Facebook denuncia NSO Group per gli attacchi agli utenti Whatsapp

Ott 30, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, Privacy, RSS, Scenario 0

L'azienda di Zuckerberg porta NSO Group in tribunale. Avrebbero usato lo zero-day di Whatsapp per colpire 1.400 utenti con il loro spyware Pegasus.

Quando lo scorso maggio è comparsa una grave vulnerabilità zero-day di **Whatsapp**, il nome di **NSO Group** ha cominciato immediatamente a rimbalzare sui siti specializzati. Il sospetto, infatti, era che gli attacchi registrati da Whatsapp fossero opera di uno dei tanti "clienti" della società israeliana.

Ora il sospetto è diventato qualcosa di più concreto e **Facebook**, proprietaria di Whatsapp, ha deciso di **presentare una denuncia nei confronti di NSO Group** per la violazione di leggi degli Stati Uniti e della California.

NSO Group, di cui abbiamo parlato spesso su queste pagine, è un'azienda specializzata in sistemi informatici di sorveglianza (software di spionaggio) che vende a forze di polizia e servizi segreti di tutto il mondo.

L’azienda con sede a **Herzliya** è da tempo al centro di polemiche. Come riportato in più occasioni da associazioni per la difesa dei diritti umani come la canadese **Citizen Lab**, NSO Group è sospettata di fornire i suoi software spia anche a regimi dittatoriali e a governi che utilizzerebbero i suoi software per spiare giornalisti, avvocati dei diritti civili, dissidenti politici e attivisti.

Il suo best-seller è **Pegasus**, un trojan per Android e iOS in grado di tracciare i dispositivi tramite GPS, intercettare il traffico telefonico come quello Internet o utilizzare il microfono per spiare a distanza il possessore del telefono.

Stando a quanto riportano in un report gli attivisti di Citizen Lab, gli attacchi dello scorso maggio agli utenti di Whatsapp avrebbe avuto proprio lo scopo di installare il trojan di NSO Group sugli smartphone di **centinaia di esponenti della società civile** finiti nel mirino di uno dei tanti clienti “impresentabili” dell’azienda.

Come si legge nella denuncia inoltrata da Facebook, le vittime degli attacchi (in tutto 1.400) sono cittadini del Bahrein, dell’Arabia Saudita e del Messico.

La vulnerabilità utilizzata per colpire i dispositivi era terribilmente efficace: consentiva infatti di installare in remoto il trojan semplicemente avviando una videochiamata Whatsapp. **Per avviare l'esecuzione di codice non era nemmeno necessario che la vittima rispondesse alla chiamata**.

Il cuore della denuncia riguarda la violazione di una serie di normative (prima tra tutte il **Computer Fraud and Abuse Act**) e delle condizioni di utilizzo di Whatsapp.

La battaglia legale, come già accaduto in passato, si combatterà sul livello di responsabilità di NSO Group, che invariabilmente sostiene di non essere responsabile per eventuali utilizzi "inappropriati" dei suoi strumenti di spionaggio. **Questa volta, però, l'azienda israeliana non si trova di fronte la solita associazione per i diritti civili, ma uno dei giganti del Web.**

Non solo: a collegare l'azienda israeliana agli attacchi sarebbero alcuni elementi che smentiscono la "neutralità" che NSO Group sbandiera invariabilmente. Prima di tutto i tecnici di Whatsapp avrebbero individuato alcuni server utilizzati per

portare gli attacchi, che risulterebbero essere stati usati in passato da NSO Group. **In secondo luogo, gli stessi account Whatsapp utilizzati per colpire le vittime sarebbero collegati direttamente all'azienda israeliana**.

Insomma: le solite tesi difensive di NSO Group in questo caso rischiano di essere ben poco efficaci e l'intera vicenda promette di riservare non poche sorprese.

Condividi l'articolo

Si spacciano per Fancy Bear per ricattare le aziende

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/30/facebook-denuncia-nso-group-per-gli-attacchi-agli-utenti-whatsapp/

'La privacy negli studi professionali', il nuovo ebook per la cultura della privacy

Il **27 Aprile 2016** la **Commissione Europea** ha presentato il **Regolamento 679/2016** per l'aggiornamento della normativa concernente la tutela delle persone fisiche con riguardo al

trattamento dei dati personali e alla libera circolazione di tali dati.

Il Regolamento UE, essendo un atto self executive, ai sensi dell'art. 288 del Trattato sul funzionamento della Comunità Europea, è direttamente esecutivo e non necessita di recepimento da parte degli stati membri, cosicchè a decorrere dal 25 Maggio 2018, la normativa succitata è diventata immediatamente applicabile anche nello Stato italiano.

