OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Ottobre 2025

Ottobre 2025

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

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Siti e app per bambini, in corso l'indagine internazionale. Fino al 7 novembre, l'iniziativa organizzata dal Global privacy enforcement network; [Link]

EDPB

- Orientamenti congiunti sull'interazione tra il Digital Markets Act (DMA) e il Regolamento generale sulla protezione dei dati (GDPR); [Link]
- Opinion 26/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by the United Kingdom; [Link]
- Opinion 28/2025 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data by Brazil. [Link]

AGCOM

- Age verification: dal 12 novembre in vigore gli obblighi per i siti e le piattaforme che diffondono contenuti pornografici; [Link]
- Approvate le nuove Linee guida in materia di prominence dei servizi di media audiovisivi e radiofonici di interesse generale; [Link]
- L'Autorità individua i mercati che compongono il Sistema Integrato delle Comunicazioni (SIC). [Link]

Moderazione dei contenuti e trattamento dei dati personali: l'interazione tra gli obblighi del DSA e quelli del GDPR

Il DSA, entrato pienamente in vigore il 17 febbraio 2024, istituisce un quadro uniforme per i servizi di intermediazione nel mercato digitale, volto a creare un ambiente online sicuro e affidabile e a contrastare la diffusione di contenuti illegali e disinformazione.

Le norme del DSA riguardano principalmente ai servizi intermediari di mere conduit, caching e hosting, vale a dire i servizi online, semplici siti web, di infrastruttura Internet e piattaforme online (market place, social network, piattaforme di condivisione di contenuti, app store, etc.).

Il DSA prevede tuttavia norme specifiche e obblighi più rigorosi per VLOP e VLOSE, ossia piattaforme online e intermediari che hanno più di 45 milioni di utenti al mese.

È ben noto ormai come i servizi digitali incidono profondamente sulla nostra quotidianità. Li utilizziamo per comunicare, fare acquisti, ordinare cibo, reperire informazioni, guardare film, ascoltare musica e molto altro, favorendo gli scambi commerciali tra diversi Paesi e permettendo alle imprese di raggiungere nuovi mercati.

Tuttavia, accanto ai numerosi vantaggi offerti dalla trasformazione digitale, emergono anche diverse criticità che incidono direttamente sui diritti fondamentali degli utenti, tra cui la protezione dei dati.

In tale contesto si inseriscono le Linee Guida dell'EDPB 03/2025 volte a chiarire il rapporto tra il DSA e il GDPR, al fine di garantire un'applicazione coerente e armonizzata delle due normative.

Infatti, il rapporto tra DSA e GDPR è di complementarità, non di sostituzione: il primo tutela il corretto funzionamento del mercato digitale, il secondo la protezione dei dati personali.

Le linee guida dell'EDPB intendono dunque orientare i fornitori di servizi di intermediazione nell'applicazione del GDPR nei contesti disciplinati dal DSA, promuovendo una lettura coordinata delle due discipline per garantire un ambiente digitale conforme ai principi di liceità, proporzionalità e trasparenza.

Tra le principali disposizioni del DSA, vi è la moderazione "volontaria" dei contenuti online e il meccanismo di "*notice and action*". Entrambi, tuttavia, comportano molto frequentemente il trattamento dei dati personali.

Moderazione "volontaria" dei contenuti online

Ai sensi dell'art. 7 del DSA, è prevista la possibilitàper i fornitori di servizi di mere conduit, di caching e di hosting ("**Fornitori**") di svolgere indagini volontarie di propria iniziativa o di adottare misure idonee a identificare e rimuovere contenuti illegali o disabilitare l'accesso agli stessi.

Queste azioni possono essere svolte mediante l'ausilio di tecnologie di *machine learning*, in grado di riconoscere le caratteristiche di un determinato contenuto sulla base delle grandi quantità di dati utilizzati per l'addestramento.

