Incontro sul tema ‘Privacy e Consapevolezza’. Roma, 28 giugno 2019

GDPR e Privacy:

Consapevolezza e OpportunitàPresentazione del volume di Nicola Fabiano

28 Giugno 2019

Ore 10:00 – 13:30
Sala Conferenze, Camera dei Deputati

Via del Parlamento, 9 Roma

Confronto e approfondimento sui temi della protezione dei dati in occasione della presentazione del libro “*GDPR e Privacy: Consapevolezza e Opportunità*” di **Nicola Fabiano**, Presidente dell’Autorità Garante per la protezione dei dati di San Marino.

Parteciperanno al dibattito rappresentanti delle istituzioni ed esperti in un momento significativo per l’intero settore: ad un anno dall’entrata in vigore del **GDPR** e pochi giorni dopo la nomina del nuovo Collegio del Garante, ma con uno sguardo al futuro tecnologico ed alla evoluzione della cornice normativa tra diritti della persona, mercato e dinamiche internazionali.

AGENDA

Interventi

- Avv. **Nicola Fabiano**, Presidente dell’Autorità Garante

per la protezione dei dati personali di San Marino
- Avv. **Filippo Bianchini,** Avvocato
- On. **Carla Giuliano,** Deputato M5S
- Avv. **Carolina Scarano,** Componente CNF
- Dott.ssa **Nadia Arnaboldi,** Data Protection Expert, FIP, CIPP/E,CIPP/US,CIPM
- Avv. **Stefano Mele,** Partner – Carnellutti Studio Legale Associato
- Dott. **Giovanni Buttarelli,** Garante Europeo per la protezione dei dati (EDPS)
- *Modera*: Dott. **Raffaele Barberio**, Presidente Privacy Italia

Accesso riservato previa registrazione, fino ad esaurimento posti.

Per informazioni: info@privacyitalia.euAgli uomini è richiesto di indossare la giacca.

https://www.key4biz.it/incontro-sul-tema-privacy-e-consapevolezza-roma-28-giugno-2019/261805/

Amid Privacy Firestorm, Facebook Curbs Research Tool

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ZNGaLJUpUMc/amid-privacy-firestorm-facebook-curbs-research-tool

---

Surveillance-Savvy Hong Kong Protesters Go Digitally Dark

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/uvDVML8Xrks/surveillance-savvy-hong-kong-protesters-go-digitally-dark

---

Telegram Hit by Cyber-attack, CEO Points to HK Protests, China

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/L0KuRpUD2XY/telegram-hit-cyber-attack-ceo-points-hk-protests-china

---

Riconoscimento facciale, attacco hacker alla frontiera Usa. Rubate 100mila foto

Come non detto. Il dibattito sull'utilizzo della tecnologia per il riconoscimento facciale da parte delle forze dell'ordine americane è più acceso che mai.

Qualche ora fa il **Washington Post** ha diffuso la notizia di un

attacco hacker ha preso di mira un contractor della **Us Customs and Border Protection (Cbp)**, la principale agenzia Usa per la sicurezza delle frontiere, in servizio di controllo doganale e di transito presso i varchi di confine nazionale. Secondo le stime sarebbero coinvolte 100.000 persone da questo attacco informatico.

I rischi legati alla sicurezza del riconoscimento facciale

La società hackerata (un'azienda terzista) aveva archiviato i dati raccolti dalla Cbp, ovvero le informazioni personali dei viaggiatori, comprese le foto, i passaporti, le impronte digitali.

L'agenzia americana è venuta a conoscenza del 31 maggio che il subappaltatore aveva trasferito le immagini sulla sua rete. Il CBP non ha dichiarato quando la società ha trasferito le fotografie o quando si è verificato l'attacco informatico.

Il CBP aveva raccolto le immagini dei viaggiatori negli aeroporti e ai valichi di frontiera. Ha anche iniziato a utilizzare il riconoscimento facciale per identificare i viaggiatori, compresi quelli che cercano di entrare illegalmente nel paese.

