DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Marketing, profilazione e protezione dei dati personali

Gennaio 2024

Giulia Mariuz, Counsel, Hogan Lovells
Elisabetta Nunziante, Associate, Hogan Lovells

Giulia Mariuz, Counsel, Hogan Lovells

Elisabetta Nunziante, Associate, Hogan Lovells

Studio Legale

Hogan Lovells

La difficoltà di coniugare la protezione dei dati personali con l'inevitabile necessità commerciale di pubblicizzare e promuovere i propri prodotti e attività è da sempre un tema trasversale a tutti i settori produttivi.

Da anni il rispetto della normativa a tutela dei dati personali nell'ambito del *direct marketing* e, più in generale, per i trattamenti a scopo pubblicitario o commerciale è al centro dell'attività ispettiva del Garante per la protezione dei dati personali ("**Garante**"), che ha comminato sanzioni per svariati milioni di euro a titolari del trattamento operanti in diverse *industry* (primi tra tutti il settore bancario, assicurativo e delle *utility*). In tempi più recenti, il corretto utilizzo dei dati per finalità di marketing ha assunto crescente rilevanza anche nel settore delle pratiche commerciali scorrette, dove l'Autorità garante per la concorrenza ed il mercato ("**AGCM**", competente anche per la tutela dei consumatori) ha sanzionato diversi operatori per non aver correttamente informato i consumatori in merito all'utilizzo dei loro dati per finalità commerciali, o non aver offerto loro la possibilità di scegliere liberamente in merito a tale utilizzo.

Il rispetto della normativa a tutela dei dati risulta, pertanto, di fondamentale importanza al fine di evitare danni economici e reputazionali molto pesanti, oltre che per mantenere il necessario rapporto di fiducia con la propria clientela e le proprie controparti commerciali. Nel prosieguo, si analizzerà la normativa applicabile in materia di marketing e *cookie* e verranno fornite delle pratiche indicazioni al fine di adottare correttamente le misure necessarie per conformarsi alla stessa. Verranno inoltre descritti i profili principali relativi alle regole in materia di *cookie* così come le problematiche giuridiche di maggior interesse in relazione all'*interplay* tra la normativa a tutela dei dati e le previsioni di settore in merito al trattamento dati nel settore delle comunicazioni elettroniche.

1. La regola del consenso per le comunicazioni commerciali

In Italia, la normativa relativa al marketing e alle comunicazioni promozionali (di implementazione delle previsioni della Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, **Direttiva e-Privacy**") è particolarmente rigida, dal momento che l'art. 130 (commi 1 e 2) del D. Lgs. 196/2003 ("**Codice Privacy**") richiede il consenso per qualsiasi comunicazione promozionale inviata tramite mezzi di comunicazione elettronica (quale ad

vedi l'articolo online

esempio telefono senza operatore, email, SMS, messaggi via chat), con limitate eccezioni che saranno illustrate nel prosieguo.

La necessità di ottenere un consenso informato, specifico ed esplicito (in particolare, non pre-flaggato o impostato di default) o "*opt-in*" alle attività di marketing è un principio consolidato, espressamente enunciato nelle Linee guida in materia di attività promozionale e contrasto allo spam del 4 luglio 2013[1], dove è chiarito che "*senza il consenso … non è possibile inviare comunicazioni promozionali con i predetti strumenti neanche nel caso in cui i dati personali siano tratti da registri pubblici, elenchi, siti web atti o documenti conosciuti o conoscibili da chiunque. Analogamente, senza il consenso preventivo degli interessati, non è lecito utilizzare per inviare e-mail promozionali gli indirizzi pec contenuti nell'indice nazionale degli indirizzi pec delle imprese e dei professionisti … istituito per favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica*".