Ovviamente, ciò comporta il trattamento di dati personali e dunque la necessità dei Fornitori di conformarsi alle disposizioni del GDPR, tra cui quelle relative alla liceità, correttezza e trasparenza nei confronti degli interessati, nonché alla minimizzazione dei dati e agli obblighi di privacy by design by default.

A tal fine, l'EDPB chiarisce che le indagini volontarie per identificare e rimuovere i contenuti illegali possono essere svolte sulla base delle seguenti basi giuridiche:

- l'obbligo legale (art. 6(1)(c) GDPR), quando la rimozione è imposta dalla legge;
- l'interesse legittimo (art. 6(1)(f) GDPR), quando il Fornitore agisce per tutelare i propri utenti o il proprio servizio.

In quest'ultimo caso, il Fornitore deve altresì soddisfare tre condizioni cumulative da documentare nel *legitimate interest assessment* (cd. "**LIA**"):

1. l'interesse perseguito deve essere legittimo;
2. il trattamento dei dati personali deve essere necessario per perseguire tale interesse legittimo, non potendo questo essere raggiunto altrettanto efficacemente con mezzi alternativi;
3. gli interessi o i diritti e le libertà fondamentali degli interessati non devono prevalere sull'interesse legittimo perseguito dal titolare.

Meccanismo di "notice and action" o obbligo di motivazione

L'articolo 16 del DSA impone ai fornitori di servizi di hosting, comprese le piattaforme online, di istituire meccanismi di segnalazione (cd. "*notice and action*") che permettano a chiunque di notificare, in via elettronica, la presenza di contenuti illegali. Ricevuta la segnalazione, il fornitore può decidere se intervenire, ad esempio rimuovendo o limitando il contenuto.
Tali sistemi implicano il trattamento di dati personali del "segnalatore", dei destinatari del servizio e, talvolta, di terzi.

In particolare, le Linee Guida richiamano l'esigenza di un trattamento proporzionato e limitato alle finalità del DSA, prevedendo che i fornitori (in qualità di titolari del trattamento) debbano:

- raccogliere e trattare solo i dati strettamente necessari alla finalità perseguita;
- identificare il segnalante solo in modo facoltativo, ad eccezione del caso in cui l'identificazione sia strettamente necessaria per qualificare un contenuto come "illegale";
- informare il segnalante in modo trasparente e chiaro se la sua identità viene comunicata all'utente coinvolto.

Il DSA consente inoltre l'uso di sistemi automatizzati per la gestione delle segnalazioni, purché i segnalatori siano informati in conformità all' art. 13 del GDPR.

Se tali decisioni rientrano nell'ambito dell'art. 22 del GDPR, devono essere rispettate garanzie stringenti, tra cui essere autorizzate da una norma UE o nazionale, tutelare i diritti degli interessati e non basarsi su dati di categoria particolare, salvo consenso esplicito o motivi di interesse pubblico rilevante.

Infine, l'art. 17 del DSA obbliga i fornitori di hosting a trasmettere agli utenti una motivazione chiara e dettagliata per ogni decisione di rimozione o limitazione di un contenuto, specificando l'eventuale uso di sistemi automatizzati, la base giuridica dell'intervento e le possibilità di ricorso.

Tale obbligo non si applica alle rimozioni disposte dalle autorità competenti.

Inoltre, nel quadro delle attività volte a contrastare i contenuti illegali, la Sezione 3 del Capitolo III del DSA impone solo ai fornitori di piattaforme online alcuni obblighi aggiuntivi che possono comportare il trattamento di dati personali.

Ai sensi dell'articolo 20 del DSA, sia i destinatari interessati dalle decisioni riguardanti l'illegalità dei contenuti o la loro incompatibilità con i termini e le condizioni delle piattaforme online, sia gli individui (o enti) che hanno presentato una segnalazione, hanno il diritto di presentare un reclamo per, rispettivamente, contestare una decisione che li riguarda negativamente oppure contestare una presunta azione inadeguata intrapresa sulla base della segnalazione effettuata.

