WeTransfer Security Incident: File Transfer Emails Sent to Wrong People

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/zGtCsr6fREA/wetransfer-security-incident-file-transfer-emails-sent-wrong-people

---

Marketing online, Garante Privacy: “No alla raccolta punti acchiappa dati”

All’Autorità Garante per la protezione dei dati personali è giunta una segnalazione che ha lamentato il non completo rispetto nella normativa privacy sul servizio di registrazione al sito www.pampers.it. Così il Garante ha potuto accertare le due seguenti criticità con riferimento all’acquisizione dei consensi richiesti agli interessati per il trattamento dei loro dati:

1) il primo consenso richiesto per finalità promozionali, di invio di newsletter, analisi statistiche, sondaggi d’opinione, con riguardo al marchio “Pampers” è risultato accomunare indistintamente più diverse finalità, impedendo all’interessato di poter distinguere fra di esse e di fornire il proprio consenso libero e selettivo;

2) anche il secondo consenso – ossia quello richiesto per le

medesime finalità di cui al punto precedente, ma con riguardo ai diversi marchi “Lines”; “Linidor”; “Tampax”; “Ace” ed “Infasil” – è risultato affetto dal medesimo vizio del primo ed inoltre da selezionare obbligatoriamente per poter procedere con la registrazione al sito web in questione, e, quindi, anche per poter partecipare al programma di raccolta punti.

Per la raccolta punti non obbligatorio esprimere il consenso a ricevere pubblicità

Emerge che il trattamento dei dati riferiti agli utenti, raccolti con le queste modalità, sia avvenuto in modo illecito, perché ai clienti interessati alla raccolta punti, infatti, non veniva data la possibilità, come richiesto dalla normativa, di esprimere un consenso libero e specifico per le singole finalità di trattamento che la società intendeva svolgere, tra le quali vi era appunto l’attività promozionale. Per poter completare la registrazione e aderire al programma di fidelizzazione i clienti erano invece obbligati a rilasciare due consensi generici, uno per la società e uno per i marchi collegati.

Per questo motivo il Garante ha quindi vietato all’aziendal’ulteriore trattamento per finalità promozionali dei dati di oltre un milione e mezzo di persone, acquisiti in modo illecito mediante il form “raccolta punti” del sito della società.

In virtù di questo caso, il Garante Privacy ha precisato che per poter partecipare ad un programma di raccolta punti e usufruire così di piccoli vantaggi il cliente non deve essere obbligato ad esprimere il consenso a ricevere pubblicità.

Per i trattamenti illeciti è stata applicata una sanzione amministrativa che la società ha già pagato.

https://www.key4biz.it/marketing-online-garante-privacy-no-alla-raccolta-punti-acchiappa-dati/262635/

Massive Data Breach at Canada Credit Union Giant Desjardins

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/aLXDI1aYVQE/massive-data-breach-canada-credit-union-giant-desjardins

---

UK Regulator Calls Out Compliance Failures in Targeted Advertising Industry

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/gh22KxmHUkw/uk-regulator-calls-out-compliance-failures-targeted-advertising-industry

---

Libra, l’allarme del Garante Privacy: ‘Con la moneta gli OTT diventano Stato-padroni’

“*I colossi del web hanno oggi volumi di transazioni paragonabili a quelli di molti Stati, trattano alla pari con i governi, fanno con loro accordi non solo commerciali, e adesso battono anche moneta. Quote immense di potere stanno via via passando di mano dagli Stati a soggetti privati. Se il settore non sarà vincolato in fretta a principi di governance democratica, rischiamo di consegnare un’ampia fetta dei nostri diritti ad un pugno di monarchie digitali, fondate sul potere dei dati*“.

E’ questo l’allarme lanciato oggi da **Antonello Soro**, presidente dell’Autorità Garante per la protezione dei dati personali, intervistato dal ‘**Mattino**‘, parla di emergenza democratica in riferimento al rischio legato alla moneta alternativa di **Facebook** che sarà lanciata nella prima metà del 2020.

