GARANTEPRIVACYITALIA.it

Circolare del 01 Luglio 2020

INDICE

DATA BREACH, AUMENTO DEL 66% NEI PAESI EUROPEI

Nell'ultimo anno le notifiche di violazioni dei dati personali (c.d. Data Breach) richieste dal GDPR **sono aumentate del 66%** nei principali paesi dello Spazio Economico Europeo.

L'unico paese a registrare un calo delle notifiche per Data Breach è stato il Regno Unito, che è sceso a 11.499 notifiche con una diminuizione del 17% rispetto al primo anno di piena applicazione del GDPR. Come afferma lo studio, il motivo della diminuzione si spiega in parte perché tra maggio 2018 e maggio 2019 le organizzazioni inglesi avevano comunicato le violazioni in modo eccessivo.

L'aumento delle violazioni dei dati nella maggior parte dei casi ha comportato la perdita di riservatezza sui dati e l'accesso di terze parti non autorizzate, sia attraverso atti dannosi di *Hacker* attraverso campagne di *Phishing* o per l'invio di documenti via Email a destinatari errati, sia per furto o la perdita di dispositivi mobili e *Laptop* non adeguatamente protetti.

L'analisi ha riguardato dati provenienti da **sette paesi europei**, tra cui Belgio, Francia, Germania, Italia, Polonia, Spagna e Regno Unito. In Francia, le notifiche sono quasi raddoppiate arrivando a quota 2.287, mentre in Spagna le notifiche sono state 1.609, con un **aumento di oltre il 50%.** L'aumento delle notifiche in Francia e Spagna è dovuto al fatto che le aziende sono ora più consapevoli dei loro obblighi ai sensi del GDPR.

Anche il numero di multe pubblicate nell'ultimo anno "sotto" il GDPR è stato disomogeneo in tutto il continente. L'autorità britannica per la protezione dei dati (ICO) ha riportato solo una sanzione, mentre sono state 112 quelle imposte dal Garante spagnolo. Inoltre, secondo la relazione dello studio, il garante inglese ha anche "in cantiere" sanzioni per 314 milioni di euro.

Una ricerca pubblicata da DLA Piper a gennaio 2020 aveva rilevato che le multe per violazioni del GDPR a seguito di Data Breach ammontavano allora a 114 milioni di euro, con Francia, Germania e Austria che avevano imposto le multe più elevate.

RACCOLTE FONDI: MULTATA ASSOCIAZIONE CHE INVIAVA MESSAGGI DI MARKETING A DEGLI EX DONATORI

L'Autorità belga per la protezione dei dati ha multato un'associazione che, sostenendo di avere un legittimo interesse, aveva inviato messaggi di marketing diretto a degli ex donatori che anni prima avevano contribuito a delle raccolte fondi, i quali nel frattempo avevano però esercitato il loro diritto di opposizione al trattamento ai sensi dell'21 del GDPR, richiedendo al Titolare (ovvero la stessa associazione) la cancellazione dei loro dati personali ai sensi dell'art.17 dello stesso GDPR.

La sanzione amministrativa, **pari a mille euro**, è scattata a seguito di un reclamo presentato all'autorità belga in cui gli interessati avevano lamentato il mancato riscontro all'esercizio dei loro diritti. Oltre a non aver rispettato i diritti di opposizione e di cancellazione, l'autorità belga ha anche ritenuto che nel caso di specie l'associazione non potesse validamente invocare il suo legittimo interesse come base giuridica per il trattamento, perché nel complesso non soddisfaceva le condizioni imposte dalla giurisprudenza.

Secondo recenti orientamenti, per invocare l'articolo 6.1, lettera f) del GDPR, il Titolare del trattamento deve infatti **poter dimostrare** che

1) gli interessi perseguiti possono essere riconosciuti come legittimi;

2) il trattamento è necessario ai fini del trattamento previsto;

3) che sia stato fatto un bilanciamento di tali interessi con i diritti e le libertà fondamentali delle persone interessate, il quale grava sul Titolare del trattamento o su una terza parte.

Nella fattispecie, la Camera delle controversie belga ha ritenuto che non era stata soddisfatta la terza condizione dell'articolo 6.1, lettera f), del GDPR e della giurisprudenza della Corte di Giustizia.

