ACCESSO E CONSERVAZIONE DEI DATI DI TRAFFICO TELEFONICO E TELEMATICO: SANZIONE DEL GARANTE PRIVACY PER 800 MILA EURO

Ordinanza-ingiunzione del Garante per la protezione dei dati personali n. 138 del 9 luglio 2020. Continua l'attività di controllo del Garante per la protezione dei dati personali nei confronti degli operatori telefonici anche a seguito delle centinaia di segnalazioni e reclami che settimanalmente pervengono all'Autorità per lamentare casi di "marketing selvaggio".
In particolare nella riunione del 9 luglio scorso il Garante ha preso in esame anche le risultanze degli accertamenti disposti nei confronti di un altro gestore telefonico, ILIAD, che è stato trovato carente sotto altri profili, in particolare in merito alle modalità di accesso dei propri dipendenti ai dati di traffico e che per tali ragioni, con ordinanza-ingiunzione n. 138 del 9 luglio 2020 ha disposto la sanzione pecuniaria di 800.000 euro.

di Michele IASELLI, avvocato, vicedirigente del Ministero della Difesa, docente a contratto di informatica giuridica presso l'Università di Cassino e collaboratore della cattedra di logica ed informatica giuridica dell'Università degli Studi di Napoli Federico II, della cattedra di informatica giuridica alla LUISS, Pres. dell'Associazione Nazionale per la Difesa della Privacy (ANDIP).

1. Le violazioni contestate

Il primo aspetto che il Garante nel proprio accertamento ispettivo ha esaminato è stato "l'accettazione contestuale delle condizioni contrattuali e dell'informativa privacy". In effetti l'Autorità ha avuto modo di accertare che la procedura che conduceva alla conferma dell'ordine prevedeva, una volta inseriti tutti i dati, l'obbligatoria spunta di una casella con la quale il soggetto dichiarava di aver preso visione e accettato le condizioni generali, la carta dei servizi, la brochure dei prezzi e l'informativa privacy di Iliad sul trattamento dei dati personali, tutti documenti facilmente raggiungibili mediante apposito link. In realtà i trattamenti elencati nell'informativa pubblicata sul sito web sono sia di natura facoltativa che obbligatoria e, in alcuni casi (trattamenti per finalità di marketing e profilazione) sono subordinati all'acquisizione di uno specifico consenso. **La summenzionata dichiarazione, al contrario, poteva indurre in confusione l'utente circa la necessità di prevedere per determinati trattamenti un consenso specifico**, libero ed informato come prescritto dall'art. 4 del GDPR e non certo un consenso generico.
La formulazione proposta nella schermata di conclusione del contratto risultava, quindi, inconferente richiedendo la "accettazione" dell'informativa e non solo la sua presa visione e tale richiesta era, per di più, formulata insieme alle conferme di carattere contrattuale. Come noto, l'informativa redatta dal titolare ha la funzione di rendere noto all'interessato ogni aspetto del trattamento dei dati personali; tale natura meramente esplicativa fa sì che il titolare, pur potendo pretendere dall'interessato di confermarne la presa visione, non possa tuttavia richiedere anche di esprimere, attraverso una generica e generale accettazione, una volontà che risulterebbe di fatto analoga ad un consenso.
Di conseguenza il trattamento non ha il carattere della chiarezza e dell'intelligibilità e, dunque, si pone in contrasto, in particolare, con i principi di correttezza e trasparenza espressi dall'art. 5, par. 1, lett. a) del Regolamento.Ad ogni modo a seguito di specifica contestazione la società ha predisposto le necessarie misure correttive per cui l'Autorità ha ritenuto, nello stesso provvedimento, non necessario adottare ulteriori misure.

