ItaliaOggi
QUOTIDIANO ECONOMICO, GIURIDICO E POLITICO

News
06/02/2024 11:16

DIRITTO E FISCO

Intercettazioni, Garante privacy: più tutele per i dati nelle infrastrutture centralizzate

L'Autorità dice no alla cancellazione di un articolo dall'archivio di un quotidiano. Quattro Comuni sanzionati in materia di protezione dati. Varato un documento di indirizzo sulle tutele per le mail dei dipendenti

Via libera del **Garante Privacy** allo schema di decreto del **ministero della Giustizia** riguardante i requisiti tecnici per la gestione dei dati personali raccolti dalle infrastrutture digitali centralizzate per le intercettazioni. L'Autorità ha però chiesto che venissero implementate ulteriori misure a tutela delle persone coinvolte nelle attività di captazione. Le infrastrutture digitali centralizzate o "interdistrettuali" sono state istituite nell'agosto scorso e sono destinate non solo a ospitare il relativo archivio, ma anche a consentire la realizzazione delle operazioni captative. La loro creazione - pur conservando in capo al Procuratore l'autonoma direzione (e quindi anche la responsabilità) delle operazioni - mira ad assicurare, in particolare, più elevati e uniformi livelli di sicurezza ed efficienza nelle attività di intercettazione. Lo schema dell'odierno decreto attuativo sottoposto al Garante definisce dunque i requisiti per la memorizzazione e la trasmissione da parte della Polizia giudiziaria al Pubblico ministero di registrazioni e verbali, al fine di assicurarne l'autenticità, l'integrità e la riservatezza. Considerata la rilevanza quantitativa e qualitativa delle informazioni personali trattate, nel dare il proprio parere favorevole il Garante ha però indicato alcune misure tecniche ed organizzative che dovranno essere integrate per rafforzare le garanzie di sicurezza e trasparenza.

In particolare le norme dovranno prevedere procedure di autenticazione a più fattori per l'accesso alle infrastrutture digitali, meccanismi di tracciamento delle operazioni effettuate e alert per segnalare eventuali anomalie. Tali misure dovranno essere riesaminate e aggiornate periodicamente, sulla base di una valutazione di impatto che il Ministero della Giustizia dovrà trasmettere al Garante, in modo da garantire un livello di sicurezza adeguato ai potenziali rischi.Il decreto dovrà anche specificare il ruolo assunto dal Ministero della Giustizia in merito alla gestione e manutenzione dei sistemi di collegamento digitale e alla definizione dei profili di autorizzazione per accedere all'archivio delle intercettazioni.

No a cancellazione di un articolo dall'archivio online di un quotidiano

L'archivio online di un giornale svolge un'importante funzione per la ricostruzione storica degli eventi che si sono verificati nel tempo. Lo ha ricordato il Garante privacy nel ritenere infondato il reclamo di una donna che si era rivolta all'Autorità per far cancellare i propri dati personali da un articolo conservato nell'archivio online di un editore di un quotidiano nazionale. La donna riteneva che le informazioni contenute nell'articolo le recassero pregiudizio e non fossero più attuali dal momento che riguardavano una vicenda giudiziaria per la quale era stata condannata nel 2009, peraltro senza riportare i successivi sviluppi. L'interessata aveva infatti scontato, nel frattempo, la pena detentiva di quattro anni cui era stata condannata. Il Garante ha rigettato il reclamo spiegando che la conservazione dell'articolo all'interno dell'archivio online dell'editore risponde ad una legittima finalità di archiviazione di interesse storico-documentaristico che, pur differente da quella originaria di cronaca giornalistica, è anch'essa prevista dal Regolamento europeo che stabilisce specifici limiti al potere di esercitare il diritto di cancellazione. Tuttavia, non sussistendo ragioni di interesse pubblico che giustifichino una perdurante reperibilità dell'articolo, l'Autorità ha ingiunto all'editore di adottare misure tecniche idonee ad inibire l'indicizzazione dell'articolo da parte di motori di ricerca esterni al sito del quotidiano. Ciò in quanto la deindicizzazione disposta solo da un motore di ricerca, come era avvenuto nel caso in esame, ha il solo effetto di dissociare il nome dell'interessata dall'URL collegato all'articolo, il quale resta comunque reperibile utilizzando chiavi di ricerca diverse.

