OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Dicembre ‘25 – gennaio ‘26

Dicembre ‘25 – gennaio ‘26

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

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Deepfake, il Garante avverte: a rischio diritti e libertà fondamentali; [Link]
- Giornata europea della protezione dati, Garante: educare alla cultura della privacy a partire dai più giovani. [Link]

EDPB

- EDPB Document setting forth a Cooperation Procedure for the Authorisation of Contractual Clauses under Article 46(3)(a) GDPR and for the Adoption of Standard Contractual Clauses under Article 46(2)(d) GDPR; [Link]
- Recommendations 1/2026 on the Application for Approval and on the elements and principles to be found in Processor Binding Corporate Rules (Art. 47 GDPR); [Link]
- EU-US Data Privacy Framework FAQ for European individuals - version 2.0; [Link]
- Parere congiunto dell’EDPB e del Garante europeo della protezione dei dati (GEPD) relativa all’”omnibus digitale sull’IA”. [Link]

AGCOM

- Sanzione di oltre 14 milioni di euro a Cloudflare per violazione delle norme antipirateria; [Link]
- Approvato lo schema di regolamento sulla par condicio per la consultazione referendaria del 22 e 23 marzo 2026. [Link]

La responsabilità degli intermediari infrastrutturali nel contrasto alla pirateria digitale: il caso Cloudflare

L'Autorità per le Garanzie nelle Comunicazioni ("**AGCOM**" o "**Autorità**"), con Delibera n. 333/25/CONS ("**Delibera**") ha sanzionato uno dei colossi statunitensi di servizi *Internet*, **Cloudflare Inc**. ("**Cloudflare**"), con una sanzione di oltre 14 milioni di euro per non aver bloccato i siti segnalati attraverso il Piracy Shield, lo "scudo" nazionale antipirateria.

Cloudflare ha contestato la sanzione e ha annunciato di voler presentare ricorso, ritenendo che la normativa sul Piracy Shield *"sia fondamentalmente imperfetta, tecnicamente pericolosa e rischia di causare un'interruzione generalizzata dell'economia digitale in Italia*".

Ma cosa prevede il Piracy Shield? E qual è l'oggetto della Delibera?

Il Piracy Shield

Il Piracy Shield è una piattaforma tecnologica concepita per individuare e bloccare in tempi rapidissimi siti, indirizzi IP e domini che diffondono illecitamente eventi sportivi, film, serie TV, musica e altri contenuti protetti dal diritto d'autore. Lo strumento trova il proprio fondamento nella L. 93/2023 ("**Legge Antipirateria**"), adottata in risposta al dilagare delle IPTV illegali e dello *streaming* pirata, inizialmente con riferimento alle competizioni calcistiche di Serie A e successivamente estesa all'interno compartimento dell'intrattenimento digitale.

Il meccanismo è basato sulla cooperazione tra i titolari dei diritti (come DAZN, Sky, Mediaset) e gli altri *Internet Service Provider* ("**ISP**") operanti in Italia.

A fronte di una segnalazione, la piattaforma notifica in tempo reale agli operatori l'elenco degli indirizzi segnalati, imponendo, entro 30 minuti, l'inibizione dell'accesso ovvero l'adozione di misure tecniche equivalenti volte a impedire la fruizione dei contenuti da parte degli utenti finali. L'accesso ai domini inibiti comporta la visualizzazione di una schermata informativa sull'illiceità del servizio.

I destinatari degli ordini dell'Autorità non sono soltanto gli ISP in senso stretto, ma una platea molto più ampia di soggetti: prestatori di servizi di mere *conduit* (es., punti di interscambio internet), di hosting (es., *cloud*, piattaforme *online*), di *caching* (es., *reverse proxy*), fornitori di VPN, di DNS pubblicamente disponibili e gestori di motori di ricerca. In altri termini, chiunque incida, anche indirettamente, sull'accessibilità dei contenuti.