L'attacco informatico si è verificato proprio mentre "*La Cbp sta espandendo il suo enorme apparato per il riconoscimento facciale e per la raccolta di informazioni sensibili dei viaggiatori, come le informazioni sulle targhe o gli identificatori sui social media*", ha denunciato **Neema Singh Guliani,** dell'American Civil Liberties Union (Aclu). "*Il modo migliore per evitare questo tipo di violazioni* – ha aggiunto – *è non raccogliere ed archiviare questi dati*".

Facial ID: un problema di privacy

Negli Usa, l’uso del riconoscimento facciale da parte delle agenzie governative, sta sollevando nuove domande sulla privacy e sulla sicurezza dei dati. Ieri abbiamo dato la notizia del lancio di un nuovo sito chiamato AirlinePrivacy.com ad opera di un gruppo di attivisti della privacy, che mostra agli utenti quali compagnie aeree utilizzano il riconoscimento facciale per verificare l’identità dei passeggeri prima dell’imbarco in aeroporto.

Il progetto, nato a difesa e tutela dei diritti dei viaggiatori, aiuta inoltre i clienti a prenotare voli direttamente con compagnie aeree che non utilizzano questo tipo di tecnologie invasive.

Lo scorso maggio la città di **San Francisco** ha votato per metterne al bando l’utilizzo da parte della polizia. E’ la prima città Usa ed altre municipalità americane stanno pensando di seguirne le orme.

Per approfondire

https://www.key4biz.it/riconoscimento-facciale-attacco-hacker-alla-frontiera-usa-rubate-100mila-foto/261291/

Banca dati nazionale del “Dat”, via libera del Garante privacy

È arrivato oggi il via libera definitivo da parte del **Garante privacy** al decreto proposto dal **Ministero della Salute** per l'istituzione della "***banca dati nazionale delle Disposizioni anticipate di trattamento (Dat)***", che poi è il noto argomento del "***testamento biologico***", tramite cui si consente alla persona di stabilire in anticipo "***i trattamenti sanitari ai quali intende essere sottoposta nel caso di sopravvenuta incapacità ad autodeterminarsi***".
Un tema estremamente delicato, che tocca principi di fede e laici allo stesso tempo, e che necessita di essere normato e regolamentato. Ministero e Garante lo hanno affrontato, rispettivamente istituendo e approvando la banda dati, e soprattutto con il loro lavoro hanno favorito la costituzione di "*un deposito unico nazionale di tali dichiarazioni*" (la banca appunto), seppure rilasciate su base volontaria, costantemente aggiornato e monitorato, "*con la possibilità di un accesso tempestivo alle stesse dichiarazioni da parte del personale medico in caso di necessità*".

Il funzionamento della banca dati
Al suo interno, si legge nella nota del Garante, "*saranno raccolte, con il consenso della persona che si è avvalsa del testamento biologico, le copie delle dichiarazioni, i successivi aggiornamenti, nonché la nomina e la revoca dell'eventuale fiduciario, anche di coloro che non sono iscritti al servizio sanitario nazionale*".
I dati saranno conservati per 10 anni dal decesso dell'interessato e ad essi potranno accedere il medico, che ha in cura il paziente incapace di esprimere la propria volontà, e il fiduciario, se nominato.
La banca dati, è spiegato nella nota del Garante, sarà alimentata dagli ufficiali di stato civile comunali, dai notai e dal responsabile dell'Unità organizzativa competente delle Regioni che abbiano predisposto il servizio, presso i quali

sono depositati gli “originali” delle Dat.
Tali soggetti, potranno trasmettere copia della Dat alla banca dati nazionale mediante un modulo elettronico, le cui specifiche tecniche sono definite in un disciplinare allegato al decreto.

