Hackers Can Bypass macOS Security Features With Synthetic Clicks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/CtexZakLZlQ/hackers-can-bypass-macos-security-features-synthetic-clicks

---

Amazon Digital Assistant Alexa Gets New Skill: Amnesia

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/5VPtA3FSxFc/amazon-digital-assistant-alexa-gets-new-skill-amnesia

---

ProtonMail Accused of Voluntarily Helping Police Spy on Users

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/edxKWH85J9k/protonmail-accused-voluntarily-helping-police-spy-users

Telecamere obbligatorie in asili e case di cura, via libera dal Senato

L’obbligo di installare telecamere “in tutte le aule” delle scuole dell’infanzia e “in tutte le strutture” di assistenza e cura di anziani e disabili è stato approvato, ieri, dal Senato. La norma *“Sistemi di videosorveglianza a tutela dei minori e degli anziani”* è contenuta in un emendamento, inserito nel decreto Sblocca-cantieri, presentato in veste assolutamente trasversale, portando la firma dei senatori di **Lega**, **M5S**, **Partito Democratico** e **Forza Italia.** Per diventare legge occorre l’approvazione anche della Camera.

La proposta assegna al ministero dell’Interno una dotazione di 5 milioni per il 2019 e 15 milioni per ogni anno dal 2020 al 2024: serviranno ai Comuni per installare apparecchiature finalizzate alla conservazione delle immagini per tre anni. Altrettanti ne vengono stanziati per fornire gli stessi strumenti alle “strutture socio-sanitarie e socio-assistenziali a carattere residenziale, semiresidenziale o diurno”.

L’obbligo, la novità rispetto alle precedenti proposte di legge

La novità, rispetto alle altre proposte di legge sull’installazione della videosorveglianza in asili e case di cura, è l’obbligo, e non più l’azione facoltativa. E proprio

l’obbligo ha suscitato i rilievi del Garante Privacy. Infatti Antonello Soro, nell’ultima audizione svolta al Senato sulle misure di prevenzione di maltrattamenti a danno di minori, anziani e disabili nelle strutture pubbliche e private ha sottolineato, tra l’altro, che sarebbe difficile ritenere conforme al principio di proporzionalità l’obbligo di sottoposizione costante a videosorveglianza di tutto il personale educativo e, per altro verso, di tutti i bambini presenti tanto negli asili nido quanto nelle scuole materne del Paese, a prescindere dall’effettiva sussistenza di rischi specifici (avrebbe poco senso ad esempio per le scuole con aule vetrate). Per le strutture di cura vale la stessa considerazione ai fini della proporzionalità del trattamento, benché la videosorveglianza sia lì subordinata al consenso delle persone riprese, che tuttavia è difficile possa sempre ritenersi realmente libero e, quindi, valido, tanto più rispetto ai dati inerenti la condizione di salute.

https://www.key4biz.it/telecamere-obbligatorie-in-asili-e-case-di-cura-via-libera-dal-senato/260020/

Apple e Google si sfidano a ‘colpi’ di privacy, perché è diventata più importante di software e hardware

“Per Apple la tutela dei dati personali non è un lusso riservato a pochi”. Lo ha detto **Craig Federighi**, a capo della divisione software di Cupertino, in un’intervista all’*Independent* in cui ha risposto alla critica lanciata venti

giorni fa dal Ceo di **Google**, **Sundar Pichai**.

In un intervento sul *New York Times*, Pichai aveva scritto che *“la privacy non può essere un bene di lusso offerto solo alle persone che possono permettersi di comprare prodotti e servizi costosi”.* La frase era stata interpretata come una stoccata all’indirizzo di **Apple**, che ora con Federighi ha rispedito al mittente la frecciatina.

Craig Federighi, capo divisione software – Apple
“Da un lato è gratificante” vedere che altre compagnie, *“negli ultimi mesi”,* si sono impegnate sulla privacy, ma il tema è *“più profondo”,* e non *bastano “un paio di mesi e un paio di comunicati stampa”* per affrontarlo, ha detto Federighi. *“Bisogna guardare fondamentalmente alle culture della compagnia, ai valori e al modello di business. E queste cose non cambiano da un giorno all’altro”.*

Infatti, non sono di default le ultime modifiche annunciate da Google per proteggere i dati degli utenti, come la possibilità di cancellare i dati di navigazione sul web e su Google Maps, *“ma gli utenti devono dedicare tempo e concentrazione alle modifiche. E sappiamo che spesso non ci si mettono nemmeno”,* fa notare il *Corriere della Sera a* **Kent Walker**, vicepresidente per gli affari globali di Big G, che risponde così: *“È vero, funziona così. Stiamo cercando un equilibrio fra le diverse esigenze. Le persone trovano utile che Google Maps sappia dove sono la loro casa e il loro ufficio, ma devono poter decidere altrimenti. L’obiettivo è fornire prodotti di qualità con sempre meno dati possibili”.* Meno dati, dunque, ma sempre nostri dati personali e big data su cui si fonda il business di Google, ma anche di Facebook&Co.