Per ridurre il rischio di blocchi indiscriminati, il Piracy Shield include una *whitelist* di oltre 11.000 domini. L'esperienza applicativa ha tuttavia già mostrato criticità, come dimostrato i casi di "*overblocking*", tra cui il blocco temporaneo di Google Drive di ottobre 2024. È in questo contesto che si innesta il caso Cloudflare.

Il provvedimento contro Cloudflare

La sanzione trae origine dalla mancata ottemperanza alla Delibera n. 49/25/CONS del 18 febbraio 2025, con cui l'AGCOM aveva ordinato a Cloudflare di disabilitare l'accesso a una serie di contenuti pirata segnalati tramite il Piracy Shield. Secondo l'Autorità, una percentuale significativa

dei siti coinvolti si avvaleva dei servizi di Cloudflare per la diffusione illecita di opere protette.

AGCOM ha ritenuto Cloudflare qualificabile come prestatore di servizi rilevanti ai sensi della Legge Antipirateria, in quanto fornitore di servizi di *mere conduit*, VPN e DNS pubblicamente disponibili[1].

La società statunitense, com'è noto, offre servizi infrastrutturali quali *content delivery network*, risoluzione DNS e sicurezza informatica, operando come intermediario tecnico tra utenti e siti *web*. Pur non fornendo contenuti, Cloudflare incide in modo significativo sulla loro distribuzione e accessibilità.

Richiamando precedenti giurisprudenziali sfavorevoli alla società[2], l'Autorità ha sostenuto che l'attività di *reverse proxy*[3] può integrare un concorso nella realizzazione degli illeciti commessi da terzi.

Ciò in quanto tali servizi consentirebbero di occultare l'identità dell'*hosting provider* effettivo, rendendo più complessa l'individuazione della fonte dell'illecito e permettendo, in concreto, di aggirare i blocchi disposti dall'Autorità.

La posizione di Cloudflare

Nel corso dell'istruttoria e successivamente all'adozione della Delibera, Cloudflare ha contestato radicalmente questa impostazione. La società ha ribadito che i propri servizi non danno origine alla trasmissione dei contenuti, non consentono di conoscerli, controllarli o modificarli e non incidono sulla loro disponibilità *online*, che resta legata ai *web server* di terzi.

La sospensione dei servizi Cloudflare, secondo questa prospettiva, non eliminerebbe né renderebbe inaccessibili i siti, che continuerebbero a essere fruibili indipendentemente dall'infrastruttura fornita.

Da ciò discenderebbe, a parere della società, l'impossibilità tecnica di dare esecuzione agli ordini dell'Autorità. Su queste basi Cloudflare ha annunciato il ricorso contro la Delibera, contestando anche l'impianto normativo della Legge Antipirateria, ritenuta idonea a generare effetti sistemici negativi sull'economia digitale.

Considerazioni conclusive

Il cuore della controversia non riguarda tanto la responsabilità di Cloudflare per la messa a disposizione di contenuti illeciti, quanto il mancato rispetto di ordini amministrativi volti a disabilitare l'accesso a tali contenuti. È su questo piano che l'AGCOM colloca la violazione e giustifica la sanzione.

Tuttavia, nelle proprie difese Cloudflare sembra richiamare, seppur indirettamente, la tradizionale distinzione tra *hosting provider* "attivo" e "passivo"[4], da cui discende, in determinate condizioni, l'esenzione di responsabilità.

[1] Il Digital Services Act (Regolamento UE 2065/2022) tra gli esempi di servizi di mere conduit – ossia di servizi consistenti nella trasmissione, su una rete di comunicazione, di informazioni fornite da un destinatario del servizio, o nella fornitura dell'accesso a una rete di comunicazione – prevede espressamente anche i risolutori e servizi di DNS.

[2] Tribunale di Milano; Tribunale di Roma, R.G. 14261/2024.

[3] Si tratta di un server che si posiziona di fronte a uno o più server applicativi e riceve le richieste dei client (ad es. browser, app, programma desktop) al loro posto. Il reverse proxy inoltra le richieste ai server interni appropriati e restituisce le risposte ai client, agendo come intermediario e mascherando l'infrastruttura backend.