L'EDPB accoglie con favore il fatto che, in entrambi i casi, il DSA preveda che i fornitori di piattaforme online garantiscano che le decisioni di cui all'art. 20 del DSA siano adottate sotto la supervisione di personale adeguatamente qualificato e non esclusivamente sulla base di mezzi automatizzati.

Inoltre, considerando che "*l'uso improprio delle piattaforme online attraverso la frequente diffusione di contenuti manifestamente illegali o la frequente presentazione di segnalazioni o reclami manifestamente infondati [...] mina la fiducia e danneggia i diritti e gli interessi legittimi delle parti coinvolte*", l'art. 23 del DSA consente alle piattaforme online di sospendere le relative attività nei confronti della persona che si è resa responsabile di un comportamento abusivo (ossia i destinatari che forniscono frequentemente contenuti manifestamente illegali e i segnalanti o i reclamanti che presentano frequentemente segnalazioni o reclami manifestamente infondati).

Pur prevedendo garanzie contro l'uso improprio delle piattaforme online, il DSA stabilisce anche che tali garanzie debbano essere "appropriate, proporzionate ed efficaci" e debbano "rispettare i diritti e gli interessi legittimi di tutte le parti coinvolte, inclusi i diritti e le libertà fondamentali applicabili sanciti nella Carta".

A questo riguardo, l'EDPB accoglie con favore le garanzie già individuate dal DSA, in quanto consentiranno di evitare l'adozione di decisioni automatizzate in tali casi, e richiama i fornitori di piattaforme online a tenere conto, nell'identificare le misure per contrastare gli abusi e nel definire nelle loro condizioni d'uso la relativa politica, della necessità di garantire il rispetto di tutti i principi in materia di protezione dei dati stabiliti dall'articolo 5 del GDPR e, in particolare, dei principi di minimizzazione, esattezza, trasparenza e limitazione della conservazione dei dati.

Conclusioni

L'analisi del rapporto tra DSA e GDPR evidenzia chiaramente come le due normative non vadano considerate in alternativa, bensì in un rapporto di complementarità.

Il DSA mira a garantire un ecosistema digitale più sicuro, trasparente e responsabile, mentre il GDPR continua a costituire il riferimento primario per la tutela dei dati personali degli utenti.

La moderazione dei contenuti e l'implementazione dei meccanismi di notice and action richiedono quindi un approccio integrato, in cui principi di liceità, proporzionalità, minimizzazione e trasparenza guidino ogni fase del trattamento dei dati.

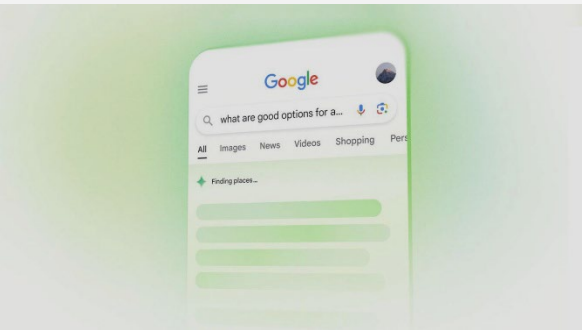
Per le aziende rientranti nell'ambito di applicazione del DSA, emerge la necessità di adottare processi strutturati e misure di

governance solide. In concreto, è possibile individuare alcune priorità operative, tra cui:

- **la mappatura dei trattamenti collegati alla moderazione dei contenuti**: le imprese dovrebbero aggiornare il proprio registro dei trattamenti, identificando chiaramente le operazioni legate sia alle indagini volontarie sia ai meccanismi di segnalazione, includendo le basi giuridiche utilizzate, le categorie di dati trattati, i tempi di conservazione, nonché gli eventuali sistemi automatizzati.
- **LIA e DPIA:** quando si fa ricorso all'interesse legittimo, è necessario documentarlo in modo rigoroso attraverso una LIA e, ove siano impiegate tecnologie di *machine learning* o moderazione automatizzata, svolgere una DPIA.
- **Informativa agli utenti:** le informative privacy e i termini di servizio devono essere rivisti in ottica DSA.
- **Sistemi di gestione dei reclami e delle contestazioni (art. 20 DSA)**: le piattaforme devono predisporre canali efficaci e accessibili per (i) consentire agli utenti di contestare la rimozione o la limitazione di contenuti e (ii) consentire ai segnalanti di contestare l'inerzia o l'inefficacia della risposta.