Più specificamente ha riscontrato che sussistevano dubbi sul fatto che l'interessato potesse ragionevolmente aspettarsi che i suoi dati personali fossero trattati per scopi di marketing diretto anni dopo la raccolta di questi dati (considerando 47 GDPR). Inoltre, il Titolare del trattamento non aveva sufficientemente agevolato il diritto di opposizione.

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI INFLIGGE UNA MULTA DA 600MILA EURO AD UNICREDIT

Al termine di una complessa istruttoria riguardante un Data Breach, causato da accessi abusivi ai dati personali di oltre 700 mila clienti di Unicredit spa, il Garante italiano ha inflitto all'istituto bancario una sanzione di **600 mila euro**. Nel 2017 era stata la banca stessa a comunicare all'autorità le violazioni subite tra aprile 2016 e luglio 2017.

Gli accessi abusivi, avvenuti in due momenti distinti, erano stati effettuati utilizzando le utenze di alcuni dipendenti di un partner commerciale esterno alla banca, ed avevano riguardato una serie di informazioni riguardanti gli interessati, tra cui dati anagrafici e di contatto, professione, livello di studio, estremi identificativi di un documento di riconoscimento e informazioni relative a datore di lavoro, salario, importo del prestito, stato del pagamento, "approssimazione della classificazione creditizia del cliente" e codice IBAN.

La sanzione, che è stata determinata applicando la disciplina precedente l'entrata in vigore del GDPR, segue la contestazione di violazioni amministrative notificata alla banca stessa nel maggio scorso, originata a sua volta da un provvedimento adottato dall'Autorità nel marzo 2019 con il quale aveva accertato la violazione da parte dell'istituto bancario delle misure minime di sicurezza previste dal Codice privacy e il mancato rispetto delle regole fissate dalla stessa Autorità nel provvedimento n. 192 del 12 maggio 2011 in materia di tracciamento delle operazioni bancarie.

Considerati i rilevanti profili di illiceità del trattamento determinati dalla mancata adozione di misure tecniche e organizzative adeguate e valutate le argomentazioni addotte dalla banca, il Garante ha ritenuto quindi necessario l'applicazione della sanzione al fine di salvaguardare i diritti e le libertà delle persone coinvolte, a prescindere dalla notificazione della violazione di dati personali effettuata dalla banca.

Nel determinare l'ammontare dell'importo in 600mila euro, l'Autorità ha tenuto conto di diversi elementi, tra i quali il fatto che le violazioni sono state commesse nei confronti di un rilevante numero di persone e che la banca, che non ha subito precedenti provvedimenti sanzionatori del Garante, a seguito del Data Breach ha adottato diverse misure e iniziative volte a rafforzare la sicurezza dei propri sistemi informatici.

AUTORITÀ GARANTE: I TRIBUNALI NON SONO TENUTI A CONOSCERE LO STATO DI SALUTE DEI SOGGETTI CUI NOTIFICARE ATTI GIUDIZIARI

Per assicurare il contenimento del contagio da Covid-19 e la protezione degli ufficiali giudiziari i Tribunali **non sono tenuti** a conoscere lo stato di salute dei soggetti cui notificare atti giudiziari, ma, come previsto dalle norme adottate dal Governo, devono predisporre adeguati dispositivi di protezione individuale.

È quanto ha precisato l'Ufficio del Garante per la protezione dei dati personali in una nota indirizzata al Ministero della Giustizia con cui ha fornito il suo parere in merito alla questione sollevata da un' azienda sanitaria di Verona, alla quale l'UNEP (Ufficio Notifiche Esecuzioni e Protesti) del Tribunale della stessa città aveva chiesto di poter avere quotidianamente gli elenchi aggiornati delle persone positive o sospette positive al Covid-19, dei soggetti in quarantena e dei loro conviventi, nonché a loro dislocazione.

Il Garante ha ritenuto che la disponibilità dei predetti elenchi delle Aziende sanitarie **non risulta necessaria** né all'esercizio delle funzioni attribuite all'UNEP, né alla protezione dal contagio del personale addetto alle notifiche.