[4] Si parla di hosting provider "attivo" quando l'attività prestata non è una mera fornitura del servizio di memorizzazione in modo tecnico e automatico, ma ha ad oggetto anche i contenuti della prestazione resa e di hosting provider "passivo" quando svolge un'attività di prestazione di servizi di ordine meramente tecnico e automatico, non potendo conoscere né controllare le informazioni trasmesse o memorizzate dalle persone alle quali forniscono i servizi. In tal senso, la giurisprudenza nazionale e europea, aveva enucleato alcuni indici di interferenza (meramente esemplificativi e non necessariamente tutti compresenti), ovvero elementi idonei a individuare la figura dell'hosting provider attivo comprendente attività quali di filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti pubblicati dagli utenti, operante mediante una gestione imprenditoriale del servizio, nonché l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione. Tali indici sono stati accolti anche dalla giurisprudenza nazionale, la quale ha affermato che in tutti i casi in cui non sussista un'attività di ordine meramente tecnico, automatico e passivo, le

Oggi il riferimento normativo da prendere in considerazione è rappresentato dall'Articolo 6 del Digital Services Act (Regolamento UE 2065/2022)[5], che subordina tale esenzione non solo all'assenza di conoscenza effettiva dell'illecito, ma anche all'adozione tempestiva di misure una volta ricevuta una segnalazione qualificata (c.d. meccanismo di *notice and action*).

Come sottolineato dall'Autorità[6], il procedimento sanzionatorio non mira ad accertare una responsabilità contenutistica in capo a Cloudflare, bensì l'inottemperanza a ordini specifici e reiterati. Da questa prospettiva, anche l'eventuale qualificazione della società come *hosting provider* "passivo" potrebbe risultare irrilevante: l'AGCOM aveva già portato a conoscenza di Cloudflare la presenza di contenuti illeciti, senza che fossero adottate misure ritenute adeguate.

Alla luce di quanto precede, la decisione dell'AGCOM suggerisce la necessità di rafforzare i presidi interni di *compliance* regolatoria, in particolare nei settori ad alta esposizione come quello della tutela del diritto d'autore, di valutare attentamente, *ex ante*, il rischio di qualificazione come intermediari rilevanti alla luce dei servizi effettivamente offerti, nonché di predisporre procedure tecniche e legali per la gestione degli ordini di blocco delle autorità, anche quando se ne intenda contestare la legittimità.

Il caso Cloudflare mostra, infatti, come la scelta di non conformarsi integralmente agli ordini, confidando in una successiva tutela giurisdizionale, possa comportare conseguenze sanzionatorie immediate e di notevole entità.

limitazioni di responsabilità non sono applicabili (CGUE 236/2010, Google France e Google, cause da C-236/08 a C-238/08; CGUE, 12 luglio 2011, L'Oréal e a., C-324/09; CGUE, 7 agosto 2018, Cooperative Vereniging SNBREACT U.A. c. Deepak Mehta, C-521/17; CGUE, 22 giugno 2021, YouTube, C-682/18 e C-683/18. Per la giurisprudenza nazionale si veda, Cass. Civ., Sez. I, 7708/2009, Cass. Civ., Sez. I, 39763/2021; CdS, Sez. VI, 10510/2023).

[5] Prima dell'entrata in vigore del DSA, la disciplina di riferimento era rappresentata invece dagli articoli 16 e 17 del D.Lgs. 70/2003 e ss.mm.ii. (c.d. Decreto e-commerce), ora abrogati.

NIS2: dalla compliance formale alla responsabilità operativa. Cosa cambia dopo le ultime Determinazioni e Linee Guida dell'ACN

L'Agenzia per la Cybersicurezza Nazionale ("**ACN**") ha recentemente adottato tre documenti destinati a consolidare il quadro normativo NIS2 in Italia: le Determinazioni nn. 379887 e 379907/2025 (rispettivamente, la "**Determinazione 379887**" e la "**Determinazione 379907**") e le Linee Guida NIS – *Specifiche di base – Definizione del processo di gestione degli incidenti di sicurezza informatica* (le "**Linee Guida**").

