OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Settembre 2025

Settembre 2025

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

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- IT-Wallet, sì del Garante privacy alla sperimentazione; [Link]
- Indagini patrimoniali, il Garante privacy dice sì a CEREBRO; [Link]
- Garante privacy: dossier sanitario accessibile solo per ragioni di cura; [Link]
- Diritto di accesso, il Garante privacy sanziona una banca per 100mila euro; [Link]
- Garanti privacy mondiali: la protezione dei dati si applica pienamente all'IA. [Link]

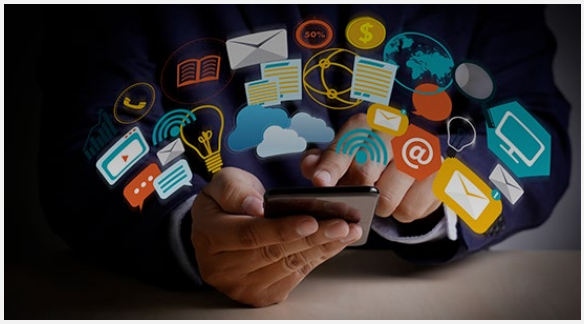
EDPB

- Guidelines 3/2025 on the interplay between the DSA and the GDPR. [Link]

AGCOM

- Spoofing, primi risultati del regolamento Agcom. Dal 19 agosto bloccate 43 milioni di chiamate; [Link]
- Determina 14/25/DTC. Approvazione del documento "linee guida per la definizione della campagne di misure sul campo (drive test) della qualità del servizio dati in mobilità – campagna 2025". [Link]

Chat control: obblighi, rischi e prospettive per i fornitori di servizi digitali



La recente Proposta di Regolamento UE per la prevenzione e la lotta contro l'abuso sessuale sui minori (il c.d. *chat control* – la "**Proposta**") potrebbe incidere in modo significativo sull'operatività dei fornitori di servizi digitali che offrono i loro servizi in Europa.

L'obiettivo dichiarato è quello di rafforzare gli strumenti di contrasto agli abusi *online*, trasformando in obblighi giuridici stringenti attività che oggi dipendono in larga parte dalla discrezionalità dei *provider*.

Ma cosa prevede in concreto la Proposta?

La Proposta introduce obblighi di valutazione e mitigazione dei rischi per *hosting provider* e servizi di comunicazione interpersonale. In presenza di un rischio significativo, un'autorità potrà emettere *detection orders* mirati che impongono l'uso di tecnologie di rilevazione (anche per servizi cifrati), con limiti temporali e garanzie di proporzionalità.

In caso di ordini o quando emergano evidenze, i *provider* saranno tenuti a segnalare al nuovo *EU Centre* [1] ; potranno inoltre essere disposte rimozioni o blocchi secondo le procedure previste.

I *provider* dovranno svolgere una valutazione del rischio di uso improprio dei loro servizi, nonché prevedere misure adeguate e proporzionate per attenuare i rischi individuati. Sono inoltre previsti specifici obblighi e responsabilità per gli *app store,* chiamati a valutare il rischio che un'app sia usata per il *grooming* e, ove il rischio sia significativo, ad adottare misure ragionevoli – inclusa l'identificazione affidabile degli utenti minori – per impedirne l'accesso.

Questa tipologia di attività comporta chiaramente il trattamento di dati personali. La Proposta, infatti, si basa sul GDPR ed esplicita la base giuridica su cui fondare tali trattamenti: l'art. 6, par. 1, lett. c), GDPR (obbligo di legge) per i trattamenti necessari all'esecuzione degli ordini e degli obblighi previsti dal Regolamento, con esclusione del consenso come presupposto, e il rinvio all'art. 15, par. 1, della Direttiva ePrivacy[2].

La Proposta si coordina inoltre con il Digital Services Act, richiamandone strumenti e concetti (es. approccio *risk-based*, *trusted flaggers*) ma introducendo un regime settoriale specifico dedicato alla prevenzione e al contrasto dell'abuso sessuale online[3].

Conseguenze per le imprese coinvolte

Sono interessati in particolare: *hosting provider*, servizi di comunicazione interpersonale, *app*

[1] La Proposta prevede che, al fine di agevolare e sostenere l'attuazione dell'emanando regolamento, verrà istituito un Centro dell'UE di prevenzione e lotto contro l'abuso sessuale sui minori.

[2] L'art. 15, par.1, prevede espressamente che gli Stati membri possano adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui all'art. 5, qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata: (i) per la salvaguardia della sicurezza dello Stato, della difesa, della sicurezza pubblica; (ii) per la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica.