* * *

Google AI Overviews: quando l'innovazione rischia di diventare abuso



C'è un'immagine che restituisce bene la sensazione degli editori – e non solo degli editori – di fronte all'ultima evoluzione del motore di ricerca più potente del mondo: quella di un **ecosistema informativo che si svuota di senso mentre in apparenza resta intatto.** Le notizie continuano a esistere, i siti sono accessibili, le parole scorrono sugli schermi, ma qualcosa si è incrinato nel modo in cui l'informazione viene trovata, letta e, soprattutto, mediata.

Con il reclamo presentato il 15 ottobre 2025 dalla FIEG (Federazione Italiana Editori Giornali) all'Agcom, nel ruolo di Coordinatore nazionale dei servizi digitali ai sensi dell'art. 49 del Reg. UE 2022/2065 (Digital Services Act), l'editoria italiana ha voluto dire con forza che, a suo avviso, **il confine tra innovazione e abuso è stato superato**.

Il bersaglio è AI Overviews e la sua evoluzione AI Mode, le nuove funzioni di **Google Search** che, attraverso l'intelligenza artificiale generativa del modello *Gemini*, elabora un "riassunto intelligente" dei risultati, offrendo una risposta autonoma nella parte alta della SERP, spesso prima dei collegamenti ai siti editoriali.

Questo processo tende a mantenere gli utenti dentro l'ecosistema Google, riducendo la visibilità e l'accesso diretto alle fonti primarie, sollevando diverse questioni giuridiche, come la **violazione**

del diritto d'autore, degli **obblighi di trasparenza del DSA** e **possibili abusi di posizione dominante**.

La posta in gioco è complessa e richiede un bilanciamento tra interessi legittimi ma potenzialmente confliggenti: l'UE saprà applicare in modo coerente e unitario le diverse normative coinvolte (DSA, DMA, GDPR, direttiva copyright e normativa antitrust) per governare la società digitale? Ne abbiamo parlato su: AI4Business – Network360

* * *

Proteggere i minori nel digitale: le linee guida della Commissione europea sul DSA

Negli ultimi anni, il dibattito sulla protezione dei minori *online* si è spostato da un piano puramente etico a uno sempre più regolamentato e tecnico. Con la pubblicazione, lo scorso 10 ottobre, della versione definitiva delle linee guida sulla protezione dei minori (le "**Linee Guida**") ai sensi del *Digital Services Act* ("**DSA**" – Regolamento UE 2022/2065), la Commissione europea ha definito degli *standard* per valutare la conformità all'art. 28, par. 1, del DSA, ossia l'obbligo per le piattaforme *online* di garantire ai minori un livello elevato di tutela, sicurezza e *privacy*.

L'obiettivo delle Linee Guida è quello di sostenere le piattaforme *online* accessibili ai minori a far fronte a tali rischi, individuando una serie di misure – a carattere non esaustivo – volte a contribuire alla protezione dei minori.

Ma quando una piattaforma *online* si considera "accessibile ai minori"?

Non è sufficiente scrivere nelle condizioni generali che il servizio è "vietato ai minori". Le Linee Guida ritengono che una piattaforma *online* possa essere considerata accessibile ai minori se:

a. consente di fatto l'accesso ai minori, senza prevedere misure efficaci per impedirne l'accesso; o
b. è utilizzata o indirizzata prevalentemente a minori; o
c. il *provider* sa o è in grado di sapere che parte dell'utenza è minorenne (ad es., piattaforma che tratta dati degli utenti in grado di rivelarne l'età o piattaforma popolare tra i minori).