Apple, infine, ha sottolineato, che vuole portare i sui prodotti al più alto numero di persone possibile, e questi prodotti *“certamente non sono solo di lusso. Crediamo che una bella esperienza di prodotto sia qualcosa che tutti dovrebbero avere, e quindi aspiriamo a svilupparla”.*

Perché ora Apple e Google (e anche Facebook) si sfidano a “colpi” di privacy e non più a chi ha realizzato lo smartphone con le “migliori prestazioni di sempre” o del software più utile per il lavoro e la vita privata? Perché la protezione dei dati è diventata, finalmente, grazie al **GDPR**, il valore aggiunto che guida il consumatore alla scelta. La privacy oggi viene prima delle caratteristiche del software e dell’hardware. E Apple l’ha capito prima di tutto. Basta guardare la sua maxi-pubblicità, al Ces di Las Vegas, sul padiglione di Google e sul suo smart speaker Google Home: *“Quello che succede sul tuo iPhone resta sul tuo iPhone*”, con richiamo al motto *“What happens in Vegas, stays in Vegas”.*

> *Apple e Google si sfidano a ‘colpi’ di privacy, perché è diventata più importante di software e hardware*

Il GDPR compie 1 anno, perché il bilancio è (quasi) un successo

Volendo redigere un bilancio del Regolamento 2016/679 ad un anno dalla sua piena efficacia, occorre distinguere due

diversi punti di vista.

Se si fa riferimento alla conoscenza, all'interesse da parte dei titolari del trattamento, o alla "domanda di privacy" dei soggetti interessati, sicuramente si può togliere il "quasi" del titolo e considerare il Regolamento un successo.

Se però ci si pone dal punto di vista della sua effettiva, corretta implementazione nelle attività di trattamento dei dati personali da parte dei Titolari, la strada per la piena affermazione della disciplina appare ancora lunga. Questo in particolare se poniamo l'attenzione ai motivi di tale improvviso, e sotto certi punti di vista inaspettato, interesse sulla materia.

Infatti, il primo "motore" che ha fatto muovere la "macchina privacy" nel nostro Paese è stato sicuramente la paura della sanzione: i famosi 10 o 20 milioni di euro che, secondo i "terroristi privacy", si sarebbero applicati indiscriminatamente a tutti coloro che usavano non correttamente dati personali, singolo dentista o grande azienda. Paura che, nell'affanno dell'ultimo momento utile, poche settimane prima del 25 maggio dell'anno scorso, ha condotto ad un esponenziale aumento degli adeguamenti alle importanti norme (anche se in genere cercando di adempiere a meno obblighi possibile, nel minor tempo, ed al più basso costo).

La seconda ragione per cui è aumentata l'attenzione probabilmente è stata la novità della figura del Responsabile della protezione dei dati personali: il famoso DPO. Nuovo "attore" del "sistema privacy" che, nonostante sia stato inizialmente identificato con l'intera disciplina (portando, una volta nominato, molti titolari a considerare erroneamente raggiunto l'obiettivo adeguamento, un po' come in passato era

successo con il DPS, il documento programmatico sulla sicurezza), ha contribuito in maniera sostanziale al successo del Regolamento. La presenza infatti di numerosissimi Responsabili (si registrano oggi più di 40.000 DPO), a parte il lavoro svolto nell'ambito della struttura del titolare che ha proceduto alla nomina, ha fatto nascere un peculiare fenomeno: la richiesta del requisito dell'adeguamento, o di elementi di esso, agli altri titolari con cui il suo entra in contatto per porre in essere, proseguire, mantenere rapporti, commerciali o meno. Che quindi si sono trovati a loro volta costretti ad occuparsi della materia, andando a creare un imprevisto effetto domino che ha portato ad un'esigenza di adeguamento che negli anni scorsi era legata soprattutto al timore del controllo dell'Autorità: mentre, dopo il Regolamento, è spesso frutto della richiesta degli altri, partner, fornitori, futuri clienti

Ma il fatto che le ragioni principali del nuovo interesse per la disciplina sulla protezione dei dati personali siano state, da una parte, la paura della sanzione (e la fretta ad essa collegata), e, dall'altra, la nomina del DPO (scelti, altrettanto di fretta, sulla base di criteri più o meno validi, spesso quello del … "primo che passa" o dell'essere "certificato", ma con certificazioni che ufficialmente non esistevano), non manifestano ancora l'acquisizione di un'aumentata consapevolezza della situazione dei dati personali, della loro fondamentale importanza nella società dell'informazione (portata ad esempio da scandali come quello di Cambridge Analytica/Facebook), di una maggiore "maturità digitale" da parte degli interessati e di una crescente responsabilizzazione dei titolari. E dunque il giudizio torna ad essere quello di un "quasi" successo.

Ma, nonostante ciò, il bilancio è comunque positivo: volendo vedere il bicchiere mezzo pieno, oggi sicuramente si deve essere contenti del forte interesse che si registra per la normativa, della creazione di un vasto pubblico molto attento.