[3] In particolare, il DSA consente di svolgere indagini volontarie di propria iniziativa al fine di rilevare contenuti illegali (art. 7) e prevede che i prestatori di servizi di memorizzazione di informazioni, incluse le piattaforme online debbano istituire meccanismi per consentire a qualsiasi persona o ente di notificare la presenza nella piattaforma di eventuali contenuti illegali (c.d. principio notice and take down – art. 16).

store e, per alcuni profili, i fornitori di accesso a Internet.

Tali fornitori – ove la normativa verrà adottata – saranno chiamati a integrare algoritmi di analisi semantica e sistemi di *hashing* per immagini e video, aggiornare o implementare processi di *risk assessment* e di rendicontazione verso le Autorità nazionali che verranno designate.

Occorrerà, inoltre, aggiornare anche tutta la necessaria documentazione privacy, indicando come base giuridica l'obbligo di legge.

Gli Stati membri dell'UE saranno chiamati a esprimere una posizione su questa Proposta il prossimo 14 ottobre (salvo modifiche di calendario).

Nel frattempo, vista anche la sensibilità del tema, sarebbe opportuno per i *provider* iniziare a mappare i propri servizi, identificando le aree più soggette a rischi di abuso messaggistica, *storage* di *file* multimediali, interazioni dirette tra utenti), al fine di valutare l'adeguatezza tecnica di eventuali misure già adottate e preparare un piano per garantire la *compliance* normativa.

Conseguenze per gli utenti: i rischi da considerare

La Proposta prevede che il rilevamento dovrebbe avere ad oggetto i contenuti pedopornografici già noti, i contenuti nuovi e i tentativi di adescamento nei confronti dei minori [4]. Il rilevamento, specie con riguardo ai contenuti nuovi, potrà avvenire tramite modelli di *machine learning* basati sull'intelligenza artificiale, ma dovrà avvenire con tecnologie affidabili e con il minor impatto possibile, secondo il principio di minimizzazione.

Qui emergono due criticità. La prima è tecnica: ogni sistema di rilevazione automatica comporta margini di errore.

I falsi positivi potrebbero portare alla segnalazione di contenuti del tutto leciti, con conseguenze dirette sulla libertà di comunicazione degli utenti.

I falsi negativi, al contrario, rischiano di lasciare inosservati contenuti realmente pericolosi, finendo così per ridurre l'efficacia stessa della misura e incidere negativamente sulla tutela dei minori.

La seconda criticità riguarda, invece, la protezione dei dati personali. L'uso estensivo di strumenti di IA applicati alle comunicazioni private comporta trattamenti particolarmente invasivi e delicati.

Occorrerà, dunque, valutare se svolgere una DPIA (*Data Protection Impact Assessment*), così da garantire un equilibrio tra esigenze di sicurezza e rispetto dei diritti fondamentali degli utenti.

Sebbene il c.d. *chat control* persegua l'obiettivo di garantire un ambiente *online* sicuro, prevedibile e affidabile, il legislatore europeo dovrà trovare un equilibrio delicato: proteggere i minori senza sacrificare i diritti fondamentali degli utenti ed evitare che la soluzione stessa diventi fonte di nuovi rischi e vulnerabilità.

* * *

[4] Tra i suoi compiti, il Centro dell'UE dovrà creare e gestire, per ciascuno dei tre tipi di abuso sessuale, dei database di indicatori di abuso sessuale su minori online, che i provider dovranno applicare per ottemperare agli obblighi di rilevazione.

Data breach negli hotel: obblighi, rischi e tutele

Nell'estate 2025 diversi hotel italiani sono stati colpiti da gravi violazioni di dati personali: migliaia di scansioni digitali di passaporti, carte d'identità e altri documenti di riconoscimento sarebbero finite nelle mani dei cybercriminali.

Secondo quanto comunicato dal Garante per la protezione dei dati personali, alcune strutture hanno notificato tempestivamente l'incidente, mentre altre sono state sollecitate a farlo senza indugio.

Parallelamente, ad agosto 2025, CERT-AGID, struttura specializzata di AGID, avente il compito, tra le altre cose, di monitorare le minacce informatiche a livello nazionale, ha peraltro rilevato la vendita illegale, nel dark web, di decine di migliaia di documenti trafugati da hotel operanti in Italia, tra giugno e luglio 2025.