Secondo aspetto che l'Autorità prende in considerazione è proprio "il consenso per finalità di marketing". Difatti, la Società, sulla base delle dichiarazioni rese, fino al luglio 2019 aveva richiesto agli interessati di prestare il proprio consenso al trattamento per finalità promozionali senza tuttavia tenere traccia di tale volontà. Ciò sarebbe avvenuto perché, come in un primo momento dichiarato a verbale, la Società non effettuava attività di marketing diretto ma anche, come successivamente sostenuto nella memoria difensiva, a causa di un bug presente nel sistema preposto alla registrazione dei consensi.
Sulla base, quindi, delle dichiarazioni rese, è evidente che la richiesta di un consenso per finalità promozionali, specificamente menzionate nell'informativa, senza che tale trattamento esista o sia previsto, **risulti in contrasto con il principio di correttezza e trasparenza** di cui all'art. 5, par. 1, lett. a), del Regolamento. Tuttavia, il Garante, preso atto dell'intenzione della Società, non menzionata nel corso dell'accertamento ispettivo, ma resa nota in sede difensiva, di voler effettivamente porre in essere un trattamento per finalità promozionali e tenuto conto degli interventi correttivi apportati, ha ritenuto di non adottare specifiche misure correttive.

Nell'ordinanza il Garante ha preso in esame anche "l'idoneità delle Simbox a garantire la riservatezza". Difatti, durante l'accertamento l'Autorità ha constatato che nel caso dell'attivazione della sim via web l'utente può scegliere se procedere subito all'identificazione tramite il sito oppure rimandare tale fase al momento della consegna della stessa scheda tramite corriere. Nel primo caso, viene richiesto, al termine della procedura, di allegare la copia del documento di riconoscimento registrando un breve video nel quale si dichiara di voler sottoscrivere il contratto; nel secondo caso, invece, l'identificazione dell'intestatario della sim viene fatta direttamente dal corriere, nominato responsabile del trattamento e appositamente istruito per tale procedura.
Se invece l'attivazione di una nuova sim viene effettuata tramite i canali fisici, la società ha predisposto delle apposite macchine, denominate "Simbox", con le quali i clienti possono effettuare l'acquisto in autonomia, inserendo i propri dati e terminando la procedura con la scansione del documento e la registrazione di un videomessaggio di assenso alla conclusione del contratto. **Il personale presente nei negozi ha solo funzione di assistenza ai clienti e non viene coinvolto nella procedura di attivazione dell'utenza.**

Le videoregistrazioni così effettuate sono visionate da operatori di back office che, effettuato un confronto con il documento caricato, concludono la procedura consentendo l'attivazione dell'utenza.
Le verifiche effettuate dall'Autorità simulando la sottoscrizione di un contratto tramite Simbox, hanno suscitato alcune perplessità in ordine alla riservatezza della procedura. Pertanto è stato contestato alla Società che un **simile trattamento può esporre gli interessati al rischio di accessi non autorizzati violando il principio di integrità e riservatezza** di cui all'art. 5, par. 1, lett. f) del Regolamento.
Ad ogni modo anche in questo caso a seguito delle misure correttive apportate dalla società il Garante ha ritenuto, ai sensi dell'art. 58, par. 2, lett. a), di dover solamente rivolgere alla Iliad un ammonimento in merito alle rilevate violazioni della riservatezza mediante l'uso della Simbox e di dover, di conseguenza, ingiungere alla stessa, ai sensi dell'art. 58, par. 2, lett. d), di adottare misure correttive idonee a garantire maggiore riservatezza agli interessati al momento dell'effettuazione della registrazione del video adottando specifici accorgimenti per il posizionamento delle macchine, collocandole in maniera tale da non poter consentire accessi indebiti alle informazioni (ad esempio in prossimità di una parete) o inserendo dei pannelli posteriori, ovvero prevedendo, distanze di cortesia ed integrando conseguentemente le istruzioni al personale addetto all'assistenza.