“*Adesso si dirà che i dati delle transazioni finanziarie resteranno separati da quelli che Facebook raccoglie sulla piattaforma social, ma in realtà abbiamo già troppe esperienze di impegni mancati rispetto alla privatezza”,* ha aggiunto Soro. “*La piattaforma americana si impegnò ad esempio a tenere distinti i dati social degli utenti da quelli raccolti su Whatsapp. Ma così non è accaduto. Pensare che non accadrà neanche questa volta è dunque del tutto legittimo. Stavolta con conseguenze ancora più preoccupanti anche per la privacy. Anche il sistema blockchain non è così sicuro come viene presentato, ma evidenzia anzi molte possibili criticità*”.

A proposito di Libra

Libra, questo il nome della criptomoneta, sarà una moneta virtuale, tecnologicamente simile al **Bitcoin**, con la quale ogni utente potrà pagare la corsa su Uber, l'abbonamento di **Spotify**, comprare su **Instagram** o inviare soldi a un parente. Il tutto tramite Facebook e le sue app associate come **Messenger** e **WhatsApp**.

La moneta sarà lanciata nella prima metà del prossimo anno e sarà gestita dalla **Libra Association**, organizzazione indipendente e non-profit con sede a Ginevra, in Svizzera, che raduna 28 partner, tra cui:

- Pagamenti: Mastercard, PayPal, PayU (braccio fintech di Naspers), Stripe, Visa;
- Tecnologia e mercati: Booking Holdings, eBay, Facebook / Calibra, Farfetch, Lyft, Mercado Pago, Spotify AB, Uber Technologies, Inc.;
- Telecomunicazioni: Iliad, Vodafone Group;
- Blockchain: Anchorage, Bison Trails, Coinbase, Inc., Xapo Holdings Limited;
- Venture Capital: Andreessen Horowitz, Iniziative innovative, Ribbit Capital, Thrive Capital, Union Square Ventures;
- Organizzazioni non profit e multilaterali e istituzioni accademiche: Creative Destruction Lab, Kiva, Mercy Corps, Women's World Banking.

"*La missione è creare un'infrastruttura finanziaria globale che serva a miliardi di persone in tutto il mondo*", ha scritto il CEO di **Facebook Mark Zuckerberg.** "*Vogliamo rendere facile per tutti inviare e ricevere denaro proprio come accade con le nostre App per condividere istantaneamente messaggi e foto*".

Libra porterà una svolta epocale, ma il rischio di un potere troppo grande dato a delle società privata fa preoccupare e non poco, per Soro infatti "O*ccorre pensare tuttavia a come costruire forme di regolazione della società digitale*".

https://www.key4biz.it/libra-lallarme-del-garante-privacy-con-la-moneta-gli-ott-diventano-stati-padroni/262455/

Google Boosts Chrome Protection Against Deceptive Sites

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/gmDZcud2SWM/google-boosts-chrome-protection-against-deceptive-sites

---

Facebook's Currency Libra Faces Financial, Privacy Pushback

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/yfqx2qxoxhY/facebooks-currency-libra-faces-financial-privacy-pushback

Privacy, Buttarelli: ‘Libra richiederà un accurato controllo da parte delle Autorità’

“*Riconosciamo il potenziale delle nuove tecnologie, ma l’introduzione della moneta digitale annunciata da Facebook richiederà un accurato controllo da parte delle diverse agenzie, comprese le Autorità per la protezione dei dati*“.

E’ quanto affermato dal Garante europeo per la protezione dei dati **Giovanni Buttarelli** in un’intervista rilasciata a **Business Insider Germany,** dopo l’annuncio di ieri fatto da **Facebook** sull’introduzione
della nuova moneta digitale ‘**Libra**‘ insieme ad 27 aziende internazionali.