Le modifiche al testo e la conformità alla privacy
Il via libera del Garante è però subordinato ad alcune azioni richieste per modificare il testo dello schema di decreto, “*per renderlo pienamente conforme alla normativa sulla protezione dei dati*”.
In particolare, in attesa della realizzazione della banca dati nazionale, “*il Garante ha chiesto maggiori tutele per quanto riguarda le modalità di accesso alle Dat, da parte del medico che ha in cura l’assistito o del fiduciario, come pure la corretta individuazione dei soggetti, che in qualità di titolari del trattamento, sono legittimati a trasmettere le Dat alla banca dati*”.
Ulteriori richieste al Ministero, già comunicate in precedenza, sono: la comunicazione all’interessato, che ne abbia fatto richiesta, dell’avvenuta acquisizione della documentazione nella banca dati nazionale; per quanto riguarda i tempi di conservazione, la cancellazione dei dati trascorsi dieci anni dal decesso del dichiarante.
Al Ministero il compito ora di individuare “*modalità più rispettose della disciplina sulla riservatezza*” per fornire al medico e al fiduciario “*le informazioni circa l’esistenza della dichiarazione ed il luogo dove la stessa è conservata*”.

https://www.key4biz.it/banda-dati-nazionale-del-dat-via-libera-del-garante-privacy/260879/

Top Russian Internet Firm Reportedly Under Pressure on Data

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/CfSn3eHOWNA/top-russian-internet-firm-reportedly-under-pressure-data

---

Aussie Police Raid Journalist’s Home Over Secret Spying Report

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/5UTOajUhqjI/aussie-police-raid-journalists-home-over-secret-spying-report

---

Apple Unveils Privacy-Focused Authentication System

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/1gTPM6rW_pQ/apple-unveils-privacy-focused-authentication-system

Telemarketing, Garante Privacy: “Reset di tutti i consensi. Si parte da zero con il nuovo registro opposizioni”

Si parte da zero. Resettare tutti i consensi, da chiunque effettuati, manifestati prima dell’entrata in vigore delle nuove regole per il funzionamento del Registro pubblico delle opposizioni (**Rpo**): questa è la richiesta principale e rivoluzionaria richiesta dal Garante della Privacy al Ministero dello Sviluppo Economico (**Mise**) che ha affidato il registro pubblico delle opposizioni alla **Fondazione Ugo Bordoni**.

Dunque è un sì condizionato quello dell’Autorità garante per la protezione dei dati personali alla riforma del Rpo, a cui ora possono iscriversi gli utenti che non intendono ricevere offerte promozionali, né sul telefono fisso né sul cellulare, né tramite la posta cartacea: queste ultime due modalità sono state inserite nelle nuove regole.

Dunque un bel passo avanti. Prima avrebbero potuto iscriversi al registro pubblico delle opposizioni al massimo 13 milioni di italiani (i soli possessori del telefono fisso) ora la platea, che non vuole essere raggiunta da telefonate o posta cartacera (tranne i volantini) per finalità pubblicitarie, può raggiungere oltre 117 milioni di utenze telefoniche – numeri fissi e cellulari.

Tuttavia, secondo il Garante Privacy, le nuove regole

necessitano ancora di migliorie.

L’Autorità, infatti, per rendere il regolamento pienamente conforme alla normativa sulla protezione dei dati personali e realmente effettive le garanzie per gli utenti, ha fornito al Mise ulteriori indicazioni.

- In primo luogo, come detto, il Garante ritiene che sia necessario precisare ulteriormente che l’iscrizione al Registro comporta automaticamente l’opposizione a tutti i trattamenti a fini promozionali, da chiunque effettuati, con la revoca anche dei consensi manifestati in precedenza. Su questo specifico punto il testo va quindi emendato eliminando ogni riferimento alle categorie merceologiche degli operatori che potrebbero generare dubbi interpretativi e alimentare il contenzioso.
- L’Autorità chiede, inoltre, di valutare l’opportunità che nel Rpo possano confluire tutti gli indirizzi postali indicati dai contraenti, anche quelli non presenti negli elenchi telefonici.
- Il Garante, infine, per rendere più esplicito l’obbligo della norma ed evitare comportamenti non corretti, suggerisce al Mise di prevedere in caso di illeciti, una responsabilità della società *“non derogabile contrattualmente in concorso o in solido”* con i call center che hanno effettuato la chiamata promozionale.

Telemarketing, Garante Privacy: “Reset di tutti i consensi. Si parte da zero con il nuovo registro opposizioni”