Il Garante nel proprio accertamento ispettivo ha dovuto anche considerare il "rispetto delle norme in materia di accesso e conservazione dei dati di traffico telefonico e telematico", argomento questo molto delicato. Difatti, a seguito di verifica dell'accesso al sistema CRM della società, sia con profilo di operatore sia con profilo di amministratore, per verificarne il contenuto, l'Autorità ha rilevato che **il profilo "amministratore del reparto di customer care" poteva visualizzare i dati di traffico telefonico degli utenti in chiaro accedendo al sistema mediante digitazione di userid e password. Inoltre, i dati accessibili erano relativi al traffico effettuato da agosto 2018.** È stato pertanto contestato alla società che tale procedura non poteva considerarsi conforme alle norme in materia di conservazione dei dati di traffico telefonico e telematico di cui agli art. 123, 132 e 132-ter del Codice e sulla base di quanto prescritto dal Garante con provvedimento generale del 17 gennaio 2018 poiché:
1. l'incaricato con profilo di amministratore essendo addetto alla funzione customer care, avrebbe potuto avere accesso solo ai dati conservati per finalità di fatturazione, ed invece **poteva visualizzare dati conservati per un periodo superiore ai sei mesi consentiti dall'art. 123 del Codice** (sono risultati presenti dati di traffico di agosto 2018 alla data di maggio 2019);
2. lo stesso ha avuto accesso al sistema contenente i dati di traffico digitando unicamente username e password, **senza pertanto utilizzare tecniche di strong authentication al momento dell'accertamento**.

Inoltre, in conseguenza di quanto accertato sopra, non risultava attuata la prescrizione di conservare le diverse tipologie di dati in sistemi informatici separati, dal momento che l'operatore, accedendo al sistema CRM, poteva visualizzare anche dati generati in un periodo eccedente i sei mesi.
Si ricorda che l'art. 132-ter impone ai fornitori di servizi di comunicazione elettronica di avvalersi, ai sensi dell'art. 32 del Regolamento, di misure tecniche e organizzative adeguate al rischio esistente. Tali misure, da considerarsi, allo stato dell'arte, quale requisito minimo di sicurezza generalmente utilizzato dagli operatori presenti sul mercato, sono in concreto identificabili con quanto prescritto dal Garante, in materia di conservazione dei dati di traffico, con provvedimento generale del 17 gennaio 2008 (come modificato dal successivo provvedimento del 24 luglio 2008), in base al quale:

- il trattamento dei dati di traffico telefonico e telematico da parte dei fornitori deve essere consentito solo ad incaricati specificamente autorizzati e unicamente sulla base del preventivo utilizzo di specifici sistemi di autenticazione informatica basati su tecniche di strong authentication; per i dati di traffico conservati per esclusive finalità di accertamento e repressione dei reati, una di tali tecnologie deve essere basata sull'elaborazione di caratteristiche biometriche dell'incaricato;
- i sistemi informatici utilizzati per i trattamenti di dati di traffico conservati per esclusiva finalità di giustizia devono essere differenti da quelli utilizzati anche per altre funzioni aziendali (come fatturazione, marketing, antifrode); è tuttavia ammissibile un primo periodo, di 6 mesi dalla generazione, durante il quale i dati possono essere trattati con sistemi

informatici non esclusivamente riservati alle finalità di giustizia.