Ma la criptovaluta ha già fatto storcere il naso a esperti e Istituzioni
dato che il potenziale di **Libra** è enorme, soprattutto perché **Facebook** ha già 2,7 miliardi di utenti attivi insieme a **Whatsapp** e **Instagram**.

La criptovaluta

Facebook prevede di lanciare la criptovaluta **Libra** nella prima metà del prossimo anno. I partner includono i fornitori di servizi di pagamento **Mastercard**, **Visa** e **Paypal**. Ci sono anche aziende come **Uber**, **Ebay** e **Spotify** e telco come **Vodafone ed Iliad.** Con Libra, non sono fatte solo transazioni tra aziende e consumatori che usano Facebook. La Criptovaluta intende

offrire alle persone senza un conto bancario l'accesso ai servizi finanziari per la prima volta. Soprattutto in regioni come l'Asia e l'Africa il potenziale della criptovaluta risulterà essere immenso.

"*Qualsiasi combinazione di dati personali, comporta ulteriori rischi per i diritti e le libertà dei cittadini*", ha dichiarato Buttarelli. Sarebbe "*molto discutibile se un'azienda che ha accesso a enormi quantità di dati personali raccolti attraverso le sue piattaforme di social media e servizi di comunicazione sarebbe in grado di combinare tali informazioni con il perseguimento di acquisti digitali online", avverte il responsabile della protezione dei dati.*

Ma Facebook è stato in passato più volte criticato, soprattutto a causa di una mancanza di impegno in termini di protezione dei dati – non da ultimo con lo scandalo **Cambridge Analytica**, dove sono stati sottratti milioni di dati personali.

L'appello di Francesco Boccia (PD)

"*Facebook lancia Libra nel 2020, la sua criptovaluta che si somma a tutte le altre esistenti e senza regolazione. I governi cosa pensano? E le Banche centrali? E la Commissione europea? Tutti in silenzio. E chi tra noi, da anni, pone il problema passa per matto...*", ha dichiarato ieri **Francesco Boccia**, deputato e economista PD.

"*Com'era facilmente prevedibile aumentano criptovalute di ogni genere e mezzi di pagamento alternativi,* ha aggiunto Boccia, *con un utilizzo sempre più disinvolto. Non c'è alcuna regolazione e il rischio caos è dietro l'angolo. La politica, a tutti i livelli, nazionali e comunitari, non può restare a guardare*".

https://www.key4biz.it/privacy-buttarelli-libra-richiedera-un-accurato-controllo-da-parte-delle-autorita/262204/

Modelli organizzativi per la gestione dei rischi informatici. Il caso Rousseau

La conformità del trattamento dei dati personali alla disciplina del regolamento 2016/679 (e ad altre disposizioni del diritto europeo o nazionale) riposa sull'adozione di un modello organizzativo in cui, seguendo il noto princìpio della divisione del lavoro di **Adam Smith**, il titolare e il responsabile del trattamento definiscono compiti e funzioni connessi al trattamento per il cui svolgimento vengono opportunamente designate figure interne ed esterne all'organizzazione (responsabili del trattamento, amministratori di sistema, persone autorizzate al trattamento). La designazione – peraltro richiesta dal nuovo d.lgs. 196/2003 all'art. 2-*quaterdecies* nel caso in cui i citati titolari e responsabili prevedano un'organizzazione delle attività di trattamento[1] – appare opportuna sotto il profilo dell'*accountability*, rappresentando la testimonianza di uno sforzo organizzativo compiuto per conseguire i predetti obiettivi di *compliance*. Il d.lgs. 231/2001, con la previsione dell'organismo di vigilanza per l'attuazione, da parte dell'ente, del Modello di Organizzazione, Gestione e Controllo (art. 6, c.1, lett. b)), ci offre un ulteriore spunto circa l'opportunità di costituire una struttura di controllo del funzionamento del modello organizzativo per la protezione dei dati, e dunque dello stato di adeguamento alla normativa. In questa prospettiva, si delineano ipotesi di costituzione di