Responsabile protezione dati, 4 Comuni sanzionati

Al via una nuova serie di controlli su una vasta platea di enti locali. Con l'adozione di quattro provvedimenti sanzionatori nei confronti di enti locali, il Garante Privacy ha concluso la prima fase dell'indagine avviata per verificare il rispetto dell'obbligo di comunicazione all'Autorità dei dati di contatto del Responsabile della protezione dei dati (**RPD**,

o **Data protection officer**, **DPO**). Ed è già al via una nuova serie di controlli indirizzati ad una platea ancora più ampia di Comuni che non hanno comunicato all'Autorità i dati di contatto del RPD. Rilevata la violazione per la mancata comunicazione del RPD il Garante ha comminato a tre enti locali una sanzione di 2.000 euro ciascuno, mentre al quarto ha applicato una sanzione di 5.000 euro, maggiorata poiché l'inadempimento ha riguardato la nomina di due RPD. In tutti i provvedimenti sanzionatori il Garante ha ricordato che, per essere in linea con il Regolamento Ue, se il titolare del trattamento dei dati personali è un soggetto pubblico, quali, ad esempio, amministrazioni dello Stato, Regioni, Province, Comuni, università, aziende del Servizio sanitario nazionale, è obbligato a designare un RPD e a comunicarne i dati di contatto al Garante privacy, attraverso l'apposita procedura messa a disposizione dall'Autorità sul suo sito. L'obbligo della comunicazione, previsto nel Regolamento Ue, mira a garantire la possibilità per l'Autorità di garanzia di contattare in modo facile e diretto il RPD, figura che ha tra i suoi compiti anche quello di fungere da punto di riferimento fra il titolare (o responsabile) del trattamento e l'Autorità stessa.

Lavoro: dal Garante nuove tutele per la email dei dipendenti

Varato un documento di indirizzo sulla conservazione dei **metadati**. I datori di lavoro pubblici e privati che per la gestione della posta elettronica utilizzano programmi forniti anche in modalità cloud da oggi hanno a disposizione nuove indicazioni utili a prevenire trattamenti di dati in contrasto con la disciplina sulla protezione dei dati e le norme che tutelano la libertà e la dignità dei lavoratori. Il Garante per la protezione dei dati personali ha infatti adottato un documento di indirizzo denominato "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" rivolto ai datori di lavoro pubblici e privati. Il documento nasce a seguito di accertamenti effettuati dall'Autorità dai quali è emerso che alcuni programmi e servizi informatici per la gestione della posta elettronica, commercializzati da fornitori anche in modalità cloud, sono configurati in modo da raccogliere e conservare - per impostazione predefinita, in modo preventivo e generalizzato - i metadati relativi all'utilizzo degli account di posta elettronica dei dipendenti (ad esempio, giorno, ora, mittente, destinatario, oggetto e dimensione dell'**e-mail**). In alcuni casi è emerso anche che i sistemi non consentono ai datori di lavoro di disabilitare la raccolta sistematica dei dati e ridurre il periodo di conservazione.

Con il documento il Garante chiede quindi ai datori di lavoro di verificare che i programmi e i servizi informatici di gestione della posta elettronica in uso ai dipendenti (specialmente in caso di prodotti di mercato forniti in **cloud** o **as-a-service**) consentano di modificare le impostazioni di base, impedendo la raccolta dei metadati o limitando il loro periodo di conservazione ad un massimo di 7 giorni, estensibili, in presenza di comprovate esigenze, di ulteriori 48 ore. Periodo considerato congruo, sotto il profilo prettamente tecnico, per assicurare il regolare funzionamento della posta elettronica in uso al lavoratore. I datori di lavoro che per esigenze organizzative e produttive o di tutela del patrimonio anche informativo del titolare (in particolare, ad esempio, per specifiche esigenze di sicurezza dei sistemi) avessero necessità di trattare i metadati per un periodo di tempo più esteso, dovranno espletare le procedure di garanzia previste dallo Statuto dei lavoratori (accordo sindacale o autorizzazione dell'ispettorato del lavoro). L'estensione del periodo di conservazione oltre l'arco temporale fissato dal Garante può infatti comportare un indiretto controllo a distanza dell'attività del lavoratore.

ItaliaOggi copyright - 2024. Tutti i diritti riservati

Le informazioni sono fornite ad uso personale e puramente informativo. Ne è vietata la commercializzazione e redistribuzione con qualsiasi mezzo secondo i termini delle condizioni generali di utilizzo del sito e secondo le leggi sul diritto d'autore. Per utilizzi diversi da quelli qui previsti vi preghiamo di contattare mfhelp@class.it

Stampa la pagina