Recentemente, il Garante ha evidenziato come, anche successivamente all'entrata in vigore del Regolamento 679/2016 ("**GDPR**"), al di fuori delle eccezioni previste per legge non sia possibile ricorrere a basi giuridiche alternative e, in particolare al legittimo interesse. In particolare, nel provvedimento doc. web. 9899880 del 17 maggio 2023, il Garante ha sottolineato come non possa essere invocato direttamente il considerando 47 del GDPR nella parte in cui indica che "*Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.*", sottolineando la portata non prescrittiva dei considerando e sottolineando come la disciplina relativa alle comunicazioni promozionali, essendo un'implementazione della Direttiva e-Privacy, costituisce *lex specialis*, che "specifica ed integra" quanto previsto dal GDPR.

2. Le limitate eccezioni alla regola del consenso per le comunicazioni commerciali

Come anticipato, il Codice Privacy prevede unicamente due eccezioni alla regola del consenso preventivo:

1 Linee guida in materia di attività promozionale e contrasto allo spam - 4… - Garante Privacy

- Numeri pubblici iscritti al registro delle opposizioni: Le operazioni di telemarketing svolte su numerazioni presenti in un elenco pubblico e non iscritte al registro pubblico delle opposizioni ("**RPO**"). Nonostante la Legge 5/2018 abbia esteso l'applicazione del RPO a tutte le numerazioni, fisse e mobili, rendendo la relativa consultazione un requisito indispensabile per qualsiasi operazione di telemarketing, l'ambito dell'eccezione al consenso rimane ristretto alle numerazioni presenti sugli elenchi, come ben chiarito dalle FAQ del RPO.

- Soft-spam a clienti già esistenti via email: In base al comma 4 dell'art. 130 del Codice Privacy, è lecito l'invio da parte del titolare del trattamento di email promozionali a utenti che non abbiano espresso il proprio dissenso ("*opt-out*") al momento della raccolta dei dati o successivamente, limitatamente a prodotti e servizi simili a quelli già acquistati. Tale eccezione, definita anche "*soft-spam*", valorizza il rapporto esistente tra titolari e interessati, in particolare, consentendo l'invio di comunicazioni in assenza di un consenso ("*opt-in*") preventivo. Tuttavia, come evidenziato dal Garante nel provvedimento doc. web 0020942 del 18 luglio 2023 nei confronti di Tiscali, tale eccezione va interpretata restrittivamente e non è suscettibile di applicazione analogica ad altre ipotesi di comunicazione commerciale, quale ad esempio marketing tramite SMS. In aggiunta, tale possibilità, secondo il Garante, non dovrebbe considerarsi (né indicarsi nelle informative privacy) come espressione del "legittimo interesse" del titolare, bensì come una norma "speciale" che non richiede un bilanciamento di interessi, in quanto lo stesso è già stato effettuato dal legislatore in sede di approvazione del comma 4 dell'art. 130 (provvedimento doc.web 9861941 dell'11 gennaio 2023)

3. La raccolta dei consensi per comunicazioni commerciali: gli errori principali da evitare

Così delineata la normativa applicabile, di seguito alcune indicazioni pratiche per evitare di incappare in alcune delle violazioni più comuni nel rispetto del principio di *accountability*:

I. Attenzione ai database di terzi e alla *supply chain*: L'attività di marketing, in particolare quando svolta telefonicamente, vede la partecipazione di molti e numerosi soggetti. Non è un caso che, infatti, i più recenti provvedimenti sanzionatori del Garante si concentrino proprio sulla cd. "supply chain" del telemarketing.

vedi l'articolo online

Il Garante ha già avuto modo di affermare che nell'affidarsi a terzi per attività eseguite per proprio conto è necessario effettuare opportune verifiche sulle effettività delle misure adottate per garantire la tutela della protezione dei dati personali. A tal proposito, vale la pena sottolineare come una mera verifica di qualità contrattuale non sarebbe sufficiente a sollevare la committente dai propri obblighi, essendo al contrario necessario un "privacy check" (provvedimento doc. web. 9893693 del 14 aprile 2023), alla luce dei principi di accountability e privacy by design, dal momento del primo contatto e fino alla sottoscrizione, adottando misure adeguate ad evitare il cd. "fenomeno dei procacciatori non ufficiali".