Nel fornire la sua risposta, l'Autorità ha tenuto conto del fatto che, in assenza di una mappatura dell'intera popolazione in merito al contagio Covid-19, l'eventuale stato di positività dei destinatari degli atti potrebbe sussistere, seppure non ancora accertato.

Di conseguenza, in linea con le raccomandazioni dell'Istituto Superiore di Sanità, i Tribunali devono adottare le misure di protezione individuale, disposte dal Governo per i lavoratori a contatto con il pubblico, nei confronti di tutti gli operatori UNEP **a prescindere** dal fatto che essi accedono a locali ove è domiciliata una persona accertata Covid-19.

Occorre inoltre considerare, che anche ove tali elenchi fossero acquisiti spetterebbe ai tribunali una difficile opera di aggiornamento, tenuto conto che gli stessi sono in continua evoluzione sulla base dei risultati dei tamponi.

L'Ufficio del Garante si è comunque reso disponibile a interloquire con il Ministero della giustizia per trovare una soluzione che consenta lo svolgimento dei compiti degli UNEP assicurando, al contempo, la protezione dal contagio del personale impiegato e la riservatezza dei soggetti posti in isolamento domiciliare per Covid-19.

TIM: DIPENDENTI INFEDELI VENDEVANO DATI PERSONALI DEI CLIENTI AI CALL CENTER, 13 ARRESTI

Decine di migliaia di euro spartiti tra gli operatori infedeli ed i collettori/rivenditori dei dati. Ecco il volume di affari scoperto dalla Polizia Postale e delle Comunicazioni, con il coordinamento della Procura di Roma, nell'ambito della fase conclusiva dell'operazione ***Data Room***. Di assoluto livello criminale la mole dei proventi, come emerge da più di una conversazione nella quale alcuni indagati discutono dei corrispettivi, mettendosi d'accordo sulla ripartizione degli incassi illeciti del mese.

L'attività di commercializzazione delle liste di utenti e i relativi recapiti, riguardava anche i sistemi informatici in uso a gestori operanti nel settore dell'energia, un filone dell'indagine in corso di ulteriore approfondimento.

Le indagini sono state portate avanti dagli specialisti del Servizio Polizia Postale e delle Comunicazioni che hanno svolto intercettazioni telefoniche e pedinato gli indagati, analizzato i sistemi informatici delle piattaforme contenenti i dati, analisi rese possibili anche grazie alla collaborazione della struttura di sicurezza aziendale di Telecom Italia.

È **la prima operazione** su larga scala per la tutela dei dati personali trafugati, un fenomeno noto a tutti che vede coinvolti dipendenti infedeli, call center compiacenti ed intermediari e che ha quale oggetto ciò che sul mercato ha assunto un significativo valore commerciale: i dati riservati relativi all'utenza.

Per l'esecuzione dei provvedimenti restrittivi e di perquisizione, per l'attività informativa, il CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) ha coordinato un team di specialisti in collaborazione con i compartimenti della polizia Postale di Roma, Napoli, Perugia ed Ancona.

Impiegati 100 specialisti della polizia Postale per i 20 provvedimenti cautelari, **13 ordinanze di arresti domiciliari e 7 di obbligo di dimora** nel comune di residenza. Notificate anche ordinanze che stabiliscono per altri indagati il divieto di aprire imprese o ricoprire incarichi direttivi: nei loro uffici ci sono state perquisizioni anche informatiche. Gli indagati sono responsabili, a vario titolo ed in concorso tra loro, della violazione aggravata dei reati di **accesso abusivo a sistema informatico** e di **detenzione**

abusiva e diffusione di codici di accesso, e della **violazione della legge sulla privacy** e **diffusione illecita di dati personali** oggetto di trattamento su larga scala.

Tra gli arrestati ci sono dipendenti infedeli di compagnie telefoniche, (i procacciatori materiali dei "preziosi" dati), gli intermediari che si occupavano di gestire il commercio delle informazioni estratte dalle banche dati, e i titolari di call center telefonici, che sfruttavano le informazioni per contattare potenziali clienti e lucrare le commissioni per ogni portabilità, che arrivano fino a 400 euro per ogni nuovo contratto stipulato.