“gruppi di lavoro privacy” indipendenti (con componenti esterni all’organizzazione del trattamento) o di organi di *staff* collocati in posizioni di terzietà, in cui cioè non vengono determinate le finalità e i mezzi del trattamento; strutture che peraltro sono chiamate a supportare la funzione del *data protection officer* nei casi in cui una tale figura sia stata designata dal titolare o dal responsabile del trattamento[2]. Il modello organizzativo privacy (insieme alla struttura di controllo) descrive pertanto un assetto aziendale preordinato allo svolgimento della propria attività in chiave *data protection*, rappresentando in tale prospettiva un’evoluzione culturale dell’organizzazione con effetti favorevoli sul piano dell’immagine e dei requisiti di affidabilità attesi o richiesti dall’esterno, ad esempio, nei rapporti con le associazioni dei consumatori, nelle attività di *public affairs*, nelle procedure di gara.

Profili di sicurezza del modello organizzativo data protection

Con riguardo al profilo della sicurezza dei trattamenti, il modello dovrebbe integrare processi, *routine* organizzative e regolamenti interni a supporto della gestione dei rischi, connotandosi pertanto anche come *governance* del rischio; sotto questo aspetto, le attività operative principali indicate dalla prassi e dalla letteratura tecnica comprendono (i) l’individuazione degli asset informatici che intervengono nelle attività di trattamento e la valutazione delle loro vulnerabilità, (ii) l’individuazione delle minacce incombenti sui sistemi di Ict (con cui i dati sono trattati), (iii) la valutazione del rischio (nelle sue componenti di probabilità e gravità delle conseguenze) alla luce delle misure di sicurezza esistenti, per poi (iv) determinare gli eventuali interventi (misure) di variazione che, in linea con le previsioni dell’articolo 32 del regolamento, possano garantire un livello di sicurezza adeguato al rischio[3]. Il (sintetico) processo

operativo appena tratteggiato lascia intuire il suo carattere dinamico in ragione del fatto che il “rischio residuo”, ossia il rischio a cui sono esposti i dati con l’applicazione delle *ultime* misure di sicurezza, va necessariamente rivalutato in relazione a possibili modifiche del quadro di riferimento (cambiamenti organizzativi, evoluzione tecnologica, nuove modalità di trattamento, passaggio da dati comuni a dati particolari)[4].

I processi e le procedure che caratterizzano il modello organizzativo per gli aspetti di sicurezza vanno, altresì, integrati in relazione alla gestione dei casi di violazione che possono riguardare i dati personali, in ragione del fatto che anche l’adozione di misure di sicurezza efficaci non esclude che la minaccia possa verificarsi producendo un impatto; l’intervento *ex post*, dunque, va sempre pianificato in considerazione di un rischio che non è completamente e permanentemente eliminabile. La gestione delle violazioni (in cui la minaccia si è verificata, ma va accertato se e in che misura questa ha interessato dati personali) si caratterizza pertanto come capacità di reazione dell’organizzazione, implicando la costituzione di una *data breach unit* per il coordinamento di un complesso di attività volte a rilevare gli eventi e i comportamenti (*alert*, tracciamento degli accessi)e valutarne le caratteristiche (apertura di una scheda descrittiva) per decidere in merito alla loro registrazione[5], all’attivazione di protocolli di risposta e alle comunicazioni all’autorità di controllo e agli interessati. Una tale gestione è tanto più complessa in relazione all’esternalizzazione del trattamento in cui gli accordi di appalto e subappalto di operazioni sui dati personali coinvolgono più responsabili esterni del trattamento. Simili situazioni richiedono l’integrazione nel modello organizzativo di attività di gestione e coordinamento dei casi di violazione della sicurezza esterni al titolare – che avvengono, cioè, presso i responsabili o sub-responsabili del trattamento – affinché lo stesso possa venirne a

conoscenza nei tempi più brevi, per poi valutare come procedere nel quadro delle previsioni degli articoli 33 e 34 del regolamento[6]. Con riguardo alla valutazione del rischio *post*-violazione che, nell'ambito di tale quadro, il titolare è tenuto a svolgere, merita osservare come la disponibilità di una preventiva analisi del rischio – ad esempio, quella che ricorre nella valutazione di impatto del trattamento sulla protezione dei dati – possa rappresentare una fonte utile da cui derivare il rischio che consegue a una violazione dei dati personali; ben inteso la necessità di effettuare una valutazione aggiuntiva in relazione alle specifiche circostanze della violazione[7].