Quali sono le misure di sicurezza individuate nelle Linee Guida?

Le Linee Guida individuano diverse misure volte a garantire la protezione dei minori *online*:

(i) *Risk assessment*

Le Linee Guida suggeriscono alle piattaforme *online* di svolgere una valutazione del rischio: non si tratta solo di mappare i contenuti illegali, ma di capire come i minori interagiscono con la piattaforma, quali rischi incontrano e quanto sono efficaci le misure già in atto. La valutazione dovrà essere conforme alle norme e alle *best practices* esistenti[1], aggiornata almeno ogni anno e resa pubblica in forma

[1] Le Linee Guida richiamano i modelli, i moduli e gli altri orientamenti forniti dall'UNICEF (ad es., https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA), dal ministero neerlandese degli Affari interni e delle relazioni del Regno o dall'organismo europeo di

sintetica, indicando il rischio per i minori (ad es., basso, medio o alto).

(ii) Misure di *age assurance*

Per rendere le piattaforme più sicure – e per evitare che i minori utilizzino servizi non adatti alla loro età – è importante sapere se gli utenti hanno l'età sufficiente per accedere a determinati contenuti.

La verifica dell'età consiste nell'utilizzare strumenti che permettono di determinare o stimare l'età di un utente, oppure di confermare se una persona ha un'età superiore o inferiore a una determinata soglia.

Le Linee Guida individuano tre misure di *age assurance* più comuni:

a. **autodichiarazione**: metodo che richiede ai singoli utenti di comunicare la propria età o di confermare la propria fascia d'età. Si tratta di un metodo rapido, ma facile da aggirare: le Linee Guida, infatti, non considerano l'autodichiarazione come misura adeguata ad accertare l'età;
b. **stima dell'età**: questa tecnologia stima l'età in base a elementi come scansioni del volto, stile di digitazione, interessi o attività *online*. Esso potrebbe comportare inesattezze e risultare invasivo per la *privacy*;
c. **verifica dell'età**: metodo più preciso, in grado di controllare l'età usando documenti ufficiali (ad es., passaporto, carta d'identità), o identificativi digitali affidabili (es., ID emesso dal governo o EU *Digital Identity Wallet*[2]).

Nello scegliere la metodologia da applicare, occorre seguire il criterio della proporzionalità: le piattaforme dovrebbero usare metodi più rigorosi solo dove il rischio è più alto (come per il gioco d'azzardo o le *chat* anonime)[3], senza richiedere più informazioni del necessario[4]. Le piattaforme dovranno inoltre spiegare in modo chiaro e trasparente come e perché si chiede l'età, offrendo sempre più di un'opzione, nonché un canale di reclamo[5].

normazione CEN-CENELEC. Mentre per quanto riguarda le piattaforme e i motori di ricerca online di dimensioni molto grandi, tale analisi dei rischi potrà essere effettuata anche nell'ambito della valutazione generale dei rischi sistemici di cui all'art. 34 del DSA.

[2] Una volta implementati, i portafogli europei di identità digitale offriranno mezzi di identificazione elettronica sicuri, affidabili e privati per tutti nell'Unione. Ogni Stato membro è tenuto a fornire a tutti i suoi cittadini, residenti e imprese almeno un portafoglio, che dovrebbe consentire loro di dimostrare la loro identità e di conservare, condividere e firmare in sicurezza documenti digitali importanti entro la fine del 2026. Prima che diventino disponibili i portafogli europei di identità digitale, la Commissione sta sperimentando una soluzione europea di verifica dell'età (sotto forma di app) in grado unicamente di confermare se l'utente ha più di 18 anni, che, una volta ultimata, costituirà un esempio di conformità e uno standard di riferimento per i metodi di verifica dell'età.