Inoltre, va rilevato che alla luce del nuovo quadro normativo costituito dal Regolamento e dal Codice, si deve ritenere che le specifiche prescrizioni del provvedimento del Garante del 17 gennaio 2008 siano da considerare alla stregua delle basilari misure di sicurezza del trattamento applicabili ai fornitori di servizi di comunicazione elettronica. Il mancato rispetto di tali prescrizioni deve considerarsi equivalente alla mancanza di misure tecniche e organizzative adeguate al rischio esistente e, di conseguenza, integra la violazione dell'art. 132-ter del Codice.
In merito a tale comportamento di Iliad, l'Autorità ha ritenuto che gli elementi acquisiti possono configurare delle violazioni ed ha pertanto avviato il procedimento di cui all'art. 166, comma 5 del Codice. A fronte delle puntuali contestazioni ricevute, **la Società ha presentato una memoria di 22 pagine** ed è anche stata ascoltata in una successiva audizione, ma, in questo caso, le osservazioni fornite non hanno soddisfatto il Garante che, ai sensi dell'art. 58, par. 2, lett. d) del Regolamento, ha ritenuto di ingiungere ad Iliad di adeguare le misure di sicurezza poste a tutela dei dati di traffico conformandole a quanto prescritto dal Garante con il provvedimento del 17 gennaio 2008 come modificato dal provvedimento del 24 luglio 2008. Inoltre, tenuto conto che le contestazioni rivolte alla Società non si sono dimostrate sufficienti a sollecitare un intervento correttivo da parte di quest'ultima, ha ritenuto di dover adottare nei confronti della stessa Società un'ordinanza ingiunzione, ai sensi degli artt. 58, par. 2, lett. i), del Regolamento, 166, comma 7, del Codice e 18 della legge n. 689/1981, per l'applicazione delle sanzioni amministrative pecuniarie previste dall'art. 83, parr. 4 e 5, del Regolamento.

2. La sanzione applicata

Ai fini della quantificazione della sanzione amministrativa, per le violazioni di cui a quest'ultimo punto il citato art. 83, par. 5, nel fissare il massimo edittale nella **somma di 20 milioni di euro ovvero, per le imprese, nel 4% del fatturato mondiale annuo dell'esercizio precedente** ove superiore, specifica le modalità di quantificazione della predetta sanzione, che deve "in ogni caso essere effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento (UE) 2016/679), individuando, a tal fine, una serie di elementi, elencati al par. 2, da valutare all'atto di quantificarne il relativo importo.

In una complessiva ottica di necessario bilanciamento fra diritti degli interessati e libertà di impresa, tenuto conto da un lato in chiave aggravante:
- dell'ampia portata dei trattamenti riguardanti la conservazione dei dati di traffico dei clienti del servizio di telefonia mobile di Iliad;
- della gravità delle violazioni rilevate;
- del grado di responsabilità del titolare del trattamento, tenuto conto che le misure tecniche e organizzative descritte non sono risultate adeguate allo stato dell'arte;
- del generale approccio tenuto da Iliad nel trattamento dei dati personali (art. 83, par. 2, lett. d) del Regolamento), considerato che, oltre quanto evidenziato al punto precedente, pure le violazioni descritte ai punti precedenti pur se considerate di carattere minore, hanno comunque mostrato **un quadro complessivamente negligente nell'applicazione, sin dalla progettazione, di misure di tutela degli interessati**;
- del grado di cooperazione con l'Autorità di controllo, dal momento che **Iliad si è limitata a ritenere infondate le violazioni contestate, sostenendo le proprie ragioni con argomentazioni spesso non pertinenti** con quanto accertato;
- della maniera in cui l'Autorità di controllo ha preso conoscenza della violazione, emersa nel corso di un'attività ispettiva (art. 83, par. 2, lett. h) del Regolamento);

il Garante ha irrogato la sanzione amministrativa del pagamento di una somma pari al 4% della sanzione edittale massima di 20 milioni di euro, corrispondente a euro 800.000,00.

Dall'esame, quindi, del provvedimento del Garante è evidente che è stato proprio il mancato rispetto delle norme in materia di accesso e conservazione dei dati di traffico telefonico e telematico ad indurre l'Autorità alla irrogazione della sanzione pecuniaria poiché in tal caso alla luce anche della nuova situazione normativa determinatasi a seguito del GDPR e di quanto prescritto dall'art. 32 dello stesso Regolamento è configurabile una reale mancanza di misure tecniche e organizzative adeguate al rischio esistente.
Negli altri casi il Garante ha ritenuto sufficienti singoli ammonimenti ai sensi dell'art. 58, par. 2, lett. a), del GDPR. ©