

Sanzione per Poste Italiane e Postepay per oltre 12 milioni di euro



Studio Previtì

ASSOCIAZIONE PROFESSIONALE

152

SEGNALAZIONI E RECLAMI RICEVUTI

14,5 MILIONI

APP ANDROID COINVOLTE
(Banco Posta + PostePay)

303K

APP BLOCCATE PER MANCATO RILASCIO DEL
CONSENSO DEI CLIENTI

28 MESI

RETENTION DATI SISTEMI DI THREATMETRIX
(COMPONENTE DELLA PIATTAFORMA
ANTIFRODE DI POSTE ITALIANE)



Cronologia del procedimento

1) Aprile - Maggio 2024

140 segnalazioni e 12 reclami. AGCM apre istruttoria per pratiche commerciali scorrette.

2) Aprile 2024

Prima richiesta di informazioni del Garante ex art. 157 Codice Privacy. Il trattamento è condotto da Poste Italiane e Postepay come contitolari in adempimento di un obbligo di legge per la rilevazione di malware nei dispositivi mobili.

3) Luglio 2024

Ispezione Garante presso sede Poste Italiane. Accertamento funzionamento ThreatMetrix.

4) Ottobre 2024 - Gennaio 2025

Seconda richiesta ex art.157 Codice Privacy. Retention dei dati di 28 mesi in ThreatMetrix; I dati sono trattati per fornire alla Piattaforma Integrata Anti-Frode (PIAF) l'esito dell'analisi del rischio compendiato in uno score.

5) Aprile 2025

Avvio procedimento correttivo e sanzionatorio per violazione artt. 5,6,13, 25, 28,32, 35 GDPR.

6) Aprile 2025

Memoria difensiva della società: è ribadita l'adozione dell'app ThreatMetrix in attuazione degli obblighi normativi ed in conformità al principio di responsabilizzazione per la lotta alle frodi.

7) Giugno 2025

Audizione: la Società mantiene il punto sull'applicazione della direttiva sui sistemi di pagamento, con la vigilanza e la cooperazione della Banca d'Italia, per l'aumento dei tentativi di frode informatica.

8) 17 Aprile 2026

Adozione di ordinanza ingiunzione.



**Il nucleo delle
argomentazioni del
Garante**

La scelta di adottare una soluzione di tracciamento generalizzato sui dati personali - la lista delle applicazioni installate o in esecuzione, potenzialmente idonee a rivelare abitudini, interessi, condizioni sanitarie, convincimenti religiosi e altri aspetti potenzialmente rientranti anche nelle categorie particolari di dati di cui all'art. 9 GDPR, così come la configurazione del prodotto ThreatMetrix - risponde più a una strategia volontaria di gestione del rischio che a un effettivo obbligo normativo, poiché la disciplina antifrode richiamata (Direttiva PSD2) non impone, di per sé, la necessità dei trattamenti dei dati personali concretamente effettuati dalle Società.

Infatti, nei sette mesi di utilizzo, il sistema non ha registrato una rilevazione maggiore o più efficace di fenomeni fraudolenti.

Violazioni accertate

Art. 122 CODICE PRIVACY

La quantità e qualità di dati trattati, non necessari per l'erogazione del servizio, non può consentire alle Società di prescindere dalla raccolta di consenso degli interessati clienti.

Art 5 GDPR

Violazione del principio di minimizzazione per raccolta di dati ultronei al necessario. Retention superiore a quanto dichiarato in sede di procedimento (28 vs 24 mesi).

Art 6 GDPR

Base giuridica errata: obbligo legale non pertinente al trattamento concreto.

Art. 13 GDPR

Informativa insufficiente: mancata specificità di informazioni ai clienti sul trattamento ThreatMetrix.

Art. 25 GDPR

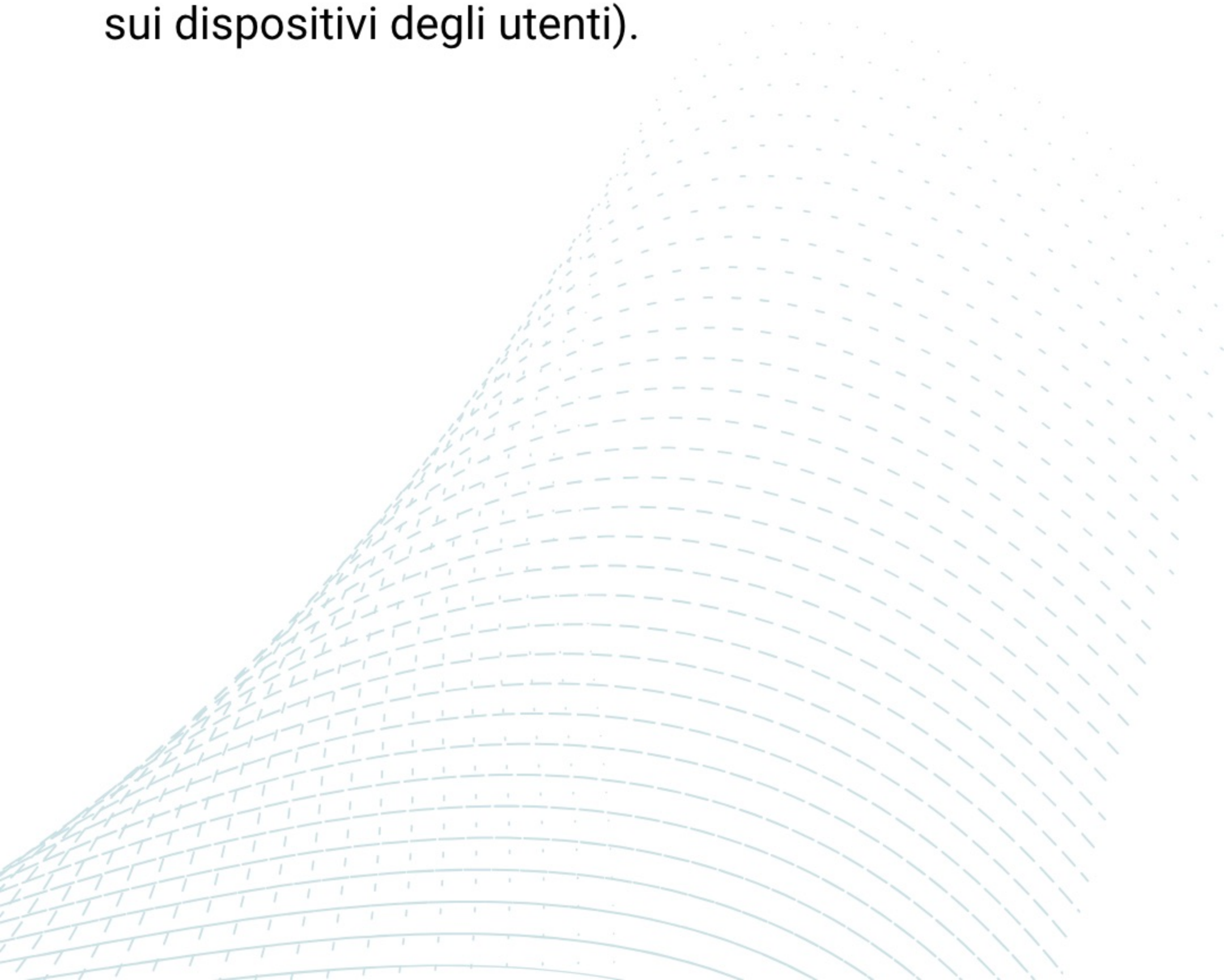
Violazione dei principi di privacy by design/default: non risulta effettuata alcuna valutazione circa l'effettiva necessità del trattamento dei dati né emergono evidenze circa l'esame di soluzioni alternative e meno invasive (esistenti sul mercato e adottate da altri operatori).

Art. 28 GDPR

Contratti con responsabili/sub-responsabili non adeguatamente strutturati e coerenti con il trattamento.

Art. 35 GDPR

DPIA effettuata con riferimento a tutti i trattamenti di dati personali necessari allo svolgimento delle attività antifrode, non anche calibrata sul trattamento specifico e sulla peculiare natura di dati trattati (informazioni rilevabili dalle app in uso sui dispositivi degli utenti).



AGCM - Provvedimento N. 31566/2025 del 20 maggio 2025

L'Autorità Garante della Concorrenza e del Mercato – nel corso della propria istruttoria – aveva rilevato pratiche commerciali scorrette ex artt. 20, 24 e 25 del Codice del Consumo. La circostanza rilevata per cui *"all'utilizzo del nuovo sistema non è corrisposto, nei primi sette mesi di attuazione, una rilevazione maggiore o più efficiente di fenomeni fraudolenti"* è stata valorizzata dal Garante per escludere che il trattamento dei dati tramite le app fosse strettamente necessario a garantire il servizio .

Misure correttive imposte

01 Interruzione del trattamento

Svolto tramite ThreatMetrix e consistente nella raccolta dei dati del dispositivo relativi all'utilizzo delle app installate e/o in esecuzione.

02 Politiche di conservazione

Individuare specifiche tempistiche di conservazione dei dati degli utenti trattati mediante l'applicativo ThreatMetrix.

03 Comunicazione all'Autorità

Riscontro sulle iniziative intraprese entro i successivi 30 giorni.





Studio Previti

ASSOCIAZIONE PROFESSIONALE

contatti@previti.it
www.previti.it



06.3234623
02.795587



Via Cicerone, 60 00193 Roma
Via Stradivari, 4 20131 Milano