[3] Le Linee Guida sottolineano come sia possibile solo alcuni contenuti, sezioni o funzioni della piattaforma rappresentino un rischio per i minori, oppure che vi siano parti in cui il rischio può essere attenuato mediante altre misure e/o parti in cui ciò non è possibile. In questi casi, anziché imporre limiti di età per l'accesso al servizio nel suo complesso, i fornitori di tali piattaforme online dovrebbero valutare quali contenuti, sezioni o funzioni sulla loro piattaforma comportano rischi per i minori e attuare restrizioni di accesso sostenute da metodi di accertamento dell'età per ridurre tali rischi per i minori in modo proporzionato e adeguato. Ad esempio, le Linee Guida ritengono il sistema di verifica dell'età proporzionato per l'accesso a contenuti relativi al gioco d'azzardo, o se, a causa dei rischi individuati per i minori, le condizioni generali impongono all'utente di avere almeno 18 anni per accedere al servizio, oppure se vengano individuati rischi legati a contenuti e comportamenti e rischi per i consumatori o rischi di contatto (es., funzioni come conversazioni via chat, messaggistica anonima, condivisione di immagini/video), se i rischi non possano essere attenuati con misure meno invasive, oppure se la normativa europea o nazionale prescrive l'obbligo di un'età minima per accedere a determinati prodotti o servizi. Al contrario sarà considerato proporzionato l'utilizzo di un sistema di stima dell'età se a causa dei rischi individuati, le condizioni generali della piattaforma impongono all'utente di superare l'età minima richiesta inferiore ai 18 anni per accedere al servizio, oppure se la piattaforma abbia individuato rischi medi per i minori sulla propria piattaforma e tali rischi non possono essere attenuati da misure meno restrittive.

[4] Nel considerare i metodi di stima dell'età che richiedono il trattamento di dati personali, i fornitori di piattaforme online accessibili ai minori dovrebbero garantire che i principi di protezione dei dati, in particolare la minimizzazione dei dati, siano attuati correttamente e rimangano solidi nel tempo, nonché tenere conto della Dichiarazione/2025 dell'EDPB sulla garanzia dell'età. In particolare, la verifica dell'età dovrebbe essere trattata come processo separato e distinto, non collegato ad altre attività di raccolta dei dati delle piattaforme online e non dovrebbe consentire di conservare dati personali al di là delle informazioni sulle fasce d'età.

[5] Le Linee Guida precisano che tale sistema potrebbe anche essere integrato nel sistema interno di gestione dei reclami (art. 20 del DSA).

(iii) Registrazione, impostazioni dell'*account*, progettazione delle interfacce e altri strumenti

Le Linee Guida ritengono che, una volta che il *provider* della piattaforma ritenga necessario procedere con l'accertamento dell'età, la registrazione o l'autenticazione possono essere un primo elemento da utilizzare per svolgere tale processo in modo proporzionato.

Le Linee Guida sottolineano inoltre l'importanza del *design* della piattaforma e di come impostazioni predefinite costituiscano uno strumento utile per attenuare i rischi: la maggior parte degli utenti, infatti, non modifica le impostazioni di *default*, le quali diventano fondamentali nell'indirizzare il comportamento dei minori.

Ciò significa, ad esempio, prevedere impostazioni di *privacy* restrittive *by default* (ad es., controllando chi può seguire o inviare messaggi al minore), disattivare in automatico funzioni rischiose (come la geolocalizzazione, la riproduzione automatica dei video, il microfono e fotocamera, la sincronizzazione dei contatti e il tracciamento), prevedere interfacce che non inducano dipendenza (come lo *scrolling* infinito, le notifiche constanti, la riproduzione automatica di video), oppure implementare strumenti di aiuto facili da trovare e utilizzare.

(iv) Sistemi di raccomandazione e pratiche commerciali

Le Linee Guida dedicano molta attenzione alle pratiche commerciali e ai sistemi di raccomandazione[6].

I minori sono particolarmente vulnerabili alle logiche persuasive: non sempre distinguono tra contenuto e pubblicità, tra suggerimento e manipolazione.

