DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Tracking pixel nelle e-mail e soft spam: obblighi e responsabilità

Adeguamento operativo per banche e assicurazioni alla luce del provvedimento del Garante

Maggio 2026

Giulio Novellini, Partner, Portolano Cavallo

Giulio Novellini, Partner, Portolano Cavallo

Giulio Novellini

Giulio Novellini si occupa di Privacy, Cyber Security e Data Protection, Internet & Ecommerce e Nuove Tecnologie (quali Intelligenza Artificiale, Blockchain e Smart Contracts). Nel corso della sua esperienza professionale, ha assistito società nazionali e multinazionali occupandosi di contenzioso e compliance in materia di Protezione dei Dati Personali. Ha maturato un'esperienza particolare nella consulenza riguardante siti web e app, compliance online in materia di cookie, trattamento dei dati per finalità di Marketing, Ecommerce, trattamento transfrontaliero di dati personali e violazione dei dati personali.

Studio Legale
Portolano Cavallo

PORTOLANO CAVALLO

1. Introduzione: un provvedimento che riguarda anche gli istituti di credito e assicurativi

Il provvedimento n. 284 adottato dal Garante per la Protezione dei Dati Personali il 17 aprile 2026 ("Provvedimento"), recante le Linee Guida in materia di utilizzo dei cd. "tracking pixel" nelle e-mail, non è un intervento rivolto esclusivamente al mondo dell'e-commerce o del marketing digitale generico. Le sue prescrizioni investono in misura significativa banche, intermediari finanziari, compagnie assicurative e, più in generale, tutti i soggetti vigilati che fanno un uso sistematico della posta elettronica per comunicare con la propria clientela.

La ragione è strutturale. Il settore bancario e assicurativo è tra i più intensivi nell'utilizzo del canale e-mail, impiegato tanto per le campagne promozionali su prodotti di investimento, polizze vita, conti correnti e mutui, quanto per le notifiche di servizio relative a operazioni effettuate, modifiche contrattuali e scadenze. A ciò si aggiungono le iniziative di cross-selling e upselling verso clienti già acquisiti, nonché gli adempimenti di compliance obbligatori, quali le informative MiFID, le comunicazioni IVASS e gli avvisi antifrode. In quasi tutte queste categorie, i tracking pixel vengono inseriti (spesso in modo inconsapevole, attraverso le piattaforme di marketing automation o i provider SaaS) per rilevare aperture, dispositivi, orari di consultazione e numero di accessi successivi.

Il Provvedimento impone ora una ricognizione sistematica di questi trattamenti, introduce obblighi informativi di portata generale, un regime di consenso strutturato e un diritto di revoca granulare che consente al destinatario di rifiutare il tracciamento senza doversi disiscrivere dalle comunicazioni stesse. Il termine di adeguamento è fissato in sei mesi dalla pubblicazione del Provvedimento in Gazzetta Ufficiale, intervenuta con la pubblicazione sulla Gazzetta Ufficiale n. 98 del 29 aprile 2026, il che rende necessario avviare senza indugio il percorso di adeguamento al fine di garantire la piena conformità entro il 29 ottobre 2026.

2. Il quadro normativo applicabile: art. 122 e art. 130 del Codice Privacy, direttiva e-Privacy, GDPR

2.1 *La struttura del doppio binario normativo*

Il Provvedimento si muove lungo due piani normativi distinti che, pur parzialmente sovrapponendosi, conservano ciascuno una propria autonoma portata applicativa.

vedi l'articolo online

Il primo è quello dell'art. 122 del d.lgs. 196/2003 ("Codice Privacy"), che dà attuazione all'art. 5(3) della direttiva e-Privacy (direttiva 2002/58/CE, come modificata dalla direttiva 2009/136/CE). La norma prevede che per memorizzare informazioni sul dispositivo dell'utente, o per accedere a informazioni già presenti su di esso, sia necessario il consenso informato dell'interessato, salvo specifiche eccezioni. Il Garante ha ricondotto i pixel di tracciamento a entrambe le ipotesi disciplinate dalla norma.

Il secondo piano è quello dell'art. 130 del Codice Privacy, che disciplina l'invio di comunicazioni promozionali tramite posta elettronica e altri strumenti automatizzati. La disposizione stabilisce, al comma 1, fermo restando quanto previsto dagli artt. 8 e 21 del d.lgs. 70/2003, la regola del consenso preventivo per l'uso di sistemi automatizzati di chiamata o di comunicazione senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale; al comma 2, estende il medesimo regime di consenso preventivo alle comunicazioni effettuate per le medesime finalità mediante posta elettronica, telefax, messaggi SMS, MMS o di altro tipo; al comma 4, la deroga del cd. soft spam per le comunicazioni a clienti con rapporto contrattuale in essere; e al comma 5, il divieto assoluto di comunicazioni con identità del mittente occultata.

I due piani, pur sovrapponendosi in parte, non coincidono. Può accadere che una comunicazione sia legittima ai sensi dell'art. 130, perché inviata in regime di soft spam a un cliente esistente, e tuttavia illecita ai sensi dell'art. 122, perché contenente un pixel di tracciamento individualizzato inserito senza autonomo consenso.