L'intero Regolamento 679/2016 è costellato da una costante dialettica tra tecnica e libertà, innovazione e diritti, iniziativa economica e garanzie. Significativa è l'esigenza di adeguamento della disciplina alla realtà nella sua evoluzione tecnologica.

Non vi è dubbio, infatti, che tanto le norme giuridiche quanto le norme tecniche formano ormai un sistema fortemente interconnesso rispetto a qualunque uso corretto dei dati , in particolare con riguardo alla legittimità della raccolta, uso e conservazione di quelli personali ed è altrettanto vero che redigere una collettanea che descriva il rapporto tra nuove tecnologie e mondo giuridico è una sfida che si presenta impossibile da vincere per il rischio che le nozioni espresse diventino obsolete al momento della pubblicazione.

Gli autori di questo ebook, **Giuseppe Miceli, Marco Miceli, Luca Malatesta,** propongono una pubblicazione snella, per avvicinare cittadini, professionisti o imprenditori, al mondo della protezione dei dati.

Il manuale nasce per iniziativa del *Consiglio dell'Ordine degli Avvocati di Roma* e l'Editore dell'ebook, **Fisco e Tasse**, **Gruppo Maggioli editore.**

https://www.key4biz.it/la-privacy-negli-studi-professionali-sc

arica-il-nuovo-ebook-per-la-cultura-della-privacy/277223/

Five months after returning rental car, man still has remote control

Enlarge / FordPass, offered by Ford Motor Company, is available for iOS and Android devices.

reader comments

100 with 81 posters participating, including story author

Share this story

When Masamba Sinclair rented a Ford Expedition from Enterprise Rent-a-Car last May, he was excited to connect it to FordPass. The app allows drivers to use their phones to remotely start and stop the engine, lock and unlock the doors, and track the vehicle’s precise location.

“I enjoyed it and logged into FordPass to be able to access vehicle features from my phone such as locking, unlocking, and starting the engine,” Sinclair, who is 34, told me. “I liked the idea of it more than I found it useful. The UI does look good and work well, though.”

Putting the onus on customers

Now, Sinclair's opinion of mobile apps in rental cars is decidedly less favorable. That's because, five months after he returned the vehicle on May 31, his app continues to have control over the vehicle. Despite multiple other people renting the SUV in the intervening months, FordPass still allows Sinclair to track the location of the vehicle, lock and unlock it, and start or stop its engine. Sinclair has brought the matter to Ford's attention, both through its website and multiple times
on Twitter. So far, Ford has done nothing to kill his access.

> *@Ford I can still track and unlock the Expedition that I rented last week via the FordPass app. HUGE safety concern for all future renters. I submitted a solution via Ford New Ideas to solve this and it was denied. THIS NEEDS TO BE FIXED pic.twitter.com/dcdfLlPceJ*
>
> *— Masamba (@MasambaS) June 4, 2019*

> *@Ford It's day 5 since I returned my rental and now someone else has rented it out. Do I need to start remotely unlocking it until they also start to complain? Please fix this! pic.twitter.com/S7UZVfIiFn*
>
> *— Masamba (@MasambaS) June 5, 2019*

> *.@Ford I returned this car two weeks ago and you've shown no willingness to allow rental companies to remove my access to unlock it and start the engine. Maybe I'll just start randomly unlocking it. pic.twitter.com/MrBVU68Jh4*
>
> *— Masamba (@MasambaS) June 14, 2019*

"All it took was me downloading the app and entering the VIN, then confirming connectivity through the infotainment system,"

Sinclair said late last week. “There MIGHT be a way to disassociate my phone from the car itself, but that hasn’t happened yet, and it’s crazy to put the onus on renters to have to do that. I have had no problems at all and have even unlocked the doors and started the engine when I could see that the vehicle was in the Missoula airport rental car parking lot.”

Below are a video and image Sinclair took documenting his control of the vehicle. He took them last week and in June, respectively:

[embedded content]
FordPass controls Enterprise rental for five months and counting

Enlarge / Screenshot of Sinclair’s phone after he unlocked the door. He performed the unlock when the vehicle was parked at an airport.
Masamba Sinclair

Tracking a vehicle daily

FordPass is offered by the Ford Motor Company and is available for both iOS and Android devices. It is one of several apps for connecting to Ford vehicles. The less-than-intuitive means for unpairing a vehicle and phone—not to mention the difficulty in knowing a device remains connected—represent a serious security and privacy risk, not just to renters, but to people buying a vehicle second hand.

While Ford said infotainment screens will indicate when a device is paired, it’s obvious that multiple Enterprise employees and renters have continued to miss