A carico degli indagati, nel corso delle indagini, sono stati acquisiti "concreti e inequivocabili elementi probatori" riguardo ai ripetuti accessi abusivi alle data room in uso ai gestori telefonici operanti sul territorio nazionale e gestite direttamente da Tim, contenenti gli ordini di lavoro di delivery e i reclami di *Assurance* provenienti dalle segnalazioni dell'utenza relativamente ai disservizi della rete di telecomunicazioni.

L'inchiesta è stata avviata nel mese di febbraio scorso dal CNAIPIC, su delega della Procura di Roma, a seguito di una **denuncia depositata da parte di Telecom Italia**, nella quale si segnalavano vari accessi abusivi ai sistemi informatici gestiti da Tim, riscontrati almeno a partire dal gennaio 2019.

Gli accessi abusivi avvenivano tramite *Account* o *Virtual Desktop* in uso ai dipendenti di gestori di servizi di telefonia e di società partner per l'accesso ai database, chiavi spesso carpite in modo fraudolento, direttamente gestiti dalla stessa società denunciante, in ragione della concessione delle attività di manutenzione della infrastruttura telefonica nazionale. Le banche dati vengono alimentate da tutti i gestori telefonici in relazione alle segnalazioni ricevute dai clienti sui disservizi, rappresentando oltretutto una vera e propria istantanea delle condizioni della infrastruttura nazionale di telecomunicazioni.

Le estrazioni, per come verificato nel corso delle intercettazioni, venivano sistematicamente portate avanti con un volume medio di centinaia di migliaia di record al mese. Gli indagati gestivano tali volumi modulandoli a seconda della illecita "domanda" di mercato, come emerge ad esempio da una conversazione nella quale uno degli indagati chiede a un dipendente infedele una integrazione di 15.000 record per arrivare ai 70.000 pattuiti per il mese in corso, preannunciando un ulteriore ordine per 60.000 utenze mobili.

Le informazioni estratte dal database, divenivano quindi oggetto di un illecito mercimonio, in quanto particolarmente appetibili per le società di vendita di contratti da remoto che cercano per l'appunto di intercettare la clientela più "vulnerabile", a causa di problemi o disservizi, per proporre quindi il cambio del proprio operatore telefonico.

Il complesso "sistema" vedeva da un lato una serie di tecnici infedeli in grado di procacciare i dati, dall'altro una vera e propria rete commerciale che ruotava attorno alla figura di un imprenditore campano, acquirente della "merce" ed a sua volta in grado di estrarre "in proprio", anche con l'utilizzo di software di automazione, grosse quantità di informazioni, in virtù di credenziali illecitamente carpite a dipendenti ignari. La "merce" veniva poi piazzata sul mercato dei call center, 13 sono quelli già individuati, tutti in area campana, ed oggetto di altrettante attività di perquisizione.

I dati stessi, adeguatamente "puliti" per essere utilizzati dai diversi call center, passavano di mano in mano, rivenduti a prezzi ridotti in base alla "freschezza" del dato stesso, motore di un movimento che alimenta il fenomeno delle continue proposte commerciali che tutti ben conoscono. Di assoluto livello criminale la mole dei proventi, come emerge da più di una una conversazione nella quale alcuni indagati discutono dei corrispettivi, frutto dell'attività illecita, pattuendo la ripartizione dei proventi illeciti del mese, per decine di migliaia di euro da spartirsi tra gli operatori infedeli ed i collettori/rivenditori dei dati.

Le indagini tecniche hanno fatto anche emergere come l'attività di commercializzazione di liste di utenti e relativi recapiti, riguardasse anche i sistemi informatici in uso a gestori operanti nel settore dell'energia, in corso di ulteriore approfondimento.

Si tratta della **prima operazione su larga scala volta alla tutela dei dati personali trafugati**, un fenomeno noto a tutti che vede coinvolti dipendenti infedeli, call center compiacenti ed intermediari e che ha quale oggetto ciò che sul mercato ha assunto un significativo valore commerciale: i dati riservati relativi all'utenza.

> Tim esprime "il più vivo ringraziamento" all'autorità giudiziaria e alla polizia "per aver portato a termine con successo l'indagine relativa alla divulgazione e commercio abusivo di dati anagrafici e numeri telefonici della clientela".