LS NEWSLETTER

a cura di LS Lexjus Sinacta

dipartimento IT & Data Protection

Contributi & Approfondimenti

- Regolamento ePrivacy: approvato il testo dal Consiglio dell'Unione Europea

Il Consiglio dell'Unione Europea ha finalmente raggiunto un accordo sulla versione finale del testo di Regolamento ePrivacy ed ha approvato un mandato per dare avvio alle negoziazioni con il Parlamento Europeo per la revisione definitiva delle norme in materia di tutela della vita privata e della riservatezza nell'uso dei servizi di comunicazione elettronica.

Il nuovo testo di legge troverà applicazione non solo con riferimento ai fornitori di servizi di comunicazione elettronica tradizionali, come gli operatori di telefonia mobile e fissa, ma introdurrà importanti cambiamenti nei settori fondamentali dell'economia digitale, come l'IoT e l'online advertising, con impatti su tutte le organizzazioni attive nel settore digital, dalle web company, alle società di telecomunicazioni, ai social network, agli sviluppatori di software e app.

Di seguito i contenuti principali del testo del Regolamento ePrivacy.

1. L'applicazione del Regolamento ePrivacy sarà estesa a **tutti gli utenti situati all'interno dell'Unione Europea**, e ciò anche nel caso in cui il fornitore dei servizi si trovi al di fuori dall'Unione Europea e/o il trattamento avvenga al di fuori dell'Unione Europea (in conformità a quanto già previsto per il GDPR).
2. Si prevede l'obbligo di ottenere il **consenso esplicito degli utenti finali** per l'installazione di cookie, tracker o qualsiasi altra tecnologia che memorizzi dati personali sulle apparecchiature terminali degli utenti, introducendo inoltre **l'obbligo della verifica periodica di tale consenso**, mediante un avviso che ricordati la possibilità di ritirare il consenso **a intervalli periodici di non più di 12 mesi**, finché il trattamento continua, a meno che l'utente finale non chieda di non ricevere tali avvisi.
3. Si prevede la possibilità (ma non l'obbligo) per i fornitori di software di **includere di default impostazioni che consentano agli utenti finali**, in maniera agevole e trasparente, **di gestire il consenso ai cookie**, effettuando scelte precise in merito all'archiviazione e all'accesso ai dati memorizzati nelle loro apparecchiature terminali, impostando e modificando facilmente delle **white-list per la categorie di cookie accettate o meno**, in modo da avere un controllo facilmente esercitabile del consenso e porre fine alla c.d. "*cookie fatigue*".
4. Si mantiene la possibilità di ricorrere al c.d. "*cookie wall*", e quindi di **condizionare l'accesso ai siti web alla prestazione del consenso all'installazione dei cookie** da parte dell'utente, a condizione che ciò "*non privi l'utente di una facoltà di scelta effettiva*"; tale condizione si ritiene verificata se l'utente finale viene posto in grado di **scegliere consapevolmente tra un'offerta di servizio** che include il consenso all'uso dei cookie per finalità aggiuntive, da un lato, **e un'offerta equivalente** dello stesso fornitore che non comporta il consenso all'uso dei dati per finalità aggiuntive.
5. Si mantiene la possibilità **di inviare comunicazioni di marketing in base alla c.d. "*eccezione soft spam*"** e si **estende la definizione di messaggio elettronico**: non solo email ma anche **qualsiasi messaggio** contenente informazioni quali testo, voce, video, suono o immagine **inviato su una rete di comunicazione elettronica che può essere memorizzato nella rete o in strutture informatiche correlate, o nell'apparecchiatura terminale del suo destinatario**, compresi SMS, MMS e applicazioni e tecniche funzionalmente equivalenti. Inoltre, si ammette la possibilità che il destinatario della comunicazione a fini marketing sia un utente coinvolto in una qualsiasi precedente transazione.
6. Si prevede la possibilità di **elaborare i metadati per finalità ulteriori e compatibili con quelle per cui sono stati originariamente raccolti** (è tuttavia necessaria l'esecuzione di una apposita valutazione e l'adozione di specifiche misure di sicurezza). Si prevede la possibilità di trattare i metadati, oltre che in base al consenso, se tale trattamento è necessario ai fini della gestione della rete o dell'ottimizzazione della rete, o per soddisfare i requisiti tecnici di qualità del servizio, o per l'esecuzione di un contratto di servizio di comunicazione elettronica di cui l'utente finale è parte, o se necessario per la fatturazione, il calcolo dei pagamenti

di interconnessione, l'individuazione o la cessazione dell'uso fraudolento o abusivo dei servizi di comunicazione elettronica o dell'abbonamento a tali servizi.