L'attenzione da parte del Garante al "sottobosco" di procacciatori ufficiali e non ufficiali e sub-committenti di terzi incaricati è tale che, in data 13 aprile 2023, l'autorità ha disposto la confisca di alcuni database detenuti da società, creati illegalmente senza consensi e informative, per utilizzi impropri volti a massimizzare provvigioni tramite attività di telemarketing "selvaggio", all'insaputa delle società i cui servizi erano promossi (provvedimento doc. web n. 9893718).

A ciò si aggiunga che la verifica delle attività della *supply chain* è necessaria anche alla luce della normativa regolamentare, ad esempio, con riferimento all'iscrizione al Registro degli Operatori di comunicazione, che è obbligatoria da parte dei soggetti terzi affidatari dei servizi di call center e deve essere contemplata nel contratto di affidamento del servizio.[2] Ancora, la normativa sul RPO prevede che, in caso di affidamento, il titolare del trattamento sia responsabile per violazioni nel caso di affidamento a terzi[3].

Ulteriore aspetto da tenere in considerazione è la verifica delle liste acquisite da banche dati di terzi che dovranno essere costitute unicamente da dati raccolti in conformità alla normativa sul trattamento dei dati, chiedendo ai partner di fornire documentazione comprovante la stessa e la base giuridica rilevante (si veda ad esempio il provvedimento del Garante doc. web. 9949453 del 12 ottobre 2023).

2 Art. 24-bis, comma 11 del Decreto Legge 83 del 2012, convertito con modificazioni dalla L. 7 agosto 2012, n. 134.
3 Legge 5 del 2018 art. 1 comma 11.

E' in ogni caso opportuno evidenziare che, come previsto dalla normativa amministrativa e come sottolineato recentemente dalla Corte di Giustizia dell'Unione Europa nelle decisioni C-683/21 e C-807/21 una "*sanzione amministrativa pecuniaria può essere inflitta (...) unicamente nel caso in cui sia accertato che il titolare del trattamento ha commesso, con dolo o colpa, una violazione*". Da questo punto di vista, la necessità di evitare forme di responsabilità *de facto* oggettiva si riflette in una corretta applicazione del principio di "accountability", secondo cui il titolare del trattamento risponde del rispetto della normativa a tutela dei dati personali in relazione ai trattamenti svolti direttamente o tramite terzi che agiscono sotto le sue istruzioni, adottando misure organizzative e di sicurezza adeguate.

II. I c.d. "*dark pattern*" nella raccolta del consenso: Un ulteriore aspetto da tenere in considerazione è la configurazione delle modalità di raccolta del consenso, al fine di evitare che si creino i c.d. *dark pattern*, ovvero quelle interfacce ed esperienze utente che inducono gli utenti a prendere decisioni involontarie, non volute e potenzialmente dannose in merito al trattamento dei loro dati personali. Il Comitato Europeo per la protezione dei dati (*European Data Protection Board*, "**EDPB**") nelle proprie linee guida relative ai dark pattern per i social media[4] ha individuato come principali categorie ingannevoli:

a. il sovraccarico di richieste/opzioni/possibilità;

b. la progettazione di interfacce che distraggano l'utente dalle scelte in materia di protezione dei dati (c.d. *skipping*);

c. il ricorso a meccanismi visivi o emotivi fuorvianti (c.d. *stirring*) e

d. l'ostacolo alla possibilità dell'utente di effettuare scelte o informarsi correttamente sul trattamento dei propri dati.