L'episodio riporta in primo piano un interrogativo centrale: è davvero necessario che gli hotel e le altre strutture ricettive raccolgano e conservino le copie dei documenti dei propri ospiti?

Cosa prevede la legge per l'identificazione degli ospiti:

Secondo la normativa italiana, gli hotel devono identificare gli ospiti e trasmettere le loro generalità alla Questura entro 24 ore dal loro arrivo (*cfr.* art. 109 del Testo unico delle leggi di pubblica sicurezza, c.d. TULPS).

Tale adempimento avviene attraverso il portale Alloggiati Web (fruibile all'indirizzo www.alloggiatiweb.poliziadistato.it), accessibile solo con credenziali e sistemi di autenticazione a due fattori (decreto ministeriale del 7 gennaio 2013 contenente disposizioni concernenti la comunicazione alle Autorità di pubblica sicurezza dell'arrivo di persone alloggiate in strutture ricettive, oggetto anche del parere del Garante dell'8 luglio 2021).

In caso di indisponibilità del portale, la trasmissione può avvenire tramite fax o PEC, ma si tratta di modalità residuali.

La normativa, tuttavia, non richiede agli hotel di trattenere o archiviare le copie dei documenti d'identità. Una volta inviati i dati richiesti, le eventuali copie digitali o cartacee dovrebbero essere eliminate, conservando solo la ricevuta dell'avvenuta trasmissione.

La prassi, ancora diffusa in molte strutture, di trattenere o archiviare copie dei documenti non risulterebbe quindi avere una base giuridica effettivamente rinveniente in un obbligo di legge.

Già nel 2005 il Garante Privacy aveva chiarito che la conservazione di copie dei documenti di riconoscimento risulta legittima solo se prevista da una norma specifica e per un tempo limitato (Provvedimento del 27 ottobre 2005).

Quando si alloggia in un hotel, tuttavia, capita frequentemente che la struttura, al check-in, richieda ed effettui una copia di un documento di identità dell'ospite. In questo caso, la struttura potrebbe operare in qualità titolare del trattamento.

Cosa fare in caso di *data breach* e cosa deve fare un hotel?

Un *data breach* è un incidente di sicurezza che comporta, in via accidentale o illecita, la perdita,

la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Gli esempi più comuni includono infezioni da *malware* o *ransomware*, attacchi hacker, accessi non autorizzati ad archivi digitali o cartacei, furto o smarrimento di dispositivi (come PC portatili, smartphone, tablet o chiavette USB), perdita di documenti cartacei contenenti dati personali, oppure e-mail inviate erroneamente a destinatari non autorizzati.

In circostanze analoghe, l'hotel dovrebbe identificare l'incidente ed effettuare le opportune valutazioni. In caso di *data breach*, l'hotel potrebbe essere obbligato – in qualità di titolare del trattamento – a:

- notificare la violazione dei dati personali al Garante Privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuta a conoscenza, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche;
- comunicare la predetta violazione ai soggetti interessati cui si riferiscono i dati personali violati senza ingiustificato ritardo, ove la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Quali sono i rischi concreti per i clienti?

I documenti d'identità costituiscono un patrimonio prezioso per la criminalità informatica. Il loro utilizzo illecito può includere, solo per citare alcuni esempi:

- la creazione di **documenti falsi basati** su identità reali;
- l'**apertura fraudolenta di conti correnti o linee di credito**;
- attività di ***social engineering*** volte a carpire altre informazioni personali o professionali;
- il **furto d'identità digitale**, con conseguenze legali ed economiche gravi per le vittime.

La crescente frequenza di tali attività criminali rende pertanto essenziale che le strutture ricettive valutino con attenzione se sia realmente necessario raccogliere e conservare le copie dei documenti di identità.

Poiché non esiste un obbligo normativo in tal senso, ogni eventuale trattamento ulteriore dovrà fondarsi su una base giuridica adeguata (ad esempio il legittimo interesse), supportata da un'attenta valutazione di proporzionalità e necessità, da inserire nella documentazione di *accountability*.

In ogni caso, le strutture devono adottare misure di sicurezza tecniche e organizzative adeguate e formare il personale sugli obblighi legati alla protezione dei dati personali.

Del pari, anche i cittadini svolgono un ruolo decisivo nella difesa della propria identità. Conoscere i propri diritti e adottare comportamenti prudenti è il primo passo per proteggere la propria identità.