Per tale motivo, le Linee Guida raccomandano di spiegare perché un contenuto è stato raccomandato, permettendo agli utenti di reimpostare il proprio *feed* e prevedono, tra l'altro, che le pubblicità o i contenuti sponsorizzati (ad es., tramite *influencer*) debbano essere chiaramente riconoscibili, che gli algoritmi non amplifichino contenuti dannosi o inadatti all'età e che i sistemi di IA non vengano usati come strumenti di influenza o vendita verso i minori (ad es., tramite *chatbot*).

(v) Moderazione dei contenuti

La moderazione consiste nel controllare e rimuovere contenuti o utenti che potrebbero danneggiare la *privacy*, la sicurezza e la protezione dei minori. Si tratta di uno strumento importante per proteggere gli utenti e prevenire rischi gravi come il bullismo, l'esposizione a contenuti dannosi o il *grooming*[7].

In tale ottica, le Linee Guida prevedono che le piattaforme dovrebbero, tra gli altri, definire chiaramente cosa si intende per contenuti e comportamenti dannosi e adottare specifiche procedure e *policy*, utili anche per rimuovere rapidamente contenuti e *account* dannosi o illegali, garantire sempre la verifica umana dei contenuti (in aggiunta a quella automatizzata), formare i moderatori, adottare soluzioni tecniche di protezione per impedire che i sistemi di IA permettano la creazione o la diffusione di contenuti dannosi e rivedere e migliorare regolarmente il funzionamento dei sistemi di moderazione.

[6] Si tratta di quei sistemi che determinano il modo in cui le informazioni sono messe in ordine di priorità, ottimizzate e mostrate ai minori. Per maggiori approfondimenti si rinvia ad un nostro precedente contributo, disponibile su AgendaDigitale.

[7] Si tratta di quei casi in cui qualcuno cerca di diventare amico di un minore per ingannarlo o metterlo a disagio.

Cosa comporta tutto ciò per le piattaforme *online*?

Per le piattaforme *online* la sfida è duplice: da un lato, garantire l'efficacia tecnica delle misure (verifica dell'età, moderazione, sistemi di raccomandazione trasparenti), dall'altro, mantenere un equilibrio con i diritti fondamentali, la *privacy* e l'esperienza d'uso.

In attesa che i sistemi di *age verification* maturino e diventino interoperabili a livello europeo, le piattaforme dovranno mappare i rischi per i minori, documentare le proprie scelte e rendere pubblica la propria valutazione.

Occorrerà adottare condizioni generali "a misura di minore" e descrivere i servizi in maniera chiara e semplice, comprensibili anche per i minori (ad esempio, potrebbe essere utile utilizzare delle infografiche).

In definitiva e come affermato nelle Linee Guida, le piattaforme *online* dovranno mettere in atto una vera e propria *governance* per garantire la protezione dei minori, con ruoli, *policy* e formazione dedicati.

* * *

NIS2 e gestione degli incidenti: l'ACN introduce il Referente CSIRT

Inizia ad avvicinarsi la scadenza, prevista per **gennaio 2026**, per il rispetto da parte delle imprese qualificate come "soggetti essenziali" o "soggetti importanti" (i "**Soggetti NIS**") degli obblighi in materia di **incidenti di sicurezza** di cui al D.Lgs. 138/2024 ("**Decreto NIS2**").

In questo contesto, lo scorso 3 ottobre, l'Autorità per la Cybersicurezza Nazionale ("**ACN**") ha pubblicato la Determinazione n. 333017/2025 (la "**Determinazione**"), che aggiorna e sostituisce la precedente Determinazione 283727/2025.

La novità principale è l'introduzione della figura del "**Referente CSIRT**".

Chi è il Referente CSIRT?

Il CSIRT Italia (*Computer Security Incident Response Team*) è l'organismo tecnico nazionale, che opera presso l'ACN, con il compito di prevenire, analizzare e gestire gli incidenti informatici che colpiscono reti e infrastrutture strategiche.

I principali compiti del CSIRT includono il monitoraggio e l'intervento in caso di incidenti a livello nazionale, la pubblicazione di campagne di sensibilizzazione, nonché l'emissione di preallarmi o *alert* alle parti interessate in merito ai rischi e agli incidenti.