Il caso della piattaforma Rousseau

Il caso *Rousseau* – la piattaforma tecnologica del **Movimento 5 Stelle** utilizzata, tra l'altro, per svolgere operazioni di votazione – mostra come una gestione 'occasionale' dei processi sottostanti la valutazione dei rischi, priva di un modello organizzativo di riferimento, possa essere all'origine delle vulnerabilità dei sistemi di Ict del Movimento 5 Stelle che, con ogni probabilità, sono state sfruttate per compiere l'intrusione informatica e determinare la violazione dell'agosto del 2017[8].

Sotto questo profilo, l'attività ispettiva del Garante ha fatto emergere un quadro della sicurezza dei siti web gestiti dal Movimento caratterizzato da misure tecniche obsolescenti e da misure organizzative che non garantivano un apprezzabile livello di riservatezza agli iscritti alla piattaforma di *e-voting*. Le *policies* adottate ammettevano l'uso di chiavi di identificazione di lunghezza inferiore a otto caratteri che, in tal modo, risultavano facilmente esposte ad azioni di tipo *brute force*[9]; le stesse politiche sono apparse limitate con

riguardo all'*auditing* informatico in ragione del mancato tracciamento degli accessi effettuati dagli amministratori di sistema e la mancata configurazione di profili di autorizzazione differenziati e limitati ai soli trattamenti e dati necessari in relazione agli specifici ambiti di operatività.

Conclusioni

La vicenda appena tratteggiata, come altre (si pensi ai casi *Ashley Madison* del 2015, *Heartbleed* del 2014, *Target* del 2013), lasciano intuire come l'assenza di una *governance* del rischio ovvero l'adozione di soluzioni destrutturate e approssimate siano l'immagine di una vulnerabilità di tipo organizzativo prima ancora che tecnico-strumentale; e come tale condizione possa generare impatti sulla sfera giuridica delle persone (diritti e libertà) o su taluni loro aspetti e interessi comunque significativi (economico-finanziario, fisico, psicologico) che possono anche determinare azioni legali da parte degli interessati. Sotto altro profilo – se pure non rilevante ai fini del regolamento – non vanno sottaciute le conseguenze sulle stesse aziende (e pubbliche amministrazioni) derivanti dalla mancanza di modelli organizzativi privacy. A tal riguardo, il caso ***Yahoo!*** – la ***data breach*** più importante della storia (oltre un miliardo di account violati) – é emblematico; gli attaccanti avrebbero sottratto nomi, indirizzi e-mail, numeri di telefono, date di nascita, password criptate e in qualche caso anche domande di sicurezza cifrate o in chiaro, con le relative risposte; tali dati sarebbero stati messi in vendita nel dark web, per circa 300.000 dollari. Anche a causa di questa violazione (e di altre precedenti, non comunicate tempestivamente dall'azienda), secondo alcuni analisti finanziari la quotazione di Yahoo!, nell'ambito dell'acquisizione da parte di Verizon, avrebbe subìto un ribasso di circa 350 milioni di dollari[10].