Non è inusuale che i *dark pattern* siano riscontrati nelle modalità di raccolta del consenso al

4 Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them | European Data Protection Board (europa.eu).

vedi l'articolo online

trattamento per marketing. Ad esempio, nel provvedimento doc. web 9870014 del 23 febbraio 2023 il Garante ha individuato come ingannevole la proposizione di un pop-up successivo alla mancata prestazione nel consenso che evidenziava la mancanza del consenso e presentava un tasto ben evidente per accettare il trattamento, mettendo in risalto l'opzione di accettazione rispetto a quella di rifiuto. In tale occasione, il Garante ha precisato che "*La proposizione del pop up non aveva alcuna utilità per lo svolgimento del processo di iscrizione ma rappresentava, evidentemente, un ulteriore tentativo di raccogliere il consenso dell'utente nonostante questi avesse già chiaramente espresso la sua volontà nella schermata precedente. Tale tentativo, oltre ad aggravare inutilmente il percorso di iscrizione, si caratterizzava per una maggiore opacità delle modalità con cui la richiesta di consenso veniva presentata aumentando le probabilità che l'interessato rilasciasse il proprio consenso non per scelta consapevole ma piuttosto perché indotto in errore o per la fretta di concludere il processo.*"

III. Tempi di conservazione: Alla luce del principio di limitazione dei tempi di conservazione di cui all'art 5. GDPR, i dati personali possono essere conservati fintantoché sia necessario alla luce delle finalità per cui sono stati raccolti in origine e successivamente trattati. Con riferimento specifico alle attività di marketing, anche successivamente all'entrata in vigore del GDPR, il Garante ha a più riprese (da ultimo nel provvedimento doc.web 9920942 del 18 luglio 2023) richiamato i termini di conservazione indicati nel provvedimento doc. web 21103045 del 24 Febbraio 2005 in materia di Fidelity card e garanzie per i consumatori che, nonostante la portata non più prescrittiva, è ancora il *benchmark* di riferimento per le tempistiche di conservazione dei dati per finalità di marketing e profilazione. In tale risalente provvedimento, il Garante aveva evidenziato come i dati relativi al dettaglio degli acquisti non possano essere conservati per finalità di profilazione o di marketing per un periodo non superiore, rispettivamente, a dodici e a ventiquattro mesi dalla loro registrazione. Rimane, tuttavia, parimenti applicabile, come orientamento di riferimento, la possibilità di derogare a tali stringenti limiti (fino ad un massimo di dieci anni) nel caso di offerte per beni di lusso, dove la frequenza media dell'acquisto è minore (provvedimenti, 24 aprile 2013, doc. web 2499354 e 30 maggio 2013, doc. web n.254783). In tali casi, tuttavia, è consigliabile lo svolgimento di una valutazione di impatto che documenti, in particolare, la proporzionalità del trattamento rispetto alle effettive esigenze del titolare, anche alla luce del settore merceologico in cui lo stesso opera. Più di recente (sempre nel provvedimento doc.web 9920942 del 18 luglio 2023), il Garante ha anche chiarito che, in ogni caso, è da ritenersi non congrua la conservazione dei dati relativi al marketing fino alla data della revoca del consenso al trattamento, anche considerato che l'interessato potrebbe anche non mutare mai la propria volontà o mantenerla invariata per anni. Allo scadere dei termini di conservazione, in assenza di una nuova manifestazione di consenso, i dati dovrebbero essere cancellati o anonimizzati (ad esempio, per poter continuare ad utilizzare statistiche sugli acquisti). Particolare attenzione va posta in questa fase all'effettiva anonimizzazione. Infatti, la conservazione di dataset separati (ad esempio, a scopi di possibile difesa da contenzioso) nella maggior parte dei casi comporta un rischio di re-identificazione che vanifica eventuali sforzi fatti in termini di aggregazione e randomizzazione.

