – a trasmettere tramite la piattaforma ACN l'elenco aggiornato delle attività e dei servizi, comprensivo degli elementi necessari alla loro categorizzazione e della relativa categoria di rilevanza.

L'elenco categorizzato non rappresenta, quindi, un mero adempimento informativo. Esso costituisce la base su cui verranno calibrate le **misure di sicurezza c.d. a lungo termine**, attese entro la fine del 2026, che si aggiungeranno a quelle "di base" già definite con la Determinazione 379907/2025[7]. Ciò significa che la categorizzazione inciderà direttamente sull'intensità e sull'estensione degli obblighi futuri, quantomeno in materia di misure di sicurezza.

[7] Per maggiori approfondimenti, si rinvia alle nostre *slide* pubblicate su LinkedIn e disponibili al seguente *link*: https://www.linkedin.com/feed/update/urn:li:activity:7374021071991242753/, nonché al nostro precedente contributo "*NIS2: dalla compliance formale alla responsabilità **operativa**. Cosa cambia dopo le ultime Determinazioni e Linee Guida dell'ACN*".

Il modello di elenco adottato dall'ACN

L'elenco deve essere predisposto in base al modello di categorizzazione elaborato dall'ACN (il "**Modello**").

I soggetti operanti nei settori dell'energia, dei trasporti, della sanità, dell'acqua potabile, delle acque reflue, dello spazio, nonché negli "altri settori critici" di cui all'Allegato II del Decreto NIS2 (quali, ad esempio, servizi postali e gestione dei rifiuti), oltre ai servizi di trasporto pubblico locale, devono utilizzare il modello di cui Allegato 1 alla Determinazione 155238. Tutti gli altri soggetti NIS (tra cui il settore bancario e dei servizi finanziari, le infrastrutture digitali come *data center* e servizi *cloud* e i fornitori di servizi ICT *business-to-business*) devono invece fare riferimento al Modello di cui all'Allegato 2.

Il Modello organizza attività e servizi in **10 macro-aree** (monitoraggio e controllo; produzione di beni e servizi; ricerca, sviluppo e progettazione; gestione finanziaria; gestione dei clienti; gestione delle risorse umane; logistica; comunicazione e *marketing*; gestione amministrativa; altri servizi e attività[8]), ciascuna caratterizzata da una denominazione, una descrizione e una categoria di rilevanza preassegnata.

La **categoria di rilevanza** – articolata in impatto "**alto**", "**medio**", "**basso**" o "**minimo**" – esprime l'impatto che una possibile compromissione dell'attività o del servizio potrebbe avere sulla capacità del soggetto di svolgere correttamente le attività e i servizi NIS. Per ciascuna macro-area, l'ACN ha già formulato una valutazione *standard*, attribuendo una categoria di rilevanza "*di default*".

Cosa devono fare in concreto i soggetti NIS

I soggetti NIS, tramite il proprio Punto di Contatto, devono accedere alla piattaforma ACN, predisporre l'elenco e attribuire la categoria di rilevanza a tutte le attività e ai servizi erogati, sia internamente sia verso l'esterno.

Le Linee Guida articolano il processo in 3 fasi:

1. identificazione attività/servizi

Occorre individuare tutte le attività svolte e i servizi erogati che risultano supportati, svolti o erogati da sistemi informativi e di rete, anche valorizzando analisi già disponibili (quali *risk assessment* o *business impact analysis*). Le Linee Guida ammettono sia un approccio *top-down* (individuando attività/servizi a partire da funzioni e processi) sia *bottom-up* (a partire dagli *asset* IT), anche in forma combinata.

Pur non essendo richiesto un livello di dettaglio predeterminato, la scelta della granularità è un passaggio rilevante: ogni attività o servizio sarà associato a **una sola categoria di rilevanza** (impatto alto, medio, basso o minimo).

È quindi opportuno individuare attività/servizi sufficientemente omogenei, evitando sia aggregazioni eccessive (che appiattiscono il rischio) sia frammentazioni artificiose: il livello di dettaglio deve consentire di distinguere funzioni con profili di rischio differenti, senza compromettere la sostenibilità operativa del processo.

In molti casi, un numero di attività/servizi allineato alle categorie di rilevanza previste dal Modello rappresenta un buon punto di equilibrio.

[8] Come precisato dalle Linee Guida, questa macro-area deve essere utilizzata se il soggetto NIS ritiene che una determinata attività o un determinato servizio non rientrino in alcuna delle altre macro-aree.

2. Mappatura attività/servizi in macro-aree

Le attività e i servizi individuati devono poi essere associate, in base alla natura dell'attività o del servizio, alle funzioni organizzative coinvolte e ai processi di *business*, a una delle 10 macro-aree che ne rappresenta meglio le finalità e le caratteristiche.

Qualora un'attività presenti caratteristiche trasversali, le Linee Guida richiedono di procedere alla sua scomposizione, al fine di garantire un'associazione univoca. Non è invece necessario valorizzare tutte le macro-aree, ove non pertinenti rispetto all'operatività del soggetto.

3. Attribuzione categoria di rilevanza

In via generale, le attività e i servizi acquisiscono la categoria di rilevanza **preassegnata** alla macro-area di riferimento (es., produzione di beni e servizi – impatto medio)[9].

Tuttavia, il soggetto NIS può discostarsi da tale classificazione, sulla base di una **valutazione dell'impatto** concreto che una loro compromissione determinerebbe sulla continuità delle attività e dei servizi NIS. In coerenza con il principio di *accountability*, tale scelta richiede un adeguato supporto documentale.

In termini pratici, questo è il momento in cui la categorizzazione diventa una vera valutazione di rischio: discostarsi dal *default* è possibile, ma solo se si è in grado di dimostrare – anche *ex post* – la razionalità della scelta.

Conclusioni

La sequenza degli adempimenti NIS2 si sta progressivamente completando: alla registrazione 2025 e agli obblighi di notifica operativi da gennaio 2026, si affiancano l'aggiornamento annuale delle informazioni (inclusi i fornitori rilevanti), la predisposizione dell'elenco categorizzato, l'adozione delle misure di sicurezza di base entro ottobre 2026 e, successivamente, l'introduzione delle misure a lungo termine.

In questo contesto, la categorizzazione rappresenta un passaggio centrale. Non solo perché è funzionale agli obblighi successivi, ma anche perché richiede alle organizzazioni di distinguere, al proprio interno, i diversi livelli di esposizione al rischio delle attività e dei servizi supportati dai sistemi informativi e di rete.

Il principio di *accountability* impone agli organi amministrativi e direttivi del soggetto NIS una responsabilizzazione diretta anche nel processo di categorizzazione: in questa prospettiva, la *Business Impact Analysis* e la documentazione a supporto delle scelte classificatorie assumono la funzione di strumenti di *governance* del rischio, oltre che di elementi probatori in sede di vigilanza.

Affrontare questo esercizio in modo meramente formale rischia, quindi, di generare classificazioni poco utili e difficilmente sostenibili, oltre a esporre il soggetto a potenziali violazioni della normativa e alle conseguenti sanzioni.

Al contrario, un'impostazione integrata con i processi di gestione del rischio e di *governance* IT consente di trasformare l'adempimento in uno strumento effettivo di supporto alle decisioni, in vista delle ulteriori evoluzioni regolatorie attese nei prossimi mesi.

[9] L'Allegato B alle Linee Guida indica le motivazioni che hanno portato l'ACN a pre-assegnare le categorie di rilevanza alle macro-aree del Modello.

Per maggiori informazioni e approfondimenti

Carlo Impalà

Partner e Responsabile Osservatorio TMT&DP

Carlo.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