La *governance* del rischio descrive un aspetto centrale del modello organizzativo per la protezione dei dati personali delineato dal regolamento; da essa promanano le decisioni sul trattamento (tecnologie utilizzate, valutazione di impatto) ovvero, nel caso di una violazione dei dati, sulla notifica al Garante e la comunicazione agli interessati, nonché sugli accordi con gli operatori esterni che dovrebbero trattare dati per conto del titolare. Nella prospettiva del regolamento, un tale modello è destinato a diventare il *driver* di una cultura organizzativa della *data protection* che, dal vertice alle unità operative, pone al centro il rischio per i diritti e le libertà degli interessati attuando processi strutturati e mezzi del trattamento che incorporano nativamente misure di anonimizzazione o pseudonimizzazione o, ancora, di minimizzazione dei dati.

---

[1] Sul punto, il primo comma dell'art. 2-*quaterdecies* stabilisce che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.*".

[2] Merita al riguardo osservare come la letteratura abbia accostato la funzione del *data protection officer* a quella dell'organismo di vigilanza *ex* d.lgs. 231, in ragione dei compiti di sorveglianza che gli sono stati attribuiti dal regolamento, ponendo tra l'altro il quesito circa una possibile sovrapposizione dei ruoli in quelle realtà in cui è stato costituito un Odv. Sul punto si veda, tra gli altri P. Ghini, *Data protection officer: ODV per la privacy?*, 3 settembre 2015, https://www.tavoli231.it/single-post/2015/09/03/Data-protection-officer-ODV-per-la-privacy A. Sannoner, *Il rapporto tra Organismo di Vigilanza e il nuovo GDPR*, 14 settembre 2018,

https://www.portale231.com/il-rapporto-tra-organismo-di-vigilanza-e-il-nuovo-gdpr/

[3] Sappiamo, al riguardo, che l'art. 32 non prescrive "misure minime" ma elenca alcune misure attuative, segnatamente (i) la pseudonimizzazione e la cifratura dei dati personali, (ii) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, (iii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, (iv) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

[4] Si pensi, ad esempio al disegno di legge appena approvato in via definitiva recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo" in virtù del quale, ai fini della verifica dell'osservanza dell'orario di lavoro, le amministrazioni pubbliche (di cui all'articolo 1, comma 2, del decreto legislativo n. 165/2001) dovranno introdurre sistemi di identificazione biometrica e di videosorveglianza in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso. Una tale modifica del trattamento di dati personali implica una rivalutazione del rischio residuo alla luce dell'introduzione di dati biometrici precedentemente non raccolti.

[5] È il caso previsto dall'art. 33, par. 5 del regolamento che, in altre parole, stabilisce l'obbligo per i titolari del trattamento di costituire un registro delle violazioni dei dati personali, indipendentemente dalla necessità di comunicazione all'autorità di controllo e agli interessati.

[6] A tal riguardo, va ricordato che, nel caso di violazione di dati personali, il responsabile del trattamento è tenuto a informare il titolare dopo essere venuto a conoscenza della

violazione stessa (art. 33, par. 2); il che lascia ragionevolmente intendere che sia il responsabile del trattamento ad attuare le misure tecniche e organizzative per la rilevazione delle violazioni della sicurezza e le loro eventuali implicazioni sui dati personali.

[7] Al riguardo, si veda Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee-guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*, p. 12.

[8] Cfr. Garante per la protezione dei dati personali, *Provvedimento su data breach – 21 dicembre 2017*, Provvedimento n. 548/2017, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7400401; *Provvedimento su data breach – 4 aprile 2019*, Provvedimento n. 83/2019, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974

[9] Il tempo necessario per compiere l'attacco aumenta esponenzialmente all'aumentare della lunghezza della password e della tipologia di caratteri. Per proteggersi da questo tipo di attacco è dunque opportuno utilizzare password molto lunghe e complesse contenenti caratteri maiuscoli, minuscoli, numerici, simboli e spazi. In tal modo il tempo necessario per completare l'attacco potrebbe passare da pochi minuti a settimane o addirittura anni secondo la velocità del calcolatore che esegue i tentativi e il tempo di risposta del server o servizio che si sta attaccando. Sull'argomento si veda A. Carriero, *Virus e sicurezza informatica: attacco Brute Force*, https://www.matematicamente.it/informatica/informatica-di-base/virus-e-sicurezza-informatica-at Si veda anche R. Rijtano, *Brute force: cosa sono, come fare e prevenire gli attacchi a forza bruta*,

https://www.cybersecurity360.it/nuove-minacce/brute-force-cosa-sono-gli-attacchi-a-forza-bruta-come-farli-e-prevenirli/