È fondamentale, inoltre, che i singoli soggetti monitorino periodicamente eventuali utilizzi indebiti dei propri dati, evitando di condividere copie dei documenti personali attraverso canali non sicuri o non necessari e, in caso di sospetto abuso o furto d'identità, rivolgersi immediatamente alle Autorità competenti.

* * *

Garante Privacy: double opt-in e consenso per finalità di marketing

Il Garante Privacy, con il Provvedimento n. 330/2025 (doc. web 10143278 – il "**Provvedimento**") ha recentemente inflitto una sanzione di 45mila euro a un rivenditore di auto *online* per trattamento illecito di dati personali a fini di *marketing*. In questi casi, per raccogliere consensi validi non è sufficiente spuntare una casella: il consenso deve essere documentato in modo certo, così da poter dimostrare chi lo ha prestato e quando.

Il Provvedimento riveste particolare importanza in quanto chiarisce i requisiti per la raccolta di un valido consenso al trattamento di dati personali per finalità di *marketing*, concentrandosi sul meccanismo del c.d. ***double opt-in***.

Sebbene questo meccanismo non sia espressamente previsto né dal Regolamento (UE) 679/2016 ("**GDPR**") né dal D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 (il "**Codice Privacy**"), il Garante Privacy lo annovera tra le misure minime di protezione, sia per l'interessato che per il titolare del trattamento.

Ma cosa si intende per "*opt-in*" e "*double opt-in*"?

L'*opt-in* consiste in un'azione positiva dell'utente con cui lo stesso fornisce esplicitamente il proprio consenso. In ambito digitale, ciò avviene spesso tramite un modulo o casella di spunta non preselezionata oppure cliccando su un apposito pulsante di conferma del consenso.

Il *double opt-in*, invece, aggiunge un secondo passaggio, configurandosi come una forma rafforzata del modello precedente.

Una volta compilato il modulo o spuntata l'apposita casella, all'utente viene inviata un'e-mail di conferma all'indirizzo registrato, dove gli viene richiesto di compiere un'ulteriore azione (ad es., *click* su un *link* di conferma) per confermare la propria iscrizione alla *mailing list* e il relativo consenso al trattamento dei dati personali per finalità di *marketing*.

Il *double opt*-in come misura minima di garanzia

Con questo Provvedimento il Garante Privacy rafforza il ruolo del *double opt-in* come *best practice* per la raccolta e la documentazione del consenso per il trattamento di dati personali per finalità di *marketing*.

Non esiste un obbligo normativo esplicito in merito; tuttavia, tra i requisiti di liceità del consenso è prevista la responsabilità del titolare di documentare che l'interessato abbia effettivamente prestato il proprio consenso.

Il Garante Privacy ha infatti più volte ricordato (Provvedimento 429/2022, doc. web 9852290; Provvedimento 413/2021, doc. web 9737185; Provvedimento 437/2017, doc. web 7320903) che la documentazione del consenso in modalità *double opt-in* rappresenta una forma di documentazione che offre maggiori garanzie e che, allo stato dell'arte, può essere configurata come una misura minima di protezione, sia per l'interessato che per il titolare.

Tuttavia, il *doble opt*-in non è l'unica "misura minima" di protezione che i titolari possono adottare: il Garante Privacy vi ricomprende infatti

anche qualsiasi altra misura in grado di fornire un pari livello di garanzia.

Il Provvedimento non elenca espressamente i meccanismi alternativi ritenuti validi, limitandosi a richiamare le modalità di documentazione del consenso indicate all'interno del codice di condotta in materia di *telemarketing* e *teleselling* (Provvedimento 148/2024), quali, ad esempio, la conservazione sia dell'indirizzo IP e dell'orario in cui l'utente ha prestato il consenso, sia della prova dell'invio di un messaggio di conferma della registrazione del consenso (ad es., un SMS).

Conclusioni

Il Provvedimento evidenzia l'importanza per i titolari del trattamento di adottare meccanismi in grado di dimostrare che il trattamento sia stato effettuato conformemente alle disposizioni del GDPR e che l'interessato abbia prestato validamente il proprio consenso.

In tale ottica, tutte le imprese che intendano trattare dati personali per finalità di *marketing* dovranno assicurarsi che i meccanismi utilizzati per raccogliere e documentare i consensi acquisiti offrano garanzie analoghe a quelle fornite con l'adozione del modello *double opt-in*.

In altri termini, quel che conta, indipendentemente dal meccanismo scelto, è che il titolare sia in grado di assicurare e comprovare la provenienza del dato per assicurare cha sia proprio l'interessato ad aver prestato il consenso.

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