IV. Specificità del consenso: La formulazione del linguaggio utilizzato nel modulo di consenso è un altro aspetto su cui occorre prestare particolare attenzione. L'art. 7 del GDPR ha, infatti, ribadito che il consenso deve essere prestato in forma specifica per potersi considerare valido. In particolare, nel caso di comunicazioni a terzi di dati personali per finalità di marketing (incluso nei confronti di società appartenenti allo stesso gruppo societario), è necessario prevedere un consenso specifico, accompagnato da adeguata informativa circa le categorie di destinatari dei dati (v. Linee Guida in materia di attività promozionale e contrasto allo spam di cui al provvedimento doc. web 2542348 del 4 luglio 2013). Tale consenso consentirà ai terzi di poter svolgere attività promozionale direttamente e senza acquisire un nuovo consenso (dando però opportuna informativa ai sensi dell'art. 14 GDPR, tra le altre cose, sull'origine e le categorie dei dati nonché sulla revoca dello stesso). La specificità del consenso non richiede, tuttavia, una moltiplicazione irragionevole dei consensi. In particolare, qualora la finalità sia unica, non sarà necessario chiedere consensi specifici per ogni attività, ma sarà sufficiente un consenso unico. Allo stesso tempo, purché l'informativa sia chiara, è accettabile la presentazione di un unico consenso per modalità "tradizionali" (es. chiamate con operatore) e "automatizzate".

4. AGCOM e il telemarketing

Come accennato in precedenza, la regolamentazione del marketing vede intersecarsi normative diverse, non solo specifiche sulla protezione dei dati personali. La disciplina sulle comunicazioni com-

merciali richiede l'analisi congiunta di diversi testi normativi, come il Codice del Consumo (D. Lgs. 206/2005), il Codice delle Comunicazioni elettroniche (D. Lgs 259/2003), la normativa di implementazione della Direttiva E-Commerce (D. Lgs. 70/2003).

In particolare, con riferimento al telemarketing, un ruolo di fondamentale importanza è assunto dall'Autorità per le Garanzie nelle Comunicazioni ("**AGCOM**"). Infatti, non solo tale autorità è dal 2016 incaricata della tenuta di una lista di operatori di call center e delle relative numerazioni utilizzate in un'apposita sezione del ROC, ma è anche deputata, ai sensi della L. 5/2018, all'individuazione delle misure relative alla identificazione della linea chiamante ("**CLI**").

Con Delibera 156/18/CIR, l'AGCOM ha individuato i prefissi 0843 e 0844 come identificativi delle chiamate telefoniche finalizzate, rispettivamente, ad attività statistiche e finalizzate al compimento di ricerche di mercato e ad attività di pubblicità, vendita e comunicazione commerciale. Ai sensi della stessa delibera, gli operatori che svolgono attività di call center per tali finalità possono utilizzare anche CLI diversi purché attivino un sistema IVR (*Interactive Voice Responder*), attivo 24 ore su 24, che fornisca all'utente le informazioni complete relative alla società chiamante (ragione sociale, sede legale) e che consenta di essere richiamati con richiesta dell'utente esplicitata attraverso la digitazione di un tasto specifico o tramite servizio di segreteria telefonica e con richiamata effettuata entro due giorni lavorativi dalla richiesta.

Di recente, inoltre, l'AGCOM ha adottato un codice di condotta ("**Codice di condotta**") per operatori di comunicazioni elettronica e call center (Delibera 197/23/CONS). Nonostante la limitata applicazione del predetto Codice di condotta e la volontarietà dell'adesione, i termini ivi stabiliti sono di particolare interesse, in quanto esemplificativi delle *best practice* che tutti i soggetti che effettuano telemarketing dovrebbero integrare, soprattutto nella gestione della *supply chain*.

Tra le altre, il Codice di condotta si concentra sulla definizione di regole di ingaggio dei call center prescrivendo la verifica preliminare dell'affidabilità del partner e dell'attività dello stesso. In particolare, gli operatori aderenti sono tenuti a prevedere nel contratto strumenti di verifica

- delle numerazione telefoniche utilizzate (che dovrebbero essere richiamabili e registrate al ROC),
- della durata del contatto,
- dell'esito,
- della numerazione di destinazione (che dovrebbe essere contenuta nelle liste fornite dall'operatore, ovvero acquisita nel rispetto della normativa in materia di protezione dei dati personali).