Questi documenti potrebbero apparire come l'ennesimo tassello regolatorio di un quadro già denso e complesso. In realtà, segnano un passaggio fondamentale: la NIS2 entra definitivamente in una fase in cui diventa essenziale dimostrare di saper governare la sicurezza informatica in modo continuo, consapevole e verificabile.

Ma cosa prevedono le Determinazioni 379887 e 379907 e le Linee Guida? E quali implicazioni comportano per le imprese rientranti nell'ambito di applicazione del Decreto NIS2 (D.Lgs. 138/2024)?

[6] Nella propria Delibera, l'AGCOM chiarisce infatti che l'obiettivo del procedimento sanzionatorio non riguarda, la sussistenza di responsabilità in capo a Cloudflare per l'aver messo a disposizione contenuti in violazione del diritto d'autore, ma nel non aver ottemperato alle richieste delle Autorità di disabilitare l'acceso a contenuti illegali e per non aver adottato le misure tecnologiche e organizzative necessarie per rendere non fruibili da parte degli utilizzatori finali i contenuti diffusi illegalmente.

Le Determinazioni 379887 e 379907

Le Determinazioni 379887 e 379907 intervengono su aspetti apparentemente procedurali, ma con effetti sostanziali sulla *governance* NIS2. Le principali novità possono essere sintetizzate in quattro direttrici:

1. la **cristallizzazione delle dichiarazioni**. Decorsi 10 giorni solari dal completamento della registrazione sul portale dei servizi dell'ACN, la dichiarazione diventa definitiva e non potrà più essere modificata;
2. il **rafforzamento del ruolo del Referente CSIRT** [7], il quale entra a pieno titolo nella *governance* NIS2. L'ACN lo include espressamente nell'organizzazione per la sicurezza informatica (*cfr*. misura di sicurezza GV.RR-02, Allegato 1 per i soggetti importanti e Allegato 2 per i soggetti essenziali, alla Determinazione 379907) e chiarisce che i suoi dati identificativi devono essere ricompresi tra le informazioni da verificare durante l'aggiornamento annuale delle informazioni, previsto tra il 15 aprile e il 31 maggio di ogni anno (*cfr*. art. 15 della Determinazione 379887);
3. le **dichiarazioni precompilate**: i soggetti già qualificati come "essenziali" o "importanti" riceveranno, nella prossima finestra di registrazione (1° gennaio – 28 febbraio), bozze di dichiarazioni precompilate sulla base dei dati forniti nel 2025;
4. la **conferma – con alcuni affinamenti – delle tempistiche e degli obblighi chiave**. Restano i 18 mesi (ottobre 2026) per l'adeguamento delle misure di sicurezza e i 9 mesi (gennaio 2026) per l'avvio degli obblighi di notifica degli incidenti significativi. Tuttavia, la Determinazione 379907 aggiorna il contenuto dei c.d. obblighi di base[8] – ossia quelle misure di sicurezza e quegli incidenti significativi che i soggetti NIS dovranno rispettivamente adottare e/o notificare in fase di prima applicazione del Decreto NIS2 – e abroga le previsioni transitorie inerenti all'obbligo di notifica per gli operatori di servizi essenziali e per gli operatori TELCO[9].

Le Linee Guida sul processo di gestione degli incidenti di sicurezza informatica

Già con le Linee Guida NIS – *Specifiche di base*, pubblicate a settembre 2025, l'ACN aveva fornito indicazioni applicative puntuali su come le imprese devono organizzare *governance*, processi e controlli per allinearsi al Decreto NIS2[10].

Con le nuove Linee Guida, invece, l'ACN si pone l'obiettivo di fornire delle indicazioni per definire il processo di gestione degli incidenti di sicurezza informatica, chiarendo la relazione tra le diverse fasi del processo con le misure di sicurezza richieste dalla normativa.