E adesso?

Adesso occorre soddisfare la richiesta di tale pubblico attento, che è quella di capire, di conoscere, di imparare (anche se poi purtroppo ancora in molti ritengono di avere altro di meglio da fare …). Situazione che deve portare allora a valorizzare sempre più la formazione come momento per aumentare la diffusione di una cultura del dato, della sua importanza, della necessità della sua protezione: ma allo stesso tempo come adempimento necessario di un'importante previsione normativa.

Ma è noto che oggi la formazione è un obbligo previsto dal Regolamento 2016/679 ?

Probabilmente no. Infatti, l'obbligo di formazione, fin dalla prima normativa sulla protezione dei dati personali nel nostro Paese (la "storica" legge 675/1996), in maniera assolutamente irrazionale non è quasi mai stato veramente sentito, capito. Questo in particolare dopo il D.L. 9 febbraio 2012 n. 5 (il cosiddetto decreto "Semplifica Italia", convertito nella legge 4 aprile 2012, n. 35) che, eliminando il D.P.S., aveva anche cancellato l'obbligo di formazione previsto al punto 19.6 del "Disciplinare tecnico in materia di misure minime di sicurezza" (l'allegato B al D.Lgs. 196/2003).

Oggi su questo tema il Regolamento 2016/679 ha (finalmente) portato significative novità grazie ad una serie di norme che, in maniera esplicita o indiretta, hanno dato rilevanza all'importante obbligo, strategico per una corretta protezione delle informazioni relative agli individui nelle attività di trattamento di qualsiasi titolare. In particolare si ricordano:

– l'**art. 39** rubricato "*Compiti del responsabile della protezione dei dati*" che, tra tali compiti, indica quello di "*sorvegliare l'osservanza del presente regolamento (…), la sensibilizzazione e* ***la formazione del personale che partecipa***

ai trattamenti e alle connesse attività di controllo";

– l'**art. 47** "*Norme vincolanti di impresa*" il cui par. 2 lett. *n*) dispone che le norme applicabili ai gruppi d'impresa che trattano dati in più Stati dovranno specificare "***l'appropriata formazione in materia di protezione dei dati*** *al personale che ha accesso permanente o regolare ai dati personali*".

mentre diverse altre norme, pur non utilizzando direttamente il termine "formazione", si riferiscono a concetti con essa correlati, come quello di "istruzione": così ad esempio

– l'**art. 29** ("*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali* ***non può trattare tali dati se non è istruito in tal senso dal titolare…***"), e

– l'**art. 39** ("*il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se* ***non è istruito in tal senso dal titolare del trattamento…***").

Più in generale a parte le indicate norme, alla luce della diversa impostazione della disciplina stabilita dal Regolamento 2016/679, si deve considerare la formazione di tutti coloro che entrano in contatto con dati personali, in nome e per conto del titolare, un elemento fondamentale per la costruzione della sua ***accountability***

Quindi problema risolto?

Purtroppo, ancora no. La formazione infatti, almeno nella mia esperienza, pur aumentata in quantità, talvolta anche in qualità, non ha ancora un'affermazione netta, non ultimo a livello di provvedimenti dell'Autorità: portando come conseguenza la mancata consapevolezza culturale dell'importanza del dato, e della necessità della sua tutela,

di cui si è parlato sopra.

E allora che fare?

Gli interpreti, i consulenti, gli esperti, i DPO, …, dovrebbero cercare di rendere consci i titolari dell'importanza della formazione nelle proprie strutture, per i propri incaricati e responsabili dell'attività di trattamento.

Ma certo non sarebbe male che l'Istituzione, l'Autorità Garante, sottolinei in maniera più … "convinta" l'importanza dell'obbligo, e del suo adempimento. E magari anche l'istituzione più "operativa", la Guardia di Finanza porti l'attenzione ispettiva anche all'adempimento di questo fondamentale adempimento … soprattutto nel nostro Paese, così lontano da un approccio culturale alle nuove tecnologie dell'informazione e della comunicazione. Per consentire di rilevare, al prossimo bilancio nella primavera del 2020, il pieno successo del Regolamento europeo 2016/679 e la piena affermazione della disciplina per la protezione dei dati personali.

https://www.key4biz.it/il-gdpr-compie-1-anno-perche-il-bilancio-e-quasi-un-successo/259529/

First American Financial Exposed Millions of Sensitive Documents

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Yj8JjOe

9o00/first-american-financial-exposed-millions-sensitive-documents

---

Georgia Supreme Court Rules that State Has No Obligation to Protect Personal Information

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/GEarvB5i9a8/georgia-supreme-court-rules-state-has-no-obligation-protect-personal-information

---

Assange Charged With 17 New Counts Under Espionage Act

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/bQ_U8n6GPyc/assange-charged-17-new-counts-under-espionage-act

---

Amazon Shareholders Support Selling Face Recognition Tech to Police

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/dVjeih_GbGA/amazon-shareholders-support-selling-face-recognition-tech-police