Al Garante per la protezione dei dati personali

protocollo@gpdp.it

Oggetto: contributo consultazione sul provvedimento dei metadati

In riferimento alla consultazione on line promossa dalla vostra Autorità https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9987602, la nostra associazione è lieta di contribuire, come per le precedenti consultazioni in materia di dati biometrici e di cookie, al fine di consentirne una migliore efficacia nei confronti dei destinatari e degli ulteriori attori chiave

Definire i metadati in funzione del ruolo ricoperto

Il presente provvedimento, da come risulta nell'introduzione, si pone lo scopo di regolamentare *"metadati relativi all'utilizzo degli account di posta elettronica in uso ai dipendenti"* in

quanto dati riconducibili a persone identificate o identificabili, appartenenti ad una categoria da ritenersi vulnerabile, a causa del rapporto di lavoro, e potenziale di un controllo sistematico.

Il documento cita quale esempio i metadati inerenti giorno, ora, mittente, destinatario, oggetto e dimensione email, ma esistendo ulteriori tipologie di metadati, appare indispensabile che la questione venga affrontata facendo particolare attenzione alla problematica tecnica e al ruolo che hanno i grandi provider di posta elettronica. La risoluzione e regolamentazione delle questioni tecniche appare propedeutica a quelle giuridiche, in quanto:

- I metadati oggetto del provvedimento sono parte integrante del messaggio di posta elettronica, e vengono utilizzati dai client di posta ***anche*** per la loro corretta gestione operativa, quali la sottoposizione al programma o alla web app di una query di ricerca, per data, ora, mittente, destinatario, oggetto, presenza o meno di un allegato). La cancellazione di tali elementi in un così breve termine potrebbe comportare problemi di efficienza organizzativa dovuta alla necessità di aumentare i tempi-lavoro legati alla ricerca dei messaggi (altrimenti non ricercabili). Sempre all'interno dell'organizzazione del lavoro, tali metadati vengono inoltre utilizzati per la corretta gestione operativa di archiviazione; i client permettono – tramite i metadati – di creare cartelle, sotto cartelle, condivise o meno, e protette o meno da password, ecc.
- Sono i provider a sapere quali siano i metadati che producono, e che trattano. Sia quando ricoprono il ruolo di Titolare del trattamento, sia quando ricoprono quello del Responsabile ai sensi dell'articolo 28 del GDPR. *Questi ultimi dovrebbero avere l'obbligo* (da specificare nei contratti stipulati con i clienti) *di indicare quali di questi*

siano indispensabili, quali facoltativi per il funzionamento dei servizi, quali strumenti di configurazione e di amministrazione rendano disponibili agli utilizzatori, e quali siano i relativi tempi di conservazione necessari, consigliati, o altro.

- I metadati oggetto del provvedimento fanno parte dei log dei sistemi. Questi ultimi appaiono particolarmente indispensabili per la cybersecurity; *cancellarl*i (tutti, e sempre che l'applicativo del gestore lo consenta) *dopo un massimo di 168 ore potrebbe comportare – a fronte della tutela del lavoratore – un aumento della vulnerabilità del perimetro informatico per tutte quelle aziende che utilizzano i metadati come strumento per riscontrare la presenza di un accesso non autorizzato e poter ricostruire la portata di uno o più incidenti avvenuti.* In questo ambito di sicurezza cibernetica, bisognerebbe inoltre tener conto di quanto previsto dalle direttive NIS, e appare ritenere congruo un periodo di conservazione di almeno sei mesi.
- La Riforma della Data Retention non risulta avere intaccato la possibilità per il fornitore di conservare, per finalità di accertamento e repressione dei reati, dati di traffico telefonico e telematico, nonché dati relativi alle chiamate senza risposta, anche fino a 6 anni dalla comunicazione, così come previsto dalla Legge 167/2017 (Legge Europea 2017), all'art. 24, che aveva esteso i tempi di retention previsti dal Codice Privacy.
- Appare di fondamentale importanza *stabilire e disciplinare quali debbano essere le modalità di conservazione dei log che assicurino la sicurezza* ed impediscano l'accesso indebito agli stessi e l'utilizzo da parte di estranei non autorizzati (quali ad esempio la cifratura). Su tali aspetti che attengono in maniera specifica ai requisiti che dovrebbero possedere i provider, sarebbe opportuno che venissero date ***precise prescrizioni ai provider*** dal momento che - per talune operazioni - essi dovrebbero essere considerati quali **titolari autonomi del**