2.2 *Il Regolamento (UE) 2016/679 ("GDPR") come cornice generale e l'esclusione del legittimo interesse*

Il GDPR costituisce la cornice normativa di riferimento per tutti i trattamenti di dati personali, ma cede il passo quando la direttiva e-Privacy — e le relative norme nazionali di recepimento contenute nel Codice Privacy — intervengono con una disciplina più specifica. In questi casi, le norme del Codice Privacy prevalgono in quanto *lex specialis*. La conseguenza pratica è che, per individuare la base giuridica di un trattamento che ricada nell'ambito di applicazione della direttiva e-Privacy, non si può attingere liberamente al catalogo dell'art. 6 GDPR: occorre guardare in primo luogo alle disposizioni del Codice Privacy, e solo in via residuale al Regolamento.

Per la pratica bancaria e assicurativa, questa gerarchia normativa produce una conseguenza di grande rilievo: il legittimo interesse di cui all'art. 6, par. 1, lett. f) GDPR non può essere invocato a fondamento né dell'e-mail marketing né del tracciamento tramite pixel. L'art. 130, comma 2, del Codice Privacy non lo contempla tra i presupposti di liceità, e lo stesso vale per l'art. 122. L'esclusione è assoluta e non ammette bilanciamento. Ciò non significa, tuttavia, che ogni comunicazione promozionale via e-mail richieda il consenso: l'art. 130, comma 4, prevede il meccanismo del cd. soft spam (v. infra, § 4), che consente l'invio senza consenso al ricorrere di cinque condizioni cumulative. Il soft spam non si fonda sul legittimo interesse del GDPR, bensì costituisce una deroga autonoma e tipizzata, prevista dalla normativa e-Privacy, che opera su presupposti propri. Quanto ai tracking pixel, anche quando l'invio è lecito in regime di soft spam, il pixel individualizzato necessita di un autonomo fondamento giuridico ai sensi dell'art. 122, individuato dal Garante nel consenso specifico o nel ricorrere di una delle tre deroghe tipizzate dal provvedimento (v. infra, § 4.4).

Le ricadute di questa esclusione sulla corretta indicazione della base giuridica nelle informative privacy, un profilo che nella prassi bancaria e assicurativa risulta frequentemente disatteso, sono esaminate più avanti (v. infra, § 4.3).

2.3 *La qualificazione costituzionale della corrispondenza e il suo rilievo per il settore*

Il Garante ha attribuito rilievo autonomo alla natura del canale comunicativo, qualificando il servizio di posta elettronica come per sua stessa natura destinato a veicolare contenuti privati, anche considerato il diritto, di rilevanza costituzionale, alla riservatezza ed inviolabilità della corrispondenza, con riferimento all'art. 15 Cost. e all'art. 8 CEDU.

Per banche e assicurazioni, ciò significa che il livello di protezione richiesto per il canale e-mail è strutturalmente più elevato rispetto a quello applicabile agli strumenti di tracciamento sui siti web. Le logiche di enforcement in materia di cookie non possono essere trasposte alla posta elettronica, che gode di una tutela rafforzata radicata nel diritto fondamentale alla segretezza della corrispondenza.

vedi l'articolo online

3. Il meccanismo tecnico del pixel e la sua qualificazione giuridica

3.1 *Come funziona il tracking pixel nelle e-mail bancarie e assicurative*

I pixel di tracciamento inseriti nei messaggi di posta elettronica sono immagini, spesso trasparenti e di dimensioni molto ridotte, non direttamente contenute nell'e-mail ma ospitate su server remoti. Ogni volta che il destinatario apre il messaggio, un codice HTML incorporato nel corpo dell'e-mail aziona in automatico una richiesta verso il server del mittente; in risposta, l'immagine viene scaricata dal client di posta e archiviata nella memoria del terminale dell'utente.

Il processo consente al mittente di rilevare l'avvenuta apertura dell'e-mail, l'indirizzo IP del destinatario, il tipo di dispositivo utilizzato, il tempo di consultazione e il numero di aperture successive. Nelle piattaforme di marketing automation utilizzate nel settore bancario (Salesforce Marketing Cloud, Adobe Campaign, HubSpot, Mailchimp e simili), il tracking pixel è quasi sempre attivato per default, per calcolare open rate, click-through rate e alimentare i motori di scoring comportamentale.

In ogni caso, il Garante ha rilevato che non esiste una standardizzazione dei nomi dei tracking pixel, né una loro codifica o sintassi universalmente condivisa. Ne consegue che l'identificazione dei pixel nei template e-mail richiede un'analisi tecnica puntuale del codice HTML e la dimostrazione della conformità impone un processo di audit tecnico sistematico.

3.2 *Dati raccolti dal pixel: rilevanza per la profilazione bancaria e assicurativa*

Un singolo tracking pixel è in grado di raccogliere una pluralità di informazioni: l'identificativo univoco associato al destinatario, l'indirizzo IP, il tipo di client di posta utilizzato (webmail, app mobile o client desktop), il sistema operativo, la data e l'ora di apertura, nonché il numero di riaperture successive. Quando questi dati vengono incrociati con le informazioni già in possesso della banca o della compagnia assicurativa — quali l'anagrafica del cliente, il portafoglio prodotti sottoscritti e lo storico delle transazioni — possono alimentare modelli di profilazione comportamentale con ricadute significative su offerte commerciali, pricing e strategie di retention.

È proprio questa dimensione profilante a collocarsi al centro della ratio del provvedimento. I pixel di tracciamento, infatti, sono marcatori particolarmente invasivi in ragione del loro carattere nascosto, e la loro installazione — non nota all'interessato — determina una violazione del principio di correttezza sancito dall'art. 5, par. 1, lett. a) GDPR.

4. Il soft spam nel settore bancario e assicurativo: condizioni, limiti e intersezione con il tracciamento

4.1 *La deroga del soft spam e la sua rilevanza nel settore*

L'art. 130, comma 4 del Codice Privacy prevede che il titolare del trattamento possa utilizzare le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, a fini di vendita diretta di propri prodotti o servizi analoghi, senza acquisire un nuovo consenso, a condizione che l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni.

Per banche e assicurazioni, questa previsione riveste un'importanza pratica di primo piano, poiché rappresenta lo strumento giuridico attraverso cui è possibile proporre al titolare di un conto corrente la sottoscrizione di un mutuo, o al cliente che ha stipulato una polizza auto l'acquisto di una copertura vita. Come già chiarito (v. supra, § 2.2), il soft spam non trae il proprio fondamento dal legittimo interesse previsto dal GDPR, ma si configura piuttosto come un'esenzione autonoma e autosufficiente, radicata direttamente nell'art. 130, comma 4, del Codice Privacy. I presupposti che ne condizionano l'operatività sono di natura cumulativa e vanno interpretati in senso restrittivo.

4.2 *Le cinque condizioni cumulative e le loro ricadute per banche e assicurazioni*

i. Rapporto contrattuale pregresso a titolo oneroso. La Corte di Cassazione ha chiarito che il concetto di "vendita" va interpretato in senso restrittivo, potendo la deroga trovare applicazione solo laddove sia già stato concluso un contratto a titolo oneroso (cfr. Cass. I sez. civile, 15 marzo 2023, n. 7555). Alla luce di questo orientamento, restano fuori dal perimetro il cliente che abbia richiesto un preventivo senza sottoscrivere alcun contratto, il lead acquisito tramite form web senza perfezionamento del rapporto e il cliente in fase di onboarding non ancora concluso;

ii. Identità del titolare del trattamento. La deroga non è invocabile da un soggetto diverso dall'originario titolare del trattamento. Le reti di agenti, i promotori finanziari e i broker assicurativi non possono autonomamente avvalersi di questo meccanismo per proprie campagne promozionali. A titolo esemplificativo, il responsabile del trattamento che riutilizzi i dati senza specifica direttiva del titolare effettua un trattamento *sine titulo*; in merito si veda il provvedimento del Garante del 12 febbraio 2026 (doc. web n. 10227039) nei confronti di Bressanelli Galli Gelpi Porta & C. S.r.l., nel quale un intermediario assicurativo aveva riutilizzato dati raccolti in qualità di responsabile per proprie finalità di marketing;

iii. Analogia merceologica. I prodotti oggetto della promozione devono essere analoghi a quelli del contratto originario. La valutazione va condotta in modo restrittivo e caso per caso: per gli istituti con offerta diversificata (bancassurance, gestione del risparmio, credito al consumo, mutui), l'analogia non può essere presunta per il solo fatto che i prodotti rientrino nel medesimo perimetro di gruppo;

iv. Informativa contestuale e continuativa. L'interessato deve essere messo in condizione di opporsi sia al momento della raccolta dell'indirizzo sia in occasione di ogni successiva comunicazione. Il rifiuto iniziale può essere espresso anche accedendo alla propria area personale dopo la sottoscrizione del contratto. Ne discende che le informative precontrattuali e contrattuali, i cd. documenti KID (Key Information Document) e i set informativi MiFID/IVASS devono contenere un riferimento esplicito e chiaro alla facoltà di opposizione al soft spam, senza relegarlo nelle note a piè di pagina; e

v. Opt-out reale, non condizionato. La mera disponibilità di un link di opposizione non sana a posteriori un invio illecito: è lo stesso inoltro dell'e-mail a risultare privo di fondamento se le condizioni di legittimità non sono soddisfatte ab origine (cfr. provvedimento del Garante dell'11 settembre 2025, doc. web n. 10224441, nei confronti di ISV Group S.r.l.s. e Ismax S.r.l.s.). In altri termini, l'opt-out deve prevenire l'invio, non limitarsi a interromperlo.

Sul piano operativo, le cinque condizioni cumulative sopra descritte impongono agli istituti di credito e alle compagnie assicurative una serie di adeguamenti strutturali che investono tanto i processi commerciali quanto i sistemi informativi. In primo luogo, la restrittiva interpretazione del requisito del contratto oneroso concluso esclude dal perimetro del soft spam intere categorie di contatti che nella prassi bancaria vengono frequentemente destinatari di comunicazioni promozionali. Ne consegue la necessità di segmentare il database clienti in modo rigoroso, distinguendo i rapporti contrattuali perfezionati da quelli meramente avviati o in fase istruttoria.

Inoltre, il requisito dell'analogia merceologica impone agli operatori bancari e assicurativi con offerta diversificata di predisporre matrici di corrispondenza prodotto per prodotto, senza presumere automaticamente l'analogia tra categorie merceologiche eterogenee come, ad esempio, tra un conto corrente e una polizza vita. Sul versante procedurale, l'obbligo di garantire un meccanismo di opposizione effettivo e non condizionato richiede che i sistemi CRM siano dotati di funzionalità di opt-out operanti in tempo reale, così da impedire l'invio di ulteriori comunicazioni dal momento stesso in cui l'opposizione viene registrata, senza dilazioni di natura tecnica o organizzativa. Infine, poiché il soft spam legittima esclusivamente l'invio della comunicazione e non il tracciamento del destinatario tramite pixel individualizzato, le banche sono tenute a disaccoppiare i due profili nella configurazione delle piattaforme di marketing automation. Le e-mail inviate in regime di soft spam dovranno pertanto essere prive di pixel individualizzati ovvero dotate di pixel esclusivamente statistici e anonimizzati.

4.3 *Il nodo dell'informativa come base giuridica: l'errore da correggere*

Come già evidenziato (v. supra, § 2.2), l'indicazione del legittimo interesse quale base giuridica per il marketing via e-mail è scorretta. L'informativa deve richiamare, a seconda dei casi, il consenso ex art. 130, commi 1 e 2, del Codice Privacy per le comunicazioni promozionali fondate su tale presupposto, ovvero la deroga ex art. 130, comma 4, per quelle inviate in regime di soft spam. L'art. 6, par. 1, lett. f) GDPR non può in alcun caso essere indicato come fondamento di liceità per tali trattamenti.

L'erronea individuazione del fondamento giuridico nell'informativa configura, di per sé, una violazione del principio di trasparenza ex art. 5(1)(a) GDPR e delle prescrizioni degli artt. 13-14 GDPR, con potenziale ricaduta sanzionatoria autonoma. Le informative che presentano tale difformità devono pertanto essere rettificate entro il termine di sei mesi dalla pubblicazione del Provvedimento in Gazzetta Ufficiale.

4.4 L'intersezione tra soft spam e tracking pixel: il doppio onere

Il punto centrale è che soft spam e tracciamento tramite pixel operano su piani normativi distinti e autonomi. Il fatto che un'e-mail sia lecitamente inviata in regime di soft spam non implica che il pixel inserito in quella stessa e-mail sia anch'esso lecito.

Il soft spam, fondato sull'art. 130, comma 4, consente di inviare l'e-mail senza consenso, ma il tracking pixel ricade nell'art. 122, che richiede un autonomo presupposto giuridico. Un'e-mail di soft spam con pixel individualizzato è lecita quanto all'invio ma illecita quanto al tracciamento, salvo che ricorra una delle tre deroghe tipizzate dal Garante o sia stato acquisito un consenso specifico. Il titolare ha dunque due strade: acquisire un consenso autonomo al pixel, oppure utilizzare esclusivamente pixel statistici anonimizzati.

Le tre deroghe al consenso per i pixel sono: (i) statistiche aggregate anonimizzate, con pixel univoci uguali per tutti i destinatari e anonimizzazione dei dati tecnici correlati; (ii) misure di sicurezza relative al processo di autenticazione dell'utente, quali ad esempio la verifica dell'effettiva ricezione di un codice OTP o di un link di conferma dell'identità; e (iii) messaggi istituzionali o di servizio che il titolare ha l'obbligo giuridico di inoltrare e rispetto ai quali rilevi l'effettiva presa di conoscenza.

Per il settore bancario e assicurativo, la terza deroga ha particolare rilievo: comunicazioni su modifiche contrattuali, incidenti di sicurezza, comunicazioni IVASS obbligatorie, avvisi antifrode possono beneficiare dell'esenzione, purché il tracciamento serva a verificare la presa di conoscenza e non sia utilizzato per profilazione.

5. Implicazioni pratiche per banche e assicurazioni: una mappatura per tipologia di comunicazione

5.1 *E-mail promozionali e DEM (Direct E-mail Marketing)*

Le campagne DEM costituiscono la categoria di comunicazione a maggiore esposizione sotto il profilo della conformità. Il motivo risiede nella necessità di un duplice presupposto di liceità: da un lato, l'invio della comunicazione promozionale richiede il consenso preventivo dell'interessato ai sensi dell'art. 130, commi 1 e 2, del Codice Privacy; dall'altro, l'inserimento di un pixel di tracciamento individualizzato nell'e-mail necessita di un autonomo consenso ai sensi dell'art. 122. Ne consegue che nessuna DEM contenente un pixel individualizzato (ovvero di tracciamento) può essere legittimamente inviata in assenza di entrambi i consensi. Qualora il destinatario sia un cliente con rapporto contrattuale in essere e il prodotto promosso sia analogo a quello già sottoscritto, l'invio dell'e-mail può avvenire in regime di soft spam senza consenso al marketing; tuttavia, anche in tale ipotesi, il pixel continua a richiedere un autonomo fondamento giuridico e non può beneficiare della medesima esenzione.

Il duplice presupposto di liceità non comporta tuttavia, necessariamente, la raccolta di due manifestazioni di volontà distinte. Il Garante ammette infatti la possibilità di un consenso unico: il consenso al tracciamento tramite pixel può essere ricompreso nella medesima manifestazione di volontà con cui l'interessato acconsente alla ricezione delle comunicazioni promozionali, senza necessità di una richiesta separata, purché la formulazione sia neutra, priva di forzature e contenga un riferimento chiaro ed esplicito alla presenza del tracking pixel e alle relative finalità di tracciamento. I form di raccolta del consenso marketing dovranno pertanto essere aggiornati per includere tale indicazione, in modo che l'interessato sia posto in condizione di comprendere che, prestando il consenso, autorizza non soltanto la ricezione delle comunicazioni ma anche il monitoraggio della propria interazione con le stesse.

5.2 *Comunicazioni obbligatorie ex lege*

Le comunicazioni che il titolare ha l'obbligo giuridico di inviare (es. informative MiFID II, documenti KID PRIIPs, comunicazioni IVASS ex art. 185 Cod. Ass., avvisi ex art. 118 TUB, comunicazioni di violazione dei dati personali all'interessato ex art. 34 GDPR) ricadono nella terza deroga, che esclude il consenso al pixel per messaggi istituzionali rispetto ai quali rilevi l'effettiva presa di conoscenza.

Il punto critico è che l'esenzione opera solo quando il tracciamento serve a verificare la presa di conoscenza e non può essere utilizzata per ricavare informazioni di profilazione. Il pixel in una comunicazione ex art. 118 TUB può rilevare se il cliente ha aperto l'e-mail; non può essere collegato a un motore di profilazione.

5.3 *Newsletter e comunicazioni editoriali*

Per le newsletter (aggiornamenti di mercato, analisi finanziarie, comunicati istituzionali), il Garante richiede consenso sia all'invio (art. 130, commi 1 e 2) sia al tracciamento individualizzato (art. 122). Il soft spam non è applicabile perché la newsletter non ha il carattere di vendita diretta di prodotti analoghi.

5.4 *Campagne di upselling e cross-selling tramite rete distributiva*

Banche e assicurazioni si avvalgono frequentemente di reti distributive esterne che inviano comunicazioni commerciali ai clienti finali. La distinzione tra titolare e responsabile del trattamento è spesso opaca, e l'uso del soft spam da parte di soggetti senza rapporto contrattuale diretto con il cliente è sistematicamente a rischio.

Il caso Bressanelli Galli Gelpi Porta (v. supra, § 4.2) è il prototipo del rischio; infatti, il riutilizzo sine titulo dei dati da parte dell'intermediario espone anche il titolare preponente a conseguenze reputazionali e alla necessità di rielaborare gli standard contrattuali per l'intera rete.

6. Profili di responsabilità: il titolare, i fornitori SaaS, le reti distributive

L'ecosistema di e-mail marketing delle banche si articola tipicamente in una pluralità di soggetti, che spazia dalla piattaforma di marketing automation al provider di e-mail delivery, dall'agenzia creativa ai fornitori di dati terzi, ciascuno dei quali può assumere un ruolo autonomo sotto il profilo della protezione dei dati. Il Garante ne è consapevole e, nel Provvedimento, individua cinque figure soggettive distinte (mittente, fornitore SaaS, fornitore di liste, fornitore della tecnologia di tracciamento e content creator), senza tuttavia cristallizzarne i ruoli in categorie rigide: la qualificazione è rimessa a una valutazione caso per caso, anche alla luce dell'art. 26 del Regolamento in materia di contitolarità. Ne discende che ogni istituto è chiamato a predisporre una mappatura documentata della propria supply chain e-mail, ricostruendo con precisione i flussi di dati e le responsabilità di ciascun attore coinvolto.

L'importanza di questo esercizio è confermata dalla prassi sanzionatoria, giacché nel provvedimento dell'11 settembre 2025 (doc. web n. 10224441) nei confronti di ISV Group S.r.l.s. e Ismax S.r.l.s. il Garante ha accertato che il titolare risponde delle violazioni commesse dal fornitore ogniqualvolta non abbia adottato adeguate misure di controllo, tanto in *eligendo* quanto in *vigilando*. Il medesimo principio si estende alla gestione delle reti distributive esterne: le banche e le compagnie che se ne avvalgono sono tenute a stabilire contrattualmente perimetro e limiti del trattamento, ivi inclusi il divieto di utilizzo autonomo del soft spam da parte degli agenti, il divieto di inserire pixel non autorizzati e le procedure di gestione delle opposizioni, posto che l'assenza di adeguate istruzioni contrattuali non esonera il titolare dalla responsabilità per le violazioni commesse dagli intermediari, imponendo l'accountability precauzioni concrete e documentate. A presidio dell'intero sistema si pone, infine, l'art. 130, comma 6, del Codice Privacy, il quale attribuisce al Garante un ulteriore potere correttivo: in caso di reiterata violazione delle disposizioni in materia di comunicazioni indesiderate, l'Autorità può ordinare ai fornitori di servizi di comunicazione elettronica di attivare procedure di filtraggio sulle coordinate di posta elettronica da cui sono stati inviati i messaggi illeciti. Si tratta di una misura particolarmente incisiva per gli istituti di credito, poiché il filtraggio può tradursi nel blocco operativo dei canali e-mail utilizzati per le comunicazioni alla clientela, con conseguenze che si estendono ben oltre il piano sanzionatorio pecuniario. Questa eventualità rende ancor più urgente, per le banche e le compagnie assicurative, il presidio rigoroso dell'intera catena di responsabilità.

7. Adattamenti operativi: CRM, processi interni, contratti con terzi, formazione

7.1 *Riprogettazione dell'architettura del consenso nel CRM*

Per conformarsi al Provvedimento, il sistema CRM bancario deve essere in grado di gestire almeno quattro stati distinti per ciascun contatto cliente, integrandoli nelle logiche di invio in modo coerente e automatizzato.

Il primo stato concerne il consenso alle comunicazioni promozionali ai sensi dell'art. 130, commi 1 e 2, del Codice Privacy. Il secondo attiene all'eleggibilità al soft spam ex art. 130, comma 4 e presuppone la verifica automatica della sussistenza di un contratto oneroso concluso, dell'analogia merceologica e dell'assenza di opposizione da parte dell'interessato. Il terzo stato registra l'eventuale opposizione specifica al soft spam, mentre il quarto traccia il consenso al tracking pixel, distinguendo tra tracciamento individualizzato, statistico o negato.

Perché questa architettura integrata è così importante? Perché un CRM che gestisca consenso marke-

ting e soft spam come compartimenti stagni, privi di reciproca interoperabilità, è strutturalmente non conforme. Lo dimostra il provvedimento del Garante del 17 luglio 2024 (doc. web n. 10084158) nei confronti di Iliad Italia S.p.A., sanzionata con euro 50.000 per aver aggirato la volontà dell'interessato di non ricevere comunicazioni promozionali, veicolandogliele comunque attraverso il canale del soft spam.

In termini operativi, la regola di invio che ne risulta può essere sintetizzata così: un contatto riceve un'e-mail promozionale con tracking individualizzato soltanto se ha prestato sia il consenso marketing sia il consenso al pixel; riceve comunicazioni in regime di soft spam — ma senza tracking individualizzato — solo se risulta eleggibile, non ha espresso opposizione e il pixel è configurato in modalità statistica anonimizzata; infine, non riceve alcuna comunicazione se ha manifestato la propria opposizione in qualsiasi forma.

7.2 *Il diritto di revoca granulare: impatti tecnici e comunicativi*

Tra le novità di maggiore impatto pratico introdotte dal Provvedimento spicca il diritto di revoca granulare. In sostanza, l'utente non è più costretto a scegliere tra il "tutto o niente": può revocare il consenso in modo totale, interrompendo la ricezione di qualsiasi messaggio, oppure in modo parziale, rifiutando il solo tracciamento tramite pixel e continuando a ricevere le comunicazioni prive di tali marcatori.

Sul piano operativo, ciò significa che ogni e-mail deve contenere un link a una pagina di gestione delle preferenze nella quale il cliente possa scegliere agevolmente tra la disiscrizione totale e l'opt-out dal solo tracciamento. Per le banche, la soluzione più efficace consiste nell'integrare questa pagina nell'area personale del cliente, rendendola accessibile anche tramite link diretto.

7.3 *L'aggiornamento delle informative e la comunicazione ai clienti esistenti*

Il principio è chiaro: tutti i titolari che già utilizzano pixel di tracciamento sono tenuti a informarne adeguatamente gli interessati; in mancanza, i dati raccolti tramite pixel risultano inutilizzabili. L'adeguamento si articola su tre fronti: la revisione delle informative precontrattuali e contrattuali, l'aggiornamento della sezione privacy del sito istituzionale e una comunicazione mirata ai clienti che siano già stati destinatari di e-mail contenenti pixel.

Per i trattamenti già in corso, il Garante ha previsto una soluzione pragmatica: il titolare potrà avvalersi dell'inoltro del primo messaggio utile — ovvero del primo momento di discontinuità nel rapporto con il cliente — per colmare il deficit informativo, senza dover procedere a una comunicazione ad hoc.

7.4 *La struttura dell'informativa per il consenso al tracciamento tramite pixel*

L'informativa relativa al tracciamento tramite pixel deve soddisfare requisiti specifici, sia di contenuto sia di forma, che si aggiungono a quelli già previsti dagli artt. 13 e 14 GDPR. Quanto al contenuto, l'informativa deve indicare in modo chiaro: (a) la presenza di pixel di tracciamento nelle e-mail inviate dal titolare; (b) la natura dei dati raccolti, quali indirizzo IP, tipo di dispositivo, sistema operativo, data e ora di apertura, numero di riaperture successive; (c) le finalità del tracciamento, distinguendo tra statistiche aggregate e profilazione individualizzata; (d) la base giuridica, che, come già chiarito (v. supra, § 4.3), va individuata nel consenso ex art. 122 del Codice Privacy o, ove applicabile, in una delle tre deroghe tipizzate dal Provvedimento, e mai nel legittimo interesse ex art. 6, par. 1, lett. f) GDPR; e (e) le modalità di esercizio del diritto di revoca granulare, precisando che è possibile rifiutare il solo tracciamento senza rinunciare alla ricezione delle comunicazioni.

Sul piano formale, l'informativa deve essere autonomamente percepibile e non può essere "nascosta" in clausole generiche o in sezioni residuali della privacy policy. Per banche e compagnie assicurative, ciò si traduce nell'inserimento di una sezione dedicata al tracciamento tramite pixel all'interno dell'informativa precontrattuale e contrattuale, con adeguata evidenza grafica. Il consenso al tracciamento, ove richiesto, deve essere raccolto mediante un'azione positiva e inequivocabile dell'interessato. Come già precisato (v. *supra*, § 5.1), il Garante ammette la possibilità di un consenso unico che ricomprenda sia la ricezione delle comunicazioni promozionali sia il tracciamento tramite pixel, senza necessità di due manifestazioni di volontà distinte, a condizione che la richiesta sia formulata in modo neutro, senza forzature, e contenga un riferimento esplicito alla presenza e alle finalità del pixel. Il consenso al tracciamento deve in ogni caso rimanere distinto dall'accettazione delle condizioni generali di contratto. Resta fermo che il rifiuto del consenso al tracciamento non può condizionare né l'erogazione del servizio né la ricezione delle comunicazioni di servizio o obbligatorie ex lege.

vedi l'articolo online

7.5 *Revisione dei contratti con i fornitori della supply chain e-mail*

I Data Processing Agreement stipulati con i fornitori della supply chain e-mail devono essere sottoposti a una revisione mirata, che includa almeno quattro profili essenziali: l'obbligo per il fornitore di dichiarare tutti i pixel incorporati per default nelle proprie piattaforme; la possibilità tecnica di procedere all'invio senza alcun tracking pixel; l'aggiornamento in tempo reale della suppression list; e il riconoscimento al titolare di un diritto di audit sulla conformità del fornitore al Provvedimento.

Con riguardo ai contratti con i fornitori di liste e le reti distributive, assume rilievo centrale la previsione di una dichiarazione e garanzia attestante che tutti gli indirizzi e-mail siano stati raccolti sulla base di un consenso valido, corredata da un obbligo di indennizzo a carico del fornitore nell'ipotesi in cui una sanzione sia riconducibile a dati da questi forniti.

Quanto ai contratti con le agenzie creative e i content creator, occorre prevedere che ogni template HTML consegnato sia privo di pixel di terze parti non dichiarati e che qualsiasi modifica successiva che introduca nuovi pixel sia subordinata all'approvazione preventiva del titolare o del DPO.

7.6 *Formazione del personale e gestione delle opposizioni*

La formazione del personale non è un adempimento meramente formale: il Garante l'ha espressamente valorizzata come misura correttiva attenuante nella quantificazione delle sanzioni, il che la rende anche un investimento strategico sul piano difensivo. I programmi formativi devono essere calibrati in funzione del profilo professionale dei destinatari.

Per i team marketing, la formazione deve assicurare la piena comprensione del doppio binario normativo tra art. 122 e art. 130 del Codice Privacy, la capacità di identificare i pixel presenti nelle piattaforme di invio, la padronanza delle procedure per configurare il tracciamento in modalità statistica anonimizzata e la gestione tempestiva delle opposizioni, con aggiornamento della suppression list entro 24-48 ore. Va inoltre ribadito che, in assenza di consenso, non è possibile inviare comunicazioni promozionali neppure utilizzando dati tratti da registri pubblici o indirizzi PEC estratti dall'indice nazionale.

Con riferimento alla formazione destinata ai team commerciali e al personale operante nelle reti distributive, i contenuti formativi devono chiarire che il soft spam non è invocabile in assenza di un contratto effettivamente concluso e che il mero tentativo di acquisto da parte del cliente non integra l'esimente. È altresì essenziale che il personale sappia distinguere tra un follow-up individuale e una campagna e-mail strutturata, e che le richieste informali di cancellazione, comunque pervenute, vengano tempestivamente convogliate nel sistema formale di gestione delle opposizioni, entro tempi predefiniti e documentati.

8. Il regime transitorio e le scadenze

L'Autorità individua un termine di sei mesi dalla pubblicazione in Gazzetta Ufficiale del Provvedimento per conformarsi alle prescrizioni ivi contenute. Per le banche e le compagnie assicurative, tale termine, in scadenza il 29 ottobre 2026 (v. *supra*, § 1), deve essere trattato come una scadenza progettuale cui associare un piano di adeguamento strutturato. Con riguardo ai trattamenti già in corso, il titolare, dopo aver assolto agli obblighi informativi, è tenuto a implementare un meccanismo di revoca anche granulare del consenso; si tratta di un regime transitorio, destinato ad essere progressivamente dismesso man mano che i rapporti vengono ricondotti al regime ordinario.

Per i trattamenti futuri, quali nuove campagne, nuovi contratti e nuovi clienti, la regola del consenso preventivo al pixel si applica invece immediatamente, senza possibilità di avvalersi del regime transitorio. Tenendo conto dei termini fissati dal Garante e della complessità degli adeguamenti richiesti per soggetti di dimensioni significative, la sequenza raccomandata per banche e assicurazioni si articola in quattro fasi successive.

In una prima fase occorre procedere all'audit tecnico del database clienti ai fini della classificazione per base giuridica (consenso marketing, soft spam, esenzione pixel), all'identificazione di tutti i pixel presenti nei template e-mail attraverso l'analisi del codice HTML, alla verifica dell'architettura CRM per l'introduzione del campo cd. pixel_consent e all'aggiornamento delle informative privacy con riferimento esplicito ai tracking pixel. Nella fase successiva è necessario provvedere alla configurazione del footer dinamico con link granulare alle preferenze, alla revisione dei DPA con i provider di piattaforme e-mail, all'aggiornamento delle clausole contrattuali con la rete distributiva e all'avvio dei programmi formativi per i team coinvolti.

In una terza fase si procede all'implementazione dell'automation di re-permission per i contatti inattivi, all'invio della prima comunicazione informativa ai clienti in regime di soft spam in corso con riferimento ai pixel e alla verifica che le piattaforme siano configurate per il rispetto del pixel_consent a livello di singolo contatto. Nella fase conclusiva devono essere completati l'aggiornamento del Registro delle Attività di Trattamento, la conclusione dei programmi formativi con documentazione tracciata e l'adeguamento di tutte le procedure interne di gestione dei consensi e delle opposizioni.

9. Conclusioni operative: una roadmap per il settore

Il provvedimento n. 284/2026 non è un provvedimento di nicchia. Per banche e assicurazioni, che comunicano con milioni di clienti via e-mail, utilizzano piattaforme con tracking attivato per default e si avvalgono di reti distributive complesse, l'intervento ha portata sistematica.

I punti fermi che emergono dalla lettura coordinata del provvedimento con la prassi sanzionatoria sono i seguenti.

Il legittimo interesse non è base giuridica utilizzabile né per l'e-mail marketing né per il tracking pixel. Le norme speciali del Codice Privacy prevalgono come lex specialis e le informative errate devono essere corrette entro il termine di adeguamento.

Il soft spam è legittimo ma strettamente perimetrato: si fonda sull'art. 130, comma 4, del Codice Privacy e non sul legittimo interesse. Funziona solo con contratto oneroso concluso, identità del mittente, analogia merceologica, informativa adeguata e opt-out funzionante. Soprattutto, legittima l'invio ma non il tracciamento: il pixel individualizzato richiede autonomo consenso o deve essere sostituito con pixel statistico anonimizzato.

Il tracking pixel richiede gestione autonoma rispetto alla base giuridica dell'invio. Le tre deroghe al consenso hanno perimetro rigoroso e non estensibile; al di fuori di esse, il consenso specifico è l'unico presupposto di liceità.

Il CRM deve essere riprogettato per gestire i quattro stati del contatto (consenso marketing, eleggibilità soft spam, opposizione soft spam, consenso pixel) in modo integrato, con logiche di invio che riflettano correttamente la volontà del cliente senza effetti incomprensibili.

I fornitori terzi, quali piattaforme SaaS, agenzie creative, fornitori di liste e rete distributiva, devono essere contrattualmente presidiati con clausole specifiche sui pixel, sulle suppression list, sugli audit e sulle garanzie di conformità. La carenza di controlli in eligendo e in vigilando espone il titolare a responsabilità solidale per le violazioni dei partner.

La documentazione è l'asset difensivo principale: ogni invio deve essere tracciato con riferimento alla base giuridica utilizzata; ogni opposizione deve essere registrata e aggiornata in tempo reale; i programmi formativi devono essere documentati con data, contenuti e partecipanti.

La conformità al provvedimento non è un costo operativo: è la condizione necessaria per un programma di e-mail marketing sostenibile nel medio-lungo termine, al riparo dal rischio di ordini di cancellazione del database, ossia la conseguenza più devastante dell'enforcement, ben più onerosa di qualsiasi sanzione pecuniaria.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it