- Brexit: le istituzioni europee hanno avviato l'iter per l'adozione della decisione di adeguatezza nei confronti del Regno Unito

Il 1° gennaio 2021 il Regno Unito ha lasciato definitivamente l'Unione Europea diventando Paese terzo anche ai fini della normativa in materia di privacy. L'Accordo Commerciale e di Cooperazione stipulato il 30 dicembre 2020 ("Accordo") prevede, tra le altre cose, che il Regno Unito continui ad applicare il GDPR fino al 30 giugno 2021. Di conseguenza, in tale periodo transitorio qualsiasi comunicazione di dati personali verso il Regno Unito non sarà considerata un trasferimento di dati verso un Paese terzo.

Indipendentemente dal suddetto periodo transitorio, i titolari e i responsabili del trattamento con sede nel Regno Unito che siano soggetti all'applicazione del GDPR, sono tenuti a designare un "Rappresentante" nell'Unione Europea a norma dell'articolo 27 del GDPR, che possa essere contattato dalle Autorità di controllo e dalle persone interessate per qualsiasi questione relativa alle attività di trattamento dei dati personali.

Sulla base dell'Accordo, **l'Unione Europea e il Regno Unito si sono impegnati a lavorare su reciproche decisioni di adeguatezza** che consentano di proseguire i flussi di dati senza interruzioni, anche a seguito della scadenza del suddetto periodo transitorio. **A febbraio 2021 la Commissione Europea ha approvato il proprio progetto di decisione** in merito all'adeguata protezione dei dati personali da parte del Regno Unito ed ha avviato la procedura per la sua adozione formale.

Ad aprile 2021 l'European Data Protection Board ("EDPB") ha emesso un parere favorevole sulla suddetta decisione di adeguatezza relativa al Regno Unito, ma ha anche **sollevato delle preoccupazioni**. In particolare, l'EDPB ha richiamato l'attenzione sul rischio che il Regno Unito diventi la porta di accesso per il trasferimento indiscriminato di dati personali in tutto il mondo, aggirando in questo modo le tutele previste dal GDPR, specialmente alla luce della sentenza Scherms II.

Nel proprio parere l'EDPB ha enunciato le seguenti considerazioni:

1. la normativa sulla protezione dei dati personali del Regno Unito è attualmente in linea con il GDPR. Tuttavia, in considerazione della intenzione dichiarata dal governo britannico di voler sviluppare politiche indipendenti sul trattamento dei dati personali, **la Commissione Europea dovrà monitorare lo sviluppo della situazione** ed essere pronta a modificare/sospendere la decisione di adeguatezza;
2. i **trasferimenti di dati personali che originano dall'UE e transitano dal Regno Unito verso Paesi terzi** devono essere consentiti solo se viene **assicurato un livello di protezione essenzialmente equivalente a quello previsto dal GDPR**;
3. le eventuali decisioni di adeguatezza emanate dall'UE o dal Regno Unito in relazione a Paesi Terzi non devono essere oggetto di **alcun riconoscimento di adeguatezza reciproco**;
4. gli **accordi internazionali tra il Regno Unito e i Paesi terzi** (ad es. gli Stati Uniti) **devono essere monitorati** in quanto potrebbero innescare trasferimenti successivi rischiosi.

A maggio 2021 il Parlamento Europeo ha adottato una risoluzione che esorta la Commissione Europea a rivedere i suoi progetti di decisioni di adeguatezza rispetto al Regno Unito. Ciò rende difficile ritenere che sarà raggiunto l'obiettivo di adottare la decisione di adeguatezza entro il 30 giugno 2021 (quando terminerà il periodo transitorio previsto dall'Accordo).

Se così fosse, nell'attesa dell'adozione della decisione di adeguatezza, le aziende dovranno eseguire anche in relazione al Regno Unito una valutazione di adeguatezza secondo i criteri stabiliti nelle

Raccomandazioni dell'EDPB - adottate a seguito della pronuncia della sentenza Scherms II – per valutare il trasferimento di dati nei confronti di Paesi Extra-UE.

- ## Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale.

Il 21 aprile la Commissione europea ha presentato la Proposta di Regolamento volta a delineare il primo quadro giuridico in assoluto sull' Intelligenza Artificiale. Tale intervento mira a porre l'Europa in una posizione di leader a livello globale per lo sviluppo di un'intelligenza artificiale che sia affidabile.

Tra gli elementi principali della Proposta si evidenzia:

(i) il *risk based approach* che si concretizza nella previsione di tre diversi livelli di rischio a cui l'uso delle IA può portare: un rischio inaccettabile; un rischio alto; un rischio basso o minimo.
(ii) La previsione di precisi obblighi di trasparenza per determinati sistemi di IA volti a tenere conto dei rischi specifici di manipolazione che tali sistemi comportano.
(iii) Il perseguimento dell'obiettivo di creare un quadro giuridico favorevole all'innovazione, incoraggiando le autorità nazionali competenti a creare spazi di sperimentazione normativa e la definizione di un quadro di base in termini di governance, controllo e responsabilità.
(iv) L'istituzione di sistemi di governance sia a livello di Unione europea sia a livello nazionale.
(v) La definizione di un quadro per la creazione di codici di condotta volto ad incoraggiare i fornitori di sistemi di IA non ad alto rischio ad applicare volontariamente i requisiti obbligatori previsti per i sistemi di IA ad alto rischio.

Giurisprudenza & Provvedimenti del Garante

- ## Provvedimento di avvertimento in merito ai trattamenti effettuati relativamente alla certificazione per Covid-19 (prevista dal d.l. n. 52 del 22 aprile 2021) del 23 aprile 2021 [doc. web. 9578184]

La norma appena approvata per la creazione e gestione delle "certificazioni verdi" (c.d. *Green Pass*) secondo il Garante presenta criticità per i diritti e le libertà dei soggetti interessati, in particolare:

(i) Lo strumento del Decreto Legge non viene ritenuto **base giuridica** idonea all'introduzione e all'utilizzo del *Green Pass*.
(ii) La mancata indicazione delle finalità del trattamento rischia di rendere sproporzionato lo strumento del *Green Pass* rispetto al pur importante interesse pubblico perseguito ossia quello della tutela della salute pubblica, ponendosi quindi in contrasto con il principio di **trasparenza** al pari della mancata indicazione del titolare del trattamento.
(iii) Viene contestato l'utilizzo – previsto dalla previsione transitoria, in attesa del decreto attuativo – delle certificazioni di guarigione rilasciate prima dell'entrata in vigore del Decreto Legge e le certificazioni verdi redatte sulla base dell'allegato 1 del predetto decreto legge.
(iv) La quantità di informazioni richieste per l'attivazione del *Green Pass* sembrerebbe porsi in contrasto con il principio di **minimizzazione.**
(v) Non è stata prevista alcuna *policy* in materia di ***retention*** dei dati ponendosi quindi in contrasto con i principi di **limitazione della conservazione e di integrità e riservatezza**.

- **La Corte di Cassazione con ordinanza n. 11019/2021 respinge il ricorso di Telecom contro il Garante per la Protezione dei Dati Personali e conferma il divieto di recupero del consenso dei dati personali.**

La Suprema Corte si è pronunciata in merito alla corretta applicazione delle norme del codice privacy relative alle “comunicazioni commerciali o promozionali”. Il caso di specie aveva ad oggetto la campagna "di contatto", denominata "recupero consenso", attuata da Telecom allo scopo di acquisire il consenso degli interessati ad essere contattati per attività di marketing.

Con l’ordinanza di rigetto, i Giudici hanno sottolineato come una comunicazione telefonica finalizzata ad ottenere il consenso per fini di marketing, da chi l'abbia precedentemente negato, sia essa stessa una "comunicazione commerciale". Infatti, occorre guardare alla finalità della comunicazione e, pertanto, qualora questa sia promuovere attività di marketing, la richiesta del consenso diventa a sua volta un trattamento dei dati a fini commerciali.

Non è, dunque, possibile recuperare legittimamente il consenso precedentemente negato o non prestato per il tramite di una campagna telefonica. La revoca del dissenso deve avvenire liberamente e volontariamente.

PER MAGGIORI INFORMAZIONI:

Lorenzo Bianchi
l.bianchi@lslex.com

Filomena Zonno
f.zonno@lslex.com