trattamento quali gestori di servizi di telecomunicazione con conseguente applicazione della disciplina prevista (Capo I del Titolo X Codice Privacy e Direttiva e-Privacy). Al riguardo, *si chiede di chiarire se è necessario che sia il Titolare del trattamento dei dati relativi ai dipendenti che utilizzano gli account aziendali dare precise istruzioni al provider (Responsabile) affinchè non utilizzi i log, li tenga in maniera protetta e sicura (cifratura) e li restituisca al termine del servizio o se, invece, si tratti di prescrizioni generali che potrebbero essere date direttamente dal Garante.*

- Nel caso del **settore pubblico**, inoltre, appare importante che vengano richiamati all'interno delle gare effettuate dalla CONSIP indicazioni e requisiti che deriveranno dai provvedimenti successivi alla presente consultazione pubblica, per prevenire che le P.A. facciano affidamenti non conformi. Inoltre, *dovrebbe essere previsto che l'Ente pubblico che affida un servizio tramite CONSIP ad un provider di posta aggiudicatario* - che ricopre il ruolo di responsabile del trattamento – *se quest'ultimo non rispetta i vincoli derivanti dal provvedimento, l'Ente, in quanto titolare del trattamento deve poter cambiare fornitore o comunque rivalersi sul responsabile.* Nel caso degli appalti CONSIP **questo fatto deve essere previsto nelle gare, altrimenti la P.A. non può fare nulla in merito.**
- Dal provvedimento oggetto della consultazione si evince che i "metadati" debbano essere sempre disponibili presso il sistema/gestore della posta elettronica, e che solo il datore di lavoro non possa più vederli dopo 7 giorni, salvo ulteriori autorizzazioni dell'Ispettorato del Lavoro. Tuttavia il datore di lavoro che acquista un pacchetto "chiavi in mano", con gli attuali strumenti informatici che gestiscono la posta elettronica, appare impossibilitato a cancellare i "metadati" dai propri sistemi, sempre che sia

in grado di accedervi. Analogamente quando stampati sotto forma di documento cartaceo, per i documenti cui sono riferibili i metadati oggetto del provvedimento dovrebbero essere adottate soluzioni di archiviazione protetta, andando a definire policy e procedure per la corretta gestione dei dati contenuti.

Sui Ruoli Privacy, e sull'opportunità di confrontarsi con "i Big Player" e l'EDBP

Il provvedimento dovrebbe inoltre richiamare l'importanza del ruoli e delle competenze del DPO (quanto previsto), e degli amministratori di sistema, figure che nella quotidianità risultano ancora sottovalutate, e che sono invece operatori di presidio strategici che sono coinvolti nella prevenzione e gestione di attacchi informatici e contenziosi con i dipendenti e collaboratori e nel caso di reati informatici.

Si suggerisce inoltre di pubblicare ulteriori dati sulle evidenze che hanno portato a questo documento di indirizzo, in quanto ad oggi risulta un solamente un provvedimento sanzionatorio a carico della Regione Lazio.

Alla luce dell'interesse mostrato dalle associazioni di imprese sul documento di indirizzo sui metadati, in quanto provvedimento che ha notevoli ripercussioni in termini di impatto sulla competitività delle aziende italiane, si ritiene opportuno condurre un confronto con il comitato europeo per la protezione dei dati personali sul tema, unitamente ad una comparatistica in materia per verificare come – specialmente i grandi provider – stiano agendo nel resto d'Europa, promuovendo un'indagine conoscitiva ispettiva nei confronti di questi ultimi per integrare il documento di indirizzo.

Il rapporto tra il cliente ed il provider rende opportuno specificare (e definire) in modo più approfondito l'esistenza dei due ruoli nell'ambito del processo di trattamento dei

metadati: quello del Titolare-Datore di lavoro e quello del Responsabile (gestore della posta, sia con server in casa del datore di lavoro, sia con fornitura esterna).