La Determinazione introduce, nel contesto di ogni organizzazione soggetta al Decreto NIS2, la figura del Referente CSIRT.

Si tratta di una persona fisica designata dal punto di contatto, ossia da quel soggetto espressamente designato come tale dai Soggetti NIS [8], con il compito di procedere alla registrazione dell'organizzazione sul portale dell'ACN e a interloquire con l'Autorità.

A differenza del punto di contatto, il Referente CSIRT non deve necessariamente far parte dell'organizzazione.

La Determinazione, infatti, non prescrive nulla sul punto, limitandosi a richiedere che il referente sia dotato di specifiche competenze in materia di sicurezza informatica e di gestione degli incidenti, e formalmente autorizzato ad agire in nome e per conto del Soggetto NIS.

La Determinazione consente anche la nomina di uno o più sostituti, che dovranno possedere le stesse competenze tecniche e conoscenza dei sistemi informavi del Soggetto NIS per cui operano.

Quali sono i compiti del Referente CSIRT?

Il Referente CSIRT è il punto di collegamento operativo con il CSIRT Italia per tutte le notifiche relative agli incidenti di sicurezza (artt. 25 e 26 del Decreto NIS2). In particolare, i Soggetti NIS dovranno:

a. inviare una **pre-notifica entro 24 ore** dalla conoscenza dell'incidente significativo, indicando, se possibile, la natura dell'incidente (malevola o meno) e l'eventuale impatto transfrontaliero;
b. trasmettere una **notifica completa entro 72 ore** (o 24 ore per i prestatori di servizi fiduciari). Attraverso questa notifica, se possibile, occorrerà aggiornare le informazioni trasmesse con la pre-notifica e indicare una valutazione iniziale dell'incidente, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
c. inviare una **relazione finale entro un mese** dalla trasmissione della notifica di incidente.

In fase di prima applicazione del Decreto NIS2, i Soggetti NIS "importanti" dovranno notificare al CSIRT Italia le tipologie di incidenti significativi riportate nell'allegato 3 della Determinazione dell'ACN n. 164179/2025, mentre i Soggetti NIS "essenziali" seguiranno l'elenco dell'allegato 4.

Inoltre, su base volontaria, i Soggetti NIS potranno notificare al CSIRT Italia anche le minacce informatiche [9] e i quasi-incidenti (c.d. *near-miss*), ossia quegli eventi che avrebbero potuto sfociare in un incidente ma che, tuttavia, non si è verificato, inclusi i casi in cui l'incidente sia stato efficacemente evitato.

Cosa devono fare i Soggetti NIS?

Dal 20 novembre al 31 dicembre 2025, sempre attraverso il portale dell'ACN, le imprese rientranti nel perimetro di applicazione del Decreto NIS2 dovranno procedere alla designazione del Referente CSIRT.

Nel caso in cui i Soggetti NIS decidano di affidare il ruolo a un soggetto esterno, dovranno regolare l'incarico con un apposito contratto di *outsourcing*, che definisca in modo chiaro

[8] Il ruolo di punto di contatto può essere ricoperto dal rappresentante legale del Soggetto NIS, da uno dei suoi procuratori generali censiti sul registro delle imprese, oppure da un suo dipendente (o un dipendente di un'altra impresa del gruppo che rientra nell'ambito di applicazione del Decreto NIS2) appositamente delegato dal rappresentante legale.

[9] Il Decreto NIS2 definisce "minacce informatiche" quelle circostanze, eventi o azioni che potrebbero danneggiare, perturbare o avere un impatto negativo sui sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone.,

responsabilità, obblighi di riservatezza, modalità di accesso ai sistemi informatici aziendali e tempi di risposta in caso di incidente.

Sarà importante, inoltre, chiarire i ruoli privacy delle parti e la titolarità delle comunicazioni trasmesse al CSIRT Italia.

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