Il Codice di condotta, inoltre, richiede di inserire nei contratti un obbligo di preventiva autorizzazione in caso di cessione di liste, con impegno a monitorare il rispetto degli obblighi normativi da parte dei *sub-contractor* e a verificare la loro affidabilità. Tale previsione, invero, dovrebbe già scaturire dagli obblighi in materia di contrattualizzazione dei responsabili del trattamento ai sensi dell'art. 28 GDPR. Tuttavia, l'AGCOM va oltre quanto prescritto dalla normativa in materia di trattamento dei dati personali, sottolineando come il contratto con call center terzi dovrebbe limitare la sub-contrattualizzazione ad un unico livello, al fine di limitare la perdita di controllo sulla "*supply chain del telemarketing*".

L'adozione di pratiche illecite da parte dei terzi affidatari dovrebbe essere disincentivata assistendo gli obblighi con apposite penali economiche (in caso di violazioni poste in essere da questi o da sub-appaltatori) nonché da clausole risolutive espresse.

5. Il tema della profilazione e dei cookie

Ancora molto attuale è il tema legato ai cookie che, nel panorama digitale (su Internet, ma anche su *smart tv*, oggetti connessi quali assistenti vocali, etc.), sono il principale strumento per massimizzare le attività pubblicitarie sfruttando, in particolare, la profilazione e l'analisi comportamentale degli individui.

Le recenti linee guida dell'EDPB sull'Articolo 5(3) della Direttiva e-Privacy (Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive) hanno confermato l'interpretazione che già traspariva dalle linee guida sul cookie del Garante del giugno 2021 (provvedimento doc.web. 9677876 10 giugno 2021), dando un'interpretazione ampia dell'ambito di applicazione della disciplina dei cookie. In particolare, sono equiparati ai cookie gli URL e i pixel, strumenti utilizzati sovente per fini pubblicitari.

Tuttavia, molti temi rimangono ancora aperti. In particolare, rimane ancora non chiara la posizione del-

le autorità di controllo, Garante compreso, sulle soluzioni "*pay or consent*", oggi largamente utilizzate da quasi tutte le testate giornalistiche *online*. Secondo tale impostazione, vengono messi in campo sistemi e filtri che condizionano l'accesso a determinati contenuti online alla sottoscrizione di un abbonamento (il cosiddetto "paywall") o, in alternativa, al rilascio del consenso da parte degli utenti all'installazione di cookie e altri strumenti di tracciamento dei dati personali per finalità di profilazione.

A più di un anno dall'annuncio dell'apertura di un'istruttoria a riguardo, infatti, ancora manca una posizione del Garante.

Nel dicembre 2023, sul tema è intervenuta la Commissione evidenziando come il numero limitato di consumatori disposti a pagare per contenuti online e l'alto numero di siti web consultati giornalmente, renderebbero non "*credibile*" l'alternativa tra consenso al tracciamento e pagamento di una somma. Per questo motivo, la Commissione EU sembra aver suggerito una terza via, ovvero la possibilità di scegliere tra consenso alla pubblicità, pagamento e una soluzione meno invasiva per la privacy.

Nella risposta inviata alla commissione, l'EDPB sottolinea che il consenso non può essere considerato in ogni caso libero nei casi in cui la sua prestazione sia stata motivata da compulsione, pressione o incapacità di fare altrimenti. Per tale motivo, il Comitato Europeo per la protezione dei dati sottolinea come non sia possibile determinare in astratto la validità di un'alternativa "*pay or consent*", dovendosi esaminare, caso per caso, elementi quali il tipo di servizio offerto, le condizioni di scelta dell'utente e la presenza di altre modalità di pubblicità (come, ad esempio, la pubblicità contestuale).