Modalità di conservazione in funzione della finalità

Come precedentemente evidenziato, a seconda dello scopo per il quale il (meta) dato viene utilizzato, il provvedimento dovrebbe tener conto – e precisare – un periodo di conservazione. Da una lettura di sistema con la disciplina giuslavoristica. Le casistiche che il provvedimento dovrebbe tenere in considerazione sono le seguenti:

- Se si utilizzano per **finalità di cybersecurity,** i tempi di conservazione non possono risultare di pochi giorni, e bisognerebbe tenere conto anche delle direttive NIS. Potrebbe essere ritenuto congruo un termine di almeno 6 mesi;
- Se si utilizzano per **finalità organizzative,** i tempi dovrebbero essere contenuti entro **pochi giorni** e risulta necessario **l'accordo sindacale ovvero l'autorizzazione** dell'Ispettorato del Lavoro;
- Se si utilizzano per **tutelare il patrimonio aziendale** i tempi potrebbero anche **essere più lunghi** (fino allo scadere dei termini di prescrizione delle azioni contrattuali o risarcitorie (10 anni) risulta necessario **l'accordo sindacale ovvero l'autorizzazione** dell'Ispettorato del Lavoro;
- Se si utilizzano **per l'esecuzione della prestazione di lavoro** (da intendersi come l'utilizzo della mail con i connessi log, il quale dovrebbe essere considerato uno **strumento di lavoro**) non risulta necessario l'accordo sindacale o l'autorizzazione, in quanto applicazione del comma 2 dell'articolo 4 della Legge 300/70, *tenuto conto che i* ***tempi debbano essere commisurati ai compiti*** *assegnati.* In ambito pubblico, almeno, il periodo di

riferimento dovrebbe essere considerato **fino al termine del procedimento amministrativo come impone anche il CAD**. Da tale considerazione deriva tuttavia la necessità di considerare che non tutte le mail inviate o ricevute confluiscono in un procedimento amministrativo, con la necessità di considerare come sia in concreto possibile "*disattivare le funzioni che non sono compatibili con le finalità del trattamento o che si pongono in contrasto con specifiche norme di settore". Prescrizione che* deriverebbe dal provvedimento in Consultazione. Si ritiene che nella prassi divenga quasi impossibile distinguere quali log cancellare dopo pochi giorni, e quali conservare per finalità amministrative.

- Nell'ambito della Pubbliche Amministrazioni, il Manuale di gestione del protocollo informatico regolamenta inoltre la gestione della documentazione, tra i quali ricade anche la posta elettronica, motivo per il quale i metadati oggetto del presente provvedimento verrebbero sempre e comunque trattati all'interno dei sistemi di protocollo o di gestione dei flussi documentali. Questi ultimi sono tipicamente integrati, in modo nativo, con le caselle di posta elettronica, pertanto i metadati sarebbero oltremodo ancor più fruibili e verificabili proprio grazie ai sistemi di protocolli.
- La norma ISO 15489:2016, che definisce il concetto di "record" (inteso come documento che entra a far parte del sistema di gestione documentale di una determinata organizzazione, e che è quindi destinato a sedimentarsi nell'archivio della stessa) per essere considerato credibile non deve essere sottoposto ad alcuna manipolazione e deve perpetuare la sua esistenza con tutti gli attributi che gli sono propri. Tale definizione si presta ad essere applicabile anche a tutti quei documenti informatici che svolgono da canale di trasmissione dei dati nello spazio e nel tempo, ovvero, nell'analisi in corso, alle mail, che

trovano una collocazione all'interno di un sistema di gestione documentale.

Da una lettura in analogia del provvedimento del Garante per la Protezione dei Dati Personali del 2009 sulla figura dell'Amministratore di Sistema, si riscontra inoltre un possibile contrasto tra i tempi di conservazione dei metadati di posta elettronica rispetto all'obbligo di conservazione dei log per un periodo non inferiore ai sei mesi.

Ulteriori strumenti oltre la posta elettronica

Oltre ai metadati di posta elettronica, bisognerebbe prendere in considerazione anche i metadati presenti su ulteriori asset, quali i firewall per gli antispam o anche quelli contenuti nei ticket restaurant digitali consegnati ai dipendenti. O ancora i centralini e chat VOIP, ovvero le piattaforme di messaggistica istantanea (incluse quelle dei social, quali Facebook, Whatsapp, Instagram, Telegram, Discord, ecc.) quando utilizzate da un'organizzazione per scopi commerciali. Anche in tali ambiti avvengono trattamenti di dati personali che devono avere quindi le medesime cautele (quali DPIA, nomina a Responsabile *ex* art. 28, ecc.) al pari di altri trattamenti di dati personali.