Il processo di gestione degli incidenti non è descritto come una sequenza astratta di *best practice*, ma come un insieme strutturato di attività che devono consentire di rilevare

[7] I Referente CSIRT è quel soggetto (interno o esterno all'organizzazione) che doveva essere designato entro il 31 dicembre 2025 e che funge da punto di collegamento operativo con il CSIRT Italia. Per maggiori approfondimenti sulla figura del Referente CSIRT, si rinvia al nostro precedente contributo "*NIS2 e gestione degli incidenti: l'ACN introduce il Referente CSIRT*".

[8] Ad esempio, viene aggiunta la previsione di rendere note le politiche alle articolazioni competenti del soggetto NIS, tenuto conto anche del principio del *need to know*.

[9] La Determinazione 379907 sarà infatti applicabile dal 15 gennaio 2026, sostituendo così la precedente Determinazione 164179 del 14 aprile 2025, la quale stabiliva anche la disciplina transitoria per gli operatori dei servizi essenziali (c.d. OSE, ossia i soggetti NIS identificati prima della data di entrata in vigore del Decreto NIS2 come operatori di servizi essenziali ai sensi del D.Lgs. 65/2018) e gli operatori TELCO (ossia i soggetti NIS che forniscono reti pubbliche di comunicazione elettronica o servizi di comunicazione elettronica accessibili al pubblico ai sensi del D.Lgs. 259/2003, ad un numero di utenti pari o superiore, anche alternativamente: (i) all'1% della base di utenti nazionale, calcolato sulla base dei dati pubblicati dall'Osservatorio trimestrale delle comunicazioni dell'AGCOM; (ii) a un milione). Per questa tipologia di soggetti, il termine per la notifica degli incidenti significativi decorreva, limitatamente ai sistemi informativi e di rete OSE e ai sistemi informativi e di rete TELCO, dal 30 aprile 2025.

[10] 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/.

tempestivamente un incidente, rispondervi in modo efficace, ripristinare i sistemi e, soprattutto, migliorare la capacità di risposta futura.

Non a caso, dal gennaio 2026, il verificarsi di un "incidente significativo" attiva l'obbligo di notifica al CSIRT Italia. In particolare, l'ACN (negli Allegati 3 e 4 alla Determinazione 379907) ha definito quattro fattispecie di incidenti – tre comuni a tutti i soggetti e una ulteriore riservata ai soli soggetti "essenziali" [11] – che, se ricorrenti, qualificano l'incidente come "significativo".

Le cinque fasi della gestione degli incidenti

Le Linee Guida propongono un modello articolato in **cinque fasi** (e specifiche sottofasi), che deve trovare formalizzazione nel piano di gestione degli incidenti (misura di sicurezza RS.MA-01) ed essere approvato dagli organi amministrativi e direttivi. È un passaggio che rafforza il legame tra sicurezza informatica e responsabilità di vertice.

La fase di "**preparazione**" riguarda tutte le attività propedeutiche: politiche di sicurezza, ruoli e responsabilità definite con la matrice RACI [12], inventari, misure tecniche e organizzative. Il messaggio è chiaro: non basta saper gestire un incidente quando accade, occorre poter dimostrare di aver predisposto in anticipo un modello organizzativo coerente e aggiornato.

Segue la fase di "**rilevamento**", dedicata all'individuazione e all'analisi degli "eventi rilevanti per la cybersicurezza". Non ogni evento è un incidente di sicurezza: si tratta unicamente di quegli eventi (di natura accidentale o intenzionale) che compromettono o potrebbero compromettere la sicurezza dei sistemi informatici e di rete e che richiedono, quindi, un'analisi al fine di verificare che si tratta di un incidente, come ad esempio un picco di traffico proveniente da molteplici indirizzi IP.

Se è possibile qualificare un evento come "incidente di sicurezza", si passa alla fase di "**risposta**", ossia la fase centrale del processo di gestione degli incidenti.