[10] Cfr. Clusit, *Rapporto 2017 sulla sicurezza ICT*, Milano, 2017, 16.

https://www.key4biz.it/modelli-organizzativi-per-la-gestione-dei-rischi-informatici-il-caso-rousseau/261942/

Udo Helmbrecht (Enisa): 'Implementare il GDPR la vera sfida per la cybersecurity'

"*Il GDPR ha fornito un solido quadro giuridico sulla protezione dei dati. Tuttavia, con il numero sostanziale di violazioni di dati su larga scala, è necessario disporre di nuovi modelli di sicurezza per la protezione dei dati personali. Mentre il GDPR è un punto di partenza per la conformità e il servizio, l'implementazione rimane una sfida.*

Sono state queste le parole del direttore esecutivo dell'Enisa, **Udo Helmbrecht**, pronunciate durante il settimo forum annuale sulla privacy dell'**Agenzia europea per la sicurezza delle reti e dell'informazione**, che si è aperto ieri a Roma, all'**Università Luiss.**

L'Annual Privacy Forum (APF) è diventato un rinomato forum per lo scambio di idee tra i responsabili delle politiche europee e gli esecutori nel settore della privacy e della protezione dei dati. All'evento sono intervenuti, oltre il Prof. Dr. **Udo Helmbrecht,** altre personalità di rilievo come **Giovanni Buttarelli**, Garante europeo della protezione dei dati.

“L’UE ha aperto un nuovo capitolo non solo per la protezione dei dati, ma anche per la sicurezza delle infrastrutture critiche, ha dichiarato Buttarelli. *“Nell’Unione europea, tutte le DPA, non solo alcune di loro, devono collaborare con l’ENISA e gli esperti di sicurezza delle informazioni per implementare la sicurezza in base alla progettazione, poiché la cybersecurity non consiste più in una serie di misure difensive.”*

L’intelligenza artificiale in aiuto della privacy

Spazio anche all’utilizzo dell’intelligenza artificiale, tra le tematiche discusse durante l’evento, e come può rappresentare uno strumento utile per la protezione della privacy e dei dati personali, aumentando la capacità di un sistema di resistere agli attacchi informatici.

“*Grazie all’intelligenza artificiale è possibile analizzare una grande mole di dati, con positive ricadute per la privacy*“, ha spiegato **Maurizio Naldi**, presidente del Forum annuale sulla privacy di quest’anno, che insegna sicurezza informatica all’Università di Roma Tor Vergata e alla **Lumsa** di Roma. “*I cosiddetti sistemi di machine learning possono, infatti, individuare facilmente eventuali anomalie nell’accesso ai sistemi informatici*“, ha chiarito l’esperto.

“*Spronato dalla ricerca di una migliore protezione della privacy, il mio gruppo di ricerca sulla sicurezza informatica e la protezione dei dati presso l’Università di Roma Tor Vergata ha studiato il progetto di algoritmi innovativi di vero anonimizzazione,* ha continuato Naldi. *“Utilizziamo tecniche di elaborazione del segnale per preservare*

l’accuratezza statistica del primo e del secondo ordine nella risposta alle query del database, ma non rilasciare alcuna informazione riguardante le persone specifiche presenti nel database. Tali metodi rappresentano un significativo passo avanti nel conciliare la ricerca di anonimato e utilità di dati allo stesso tempo, che è un problema fondamentale nella ricerca attuale sulla protezione dei dati “.

https://www.key4biz.it/helmbrecht-enisa-implementare-il-gdpr-la-vera-sfida-per-la-cybersecurity/261810/