Tuttavia, oltre alle modalità di messaggistica, anche gli ulteriori strumenti di collaborazione hanno effettuato passi da gigante negli ultimi anni; tener conto dei metadati con solo riferimento alle email (e agli eventuali strumenti di chat) significa tener conto di una sola parte del problema, in quanto ormai le piattaforme dei **Big Player** quali ad esempio Microsoft 365 e Google Workspace, *forniscono delle intere suite integrate che, mediante funzioni analitiche*, f*orniscono informazioni sull'interazione dell'utente con gli strumenti di lavoro* (quali ad esempio sistema operativo, client di posta

elettronica, chat, videoconferenze, firewall, antivirus, strumenti di diagnostica di rete e altre applicazioni da ufficio, ecc.) *che contribuiscono ad accrescere il rischio di controllo a distanza, spesso anche inconsapevole, da parte dei datori di lavoro.*

Parimenti alla PEC, che deve mantenere caratteristiche di immodificabilità e inalterabilità per essere valida in giudizio - anche grazie ai metadati che vengono "cristallizzati" e resi in grado di fornire una data certa, una non alterabilità e una non ripudiabilità - anche la posta elettronica aziendale deve essere gestita con la massima attenzione in quanto patrimonio aziendale, perché contiene informazioni essenziali per il quotidiano operato. I provider dei servizi di posta, nell'offerta di *un servizio base,* non garantiscono un backup, né tantomeno backup crittografati a garanzia dei paradigmi di riservatezza, integrità e disponibilità.

Alla luce di una lettura in chiave tecnica, con i metadati non si va a leggere il contenuto delle e-mail, ma le informazioni che sono associate al loro scambio. La protezione dei contenuti può avvenire tramite l'adozione di soluzioni di crittografia delle email - quali ad esempio il protocollo PGP e S/MIME – configurandone le funzionalità che certificano l'autenticità del dominio di posta utilizzato, dei servizi utilizzati e dell'identità dei mittenti – SPF, DKIM, DMARC, ecc. - anche gratuitamente. All'interno dell'equazione che definisce il problema della tutela dei lavoratori a seguito di possibili controlli in violazione della Legge 300/70, e dei principi del GDPR, appare necessario inserire le ulteriori variabili che caratterizzano il sistema informativo di un'impresa, quali ad esempio una corretta configurazione dell'infrastruttura e dei servizi IT, e la declinazione di una loro corretta gestione e monitoraggio; l'adeguata informazione che dovrebbero

ricevere i lavoratori sul corretto utilizzo degli strumenti aziendali di lavoro.

Si riscontra inoltre che, ai sensi dell'articolo 11, comma 2, del DPR n.68 dell'11 febbraio 2005, durante le fasi di trasmissione del messaggio di posta elettronica certificata, i gestori mantengono traccia delle operazioni svolte su un apposito log dei messaggi, e che i dati contenuti nel suddetto registro debbano essere conservati dal gestore di posta elettronica certificata per un periodo di trenta mesi.

Infine, si chiede di considerare anche quanto viene affermato dall'**EDPB** nel recente **documento tematico del 27/11/2023 sulla** *Sicurezza del trattamento e Notifica di violazione dei dati* che esamina una selezione di esempi di decisioni definitive relative allo sportello unico (OSS) tratte dal registro pubblico del Comitato europeo per la protezione dei dati. In detto digest l'EDPB ha illustrato le **misure di sicurezza tecniche ed organizzative ex art. 32 del GDPR** considerate, generalmente, adeguate dalle Autorità di Controllo, a seguito dell'analisi di una serie di pronunce emesse, affermando, a proposito dei record di log:

"Le associazioni di protezione richiedevano alle aziende di conservare i record di log che salvavano quando si accedeva a dati specifici (set di) dati e da chi [EDPBI:LT:OSS:D:2021:298]. Una LSA ha dichiarato chiaramente che l'istituzione di registri delle attività, ossia la registrazione delle attività in "file di registro" o "registri", in particolare per l'accesso ai vari server di un sistema informatico, è fondamentale in quanto consente di tracciare le attività e di rilevare eventuali anomalie o eventi legati alla sicurezza, come l'accesso fraudolento e l'uso improprio di dati personali. L'LSA ha fatto riferimento alle

raccomandazioni di sicurezza ANSSI per l'architettura del sistema di registrazione, che evidenziano l'importanza e la necessità di registrare i registri degli eventi 20 [EDPBI:FR:OSS:D:2021:313]. Allo stesso modo, è stato riscontrato che la mancanza di revisione di qualsiasi codice di registrazione ha comportato una violazione dell'articolo 32 del GDPR [EDPBI:UK:OSS:D:2020:147]. Sebbene non sia menzionato in alcuna decisione, è utile aggiungere che la registrazione degli eventi legati agli account di amministrazione è stata evidenziata anche nelle raccomandazioni ANSSI per la sicurezza dell'amministrazione dei sistemi informatici.[21] *Per quanto riguarda la revisione dei codici di registrazione, è stato fatto riferimento alla guida OWASP sulla revisione del codice, che suggerisce di eseguire una revisione di qualsiasi codice di registrazione per identificare, tra l'altro, quali informazioni non dovrebbero essere registrate, come i dati personali sensibili e alcune forme di informazioni di identificazione personale.*[22]"

Alla luce di tali affermazioni la conservazione dei file di log per un periodo di tempo adeguato costituirebbe adempimento necessario per garantire la sicurezza.

Conclusioni

A conclusione della presente consultazione, si auspica che il Garante possa intraprendere azioni concernenti i seguenti aspetti.

Il problema della conservazione dei log sulle attività dei lavoratori dovrebbe ricadere *in primis*, sulla corretta gestione di tali informazioni da parte del Service Provider che eroga i servizi di posta elettronica.

In un secondo momento, il Titolare del Trattamento dei dati, deve essere orientato verso la comprensione (e applicazione) di regole e procedure di gestione, e su come effettuare puntuali verifiche di controllo. *Tuttavia, per quanto riguarda l'ambito più tecnologico non dovrebbero ricadere in capo ad esso*. Serve quindi che *il Garante, per rendere effettivamente applicabile questo provvedimento, chieda ai soli produttori/gestori di sistemi di posta elettronica di adeguare i loro strumenti al provvedimento stesso, focalizzando l'attenzione verso i produttori di software, mentre i datori di lavoro avranno il dovere di utilizzare sistemi di posta elettronica "a norma".*

Il provvedimento dovrebbe quindi fornire indicazioni non soltanto ai Titolari (specialmente nell'ambito Pubblico per quanto riguarda i bandi di affidamento di tali servizi), ma *soprattutto ai gestori dei sistemi di posta elettronica, pensando ad una regolamentazione dei metadati di posta elettronica e degli ulteriori strumenti e servizi che ne fanno uso, e aprendo il confronto anche con il resto d'Europa per armonizzare la normativa.*

A monte di ogni valutazione, dovrebbe essere inoltre considerato in capo al cliente/Titolare/datore di lavoro *la sussistenza dell'effettiva possibilità di poter accedere (in prima persona o per mezzo di propri subordinati che non ricadano in figure dotate di autonomia e indipendenza, quale il Responsabile per la Protezione dei Dati Personali o l'Amministratore di Sistema) a tali informazioni, ed essere in grado di poterle utilizzare nel modo che lo*

Statuto dei Lavoratori vieta. **In quanto in assenza di tale possibilità, potrebbe anche non risultare necessario procedere con la richiesta di autorizzazione.**

L'occasione appare infine ottimale per aggiornare quanto previsto all'interno delle linee guida sulla posta elettronica ed internet, e sugli amministratori di sistema, previa promozione di una consultazione online.

Hanno partecipato al presente contributo: Mauro Alovisio, Pinuccia Carena, Marco Castellano, Nicola Di Mare, Giulio Ellese, Gabriella Molinelli, Salvatore Maugeri, Cristiano Ornaghi

Il contributo si intende a titolo personale e non impegna gli enti e gli studi di afferenza

Torino, 12 aprile 2024 Il direttore

Mauro Alovisio