Ancora, l'EDPB esprime perplessità sulla validità di consensi per cookie di pubblicità profilata che consentano la trasmissione a un largo numero di partner, esprimendo le proprie riserve a che questi tipi di trattamenti siano compatibili con i principi di necessità e proporzionalità. Si tratta di una valutazione particolarmente rilevante, considerato che la maggior parte dei siti che utilizzano cookie presenta, di norma, una lista di terze parti cospicua.

Anche l'attesa decisione sul sistema della "IAB Europe" relativa al *real time bidding* della pubblicità online profilata e della relativa piattaforma per la gestione del consenso potrebbe non essere dirimente, atteso che la decisione impugnata e la domanda pregiudiziale alla Corte Europea di Giustizia (C-640/22) della corte referente sono unicamente focalizzate sul GDPR e non sulla Direttiva e-Privacy.

6. GDPR e normativa e-privacy: problematiche e scenari futuri

La non sempre facile conciliazione tra GDPR e Direttiva e-Privacy deriva soprattutto da discordanze nella disciplina della *governance* e della giurisdizione applicabile tra tali normative.

Infatti, non sempre le autorità competenti per il monitoraggio della Direttiva e-Privacy sono le stesse adibite alla vigilanza e all'applicazione del GDPR. Non solo: laddove il GDPR disciplina scrupolosamente i meccanismi di cooperazione tra autorità (tramite il c.d. *one stop shop principle*), la Direttiva e-Privacy si limita ad incoraggiare la collaborazione tra le autorità di controllo degli Stati Membri. L'EDPB, nel proprio documento interno sulla competenza territoriale in materia di applicazione di norme nazionali di implementazione dell'art. 5(3) della Direttiva e-Privacy (Internal EDPB Document 4/2021) ha concluso che le autorità possono applicare i propri poteri quando il titolare o fornitore di servizi è stabilito nella loro giurisdizione, ovvero quando il trattamento è svolto nello stabilimento situato nella loro giurisdizione anche qualora la responsabilità in materia di raccolta e trattamento sia per tutto il territorio dell'Unione Europea in capo a un soggetto stabilito in un altro Stato Membro. Inoltre, l'EDPB ha aggiunto che ciascuna autorità dovrebbe limitarsi ad adottare misure che riguardino utente nella propria giurisdizione, senza impedire ad altre autorità di emanare misure relative al proprio territorio.

Tuttavia, tale conclusioni partono dall'assunto che il trattamento sia regolato esclusivamente da implementazioni della Direttiva e-Privacy. Tale scenario è di difficile individuazione, dal momento che, nelle opinione dell'EDPB circa il rapporto tra Direttiva e-Privacy e GDPR (Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities) è stato evidenziato come la validità del consenso debba misurarsi alla luce dei principi stabiliti nel GDPR.

La situazione è ancora più confusa in giurisdizioni come l'Italia che hanno implementato la Direttiva e-Privacy e GDPR congiuntamente (all'interno del Codice Privacy), adottando un apparato sanzionatorio omogeneo (quello stabilito dal GDPR). Da questo punto di vista, i provvedimenti del Garante sono chiari nel rinvenire, nella quasi totalità delle violazioni connesse al marketing, non solo un *breach* delle previsioni di settore, ma anche, più in generale, dei principi del GDPR.

La soluzione a queste problematiche sembra ancora lontana, considerato che l'approvazione di un re-

vedi l'articolo online

golamento e-Privacy con la legislatura europea in scadenza e l'attenzione sul regolamento per l'intelligenza artificiale non appare probabile o, quantomeno, prossimo.

Intanto, la tecnica sembra andare più veloce della normativa, dal momento che i maggiori player del settore pubblicitario online sembrano intenzionati ad andare verso un sistema *cookieless*, abbandonando le soluzioni di tracciamento di terze parti e proponendo soluzioni che attribuiscono agli utenti un maggiore controllo sui propri dati personali, diminuendo l'intrusività degli strumenti di profilazione. Una nuova era si apre per la pubblicità online. Riusciranno legislatori e autorità a stare al passo con l'evoluzione del mercato?

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it