Qui emerge uno dei chiarimenti più importanti delle Linee Guida: il momento dell'"evidenza dell'incidente" segna l'avvio delle tempistiche di notifica verso il CSIRT Italia[13]. Non è necessario conoscere subito la *root cause* (causa originale); è sufficiente riconoscere che l'incidente esiste e che rientra tra quelli significativi.

La fase di "**ripristino**" mira a riportare i sistemi allo stato antecedente all'incidente, assicurandosi che tutto funzioni regolarmente. Infine, il "**miglioramento**" accompagna l'intero ciclo di vita del processo.

[11] In particolare, l'Allegato 3 alla Determinazione 379907 individua i seguenti incidenti significativi per i soggetti "importanti": (i) perdita di riservatezza, verso l'esterno, di dati digitali di proprietà o sui quali esercita il controllo anche parziale; (ii) perdita di integrità, con impatto verso l'esterno, di dati digitali di proprietà o sui quali esercita il controllo anche parziale; (iii) violazione degli SLA. A queste tipologie, per i soggetti "essenziali", l'Allegato 4 alla Determinazione 379907 aggiunge anche il caso in cui il soggetto abbia evidenza dell'accesso, non autorizzato o con abuso dei privilegi concessi, a dati digitali di sua proprietà o sui quali esercita un controllo, anche parziale.

[12] La c.d. matrice RACI (*Responsible*, *Accountable*, *Consulted*, *Informed*) rappresenta uno degli strumenti utilizzati per assegnare ruoli e responsabilità, definendoli chiaramente per le varie fasi di attività di un processo. Un ruolo di fondamentale importanza dovrà essere ricoperto dal Referente CSIRT in riferimento alle attività di interlocuzione con lo CSIRT Italia e di notifica degli incidenti per conto del soggetto. Tuttavia, potrebbe rendersi necessario adottare decisioni che non rientrano nelle competenze del Referente CSIRT. A tal fine, le Linee Guida precisano che devono essere definiti ruoli, responsabilità, fasi e procedure per l'assunzione delle decisioni, che nei casi più rilevanti spettano agli organi amministrativi e direttivi.

[13] Acquisita l'evidenza dell'incidente, i soggetti NIS devono trasmettere al CSIRT Italia:

a. senza ingiustificato ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica dell'incidente che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;
b. senza ingiustificato ritardo e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le precedenti informazioni e indichi una valutazione iniziale dell'incidente significativo (gravità, impatto e, ove disponibili, indicatori di compromissione);
c. su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;
d. entro 1 mese dalla trasmissione della notifica, una relazione finale sull'incidente;
e. in caso di incidente in corso al momento della trasmissione della relazione finale, una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

Quest'ultima fase è finalizzata a potenziare la capacità di gestione degli incidenti: analisi post-incidente, *lesson learned*, aggiornamento delle procedure e del piano di gestione degli incidenti, non sono attività opzionali, ma elementi essenziali per dimostrare che l'organizzazione apprende dagli eventi e rafforza nel tempo la propria capacità di risposta.

Conclusioni

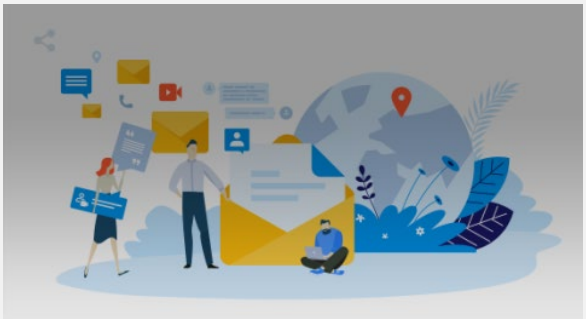
Le Determinazioni 379887 e 379907 e le nuove Linee Guida dell'ACN segnano il passaggio alla seconda fase attuativa del Decreto NIS2. Da gennaio 2026, i soggetti NIS dovranno notificare al CSIRT Italia, in caso di incidente significativo, le perdite di riservatezza e di integrità di dati digitali, la violazione degli SLA nonché, per i soggetti essenziali, anche gli accessi, non autorizzati o con abuso dei privilegi concessi, ai dati digitali.

In questo contesto, la gestione degli incidenti non è più una misura di sicurezza "da pianificare" entro ottobre 2026 [14], ma una capacità da costruire subito.

Perché quando l'incidente si verifica, non sarà il documento a fare la differenza, ma la prontezza decisionale, la chiarezza dei ruoli e delle responsabilità e la capacità di dimostrare che la sicurezza informatica è parte integrante della *governance* dell'organizzazione.

* * *

Uso distorto dell'AI: il sottile equilibrio tra efficienza e abuso comunicativo



Oltre la metà dei messaggi indesiderati viene oggi **generata da sistemi di intelligenza artificiale** ("**IA**"), con incrementi significativi di anno in anno [15]. Infatti, se nel 2024 la quota di *spam* prodotto da strumenti di IA si attestava intorno al 40%, nel 2023 non superava nemmeno il 10%.

Si tratta di **un incremento di natura esponenziale**, che testimonia la rapidità con cui le tecnologie generative stanno influenzando anche gli ambiti meno virtuosi del digitale.

Dietro questi messaggi si nascondono non solo **comunicazioni pubblicitarie invasive**, ma anche tentativi di **attacco informatico** particolarmente insidiosi.

Ma cos'è lo "spam" e perché l'IA ne accelera la proliferazione?

Il termine *spam* ha origine dal marchio di una carne in scatola prodotta negli USA e nota per la sua qualità scadente. Oggi, tale termine viene utilizzato per indicare la posta indesiderata o "spazzatura", generata tramite diversi canali di comunicazione, anche se il mezzo più comune rimane la posta elettronica.

[14] Il processo di gestione degli incidenti di sicurezza viene infatti annoverato tra le misure di sicurezza che i soggetti "importanti" e "essenziali" dovranno adottare entro 18 mesi (ottobre 2026) dalla ricezione della comunicazione di inserimento nell'elenco nazionale NIS. L'Appendice B delle Linee Guida contiene un elenco delle misure di sicurezza di base relative alle varie fasi del processo di gestione degli incidenti

[15] Questo dato emerge da uno studio congiunto condotto dalla Columbia University, dalla University of Chicago e dalla società di cybersecurity Barracuda, che ha esaminato milioni di e-mail inviate tra il 2022 e il 2025. Lo studio riporta che il 14% di questi attacchi nel 2025 è stato potenziato proprio dall'uso dell'IA.

Una delle principali potenzialità dell'IA è senza dubbio quella di produrre testi grammaticalmente impeccabili e comunicativamente efficaci, del tutto assimilabili a quelli redatti da un essere umano.

Tale prerogativa non è passata inosservata anche ai criminali informatici, i quali hanno scelto di integrare i modelli linguistici avanzati (gli stessi alla base di *chatbot* e degli assistenti virtuali) per affinare le proprie strategie di inganno digitale.

Emerge in tal modo una **nuova generazione di comunicazioni fraudolente**: uno *spam* evoluto e sempre più difficile da distinguere da un messaggio autentico.

Parallelamente, un ulteriore fattore che contribuisce all'espansione vertiginosa di questo fenomeno è sicuramente la **velocità** con cui l'IA può generare questa tipologia di e-mail *spam*. In particolare, ci si serve degli stessi strumenti che vengono utilizzati, ad esempio, nel *marketing* per migliorare i testi delle *newsletter*.

Il confine tra strumenti volti all'efficienza e strumenti potenzialmente suscettibili di abuso si è fatto, dunque, estremamente labile. Un esempio emblematico è rappresentato dalle c.d. **BEC (*Business E–mail Compromise*)**, ossia compromissioni delle caselle di posta elettronica aziendali che gli *hacker* sfruttano per fingersi clienti, colleghi o fornitori al fine di appropriarsi di informazioni sensibili.

Lo *spam* e le possibili violazioni del GDPR

Gli indirizzi e-mail sono comunemente annoverati tra i dati personali e, dunque, il loro trattamento deve avvenire nel pieno rispetto dei principi cardine del GDPR (Regolamento UE 679/2016), ossia liceità, correttezza, trasparenza, limitazione delle finalità, proporzionalità e minimizzazione.

La disciplina generale in materia di invio di comunicazioni a contenuto commerciale si fonda sul principio del previo e comprovato **consenso** dell'interessato.

Tale requisito è espressamente previsto dal legislatore italiano all'**art. 130 del Codice Privacy** (D.Lgs. 196/2003, come modificato dal D.lgs. 101/2018), in base al quale l'utilizzo di sistemi automatizzati per l'invio di materiale pubblicitario, comunicazioni commerciali, offerte di vendita diretta o per la realizzazione di indagini di mercato è ammesso esclusivamente in presenza del consenso preventivo dell'utente, il c.d. *opt-in*.

In applicazione di tale disposizione normativa, l'assenza di un consenso esplicito e validamente prestato al trattamento dei dati personali per finalità di *marketing* comporta l'illiceità **dell'invio di e-mail a contenuto promozionale o commerciale**.

Tuttavia, al fine di coniugare le esigenze degli operatori di mercato con i diritti dell'interessato, è prevista una sorta di "deroga" al principio generale costituita dal *soft spam*. Il riferimento va alle ipotesi disciplinate dall'art. 130, comma 4, del Codice della Privacy, ossia ai casi in cui il titolare del trattamento utilizza l'e-mail fornita dal cliente in occasione dell'acquisto di un bene o di un servizio per inviargli comunicazioni promozionali riguardanti prodotti o servizi analoghi a quelli che ha già acquistato in precedenza.

In altri termini, non è necessario ottenere il consenso dell'interessato se il titolare utilizza, ai fini della vendita diretta di propri prodotti o servizi l'e-mail fornite dal medesimo nel contesto della vendita o della prestazione del servizio, sempre che si tratti di servizi analoghi a quelli oggetto della vendita o del servizio e che l'interessato, adeguatamente informato, non rifiuti tale uso (c.d. *opt-out*), inizialmente o in occasione di successive comunicazioni.

Quali tutele possono attuare gli utenti e le aziende per difendersi dallo *spam*?

Il fenomeno dello *spam* ha registrato una significativa crescita con la diffusione dei sistemi di messaggistica istantanea e, più in generale, con l'affermazione dei *social media*, i quali hanno favorito una circolazione sempre più ampia e spesso incontrollata dei dati di contatto resi pubblicamente accessibili.

È ormai evidente che, come accade per la maggior parte delle minacce di natura informatica, la forma più efficace di tutela risiede nella consapevolezza degli utenti circa l'utilizzo e la protezione delle proprie informazioni personali. Invero, al fine di contrastare questo fenomeno, è fondamentale per le aziende organizzare **corsi di formazione per il proprio personale**, così da aumentare la consapevolezza sui rischi legati allo *spam*. Inoltre, potrebbe essere utile adottare delle **procedure interne** per disciplinare l'utilizzo degli strumenti informatici aziendali, tra cui le caselle di posta elettronica, fornendo delle vere e proprie linee guida di comportamento.

D'altro canto, occorrerà adottare specifiche **misure tecniche**, come adeguati strumenti di filtraggio e di rilevamento delle minacce, configurati e gestiti in modo appropriato, anche basati sull'impiego di sistemi di IA in grado di individuare schemi ricorrenti e anomalie all'interno delle e-mail più velocemente ed efficacemente, superando così le limitazioni proprie dei tradizionali filtri antispam.

Solo attraverso tale combinazione sarà possibile predisporre una difesa efficace contro un panorama di minacce in costante evoluzione e di crescente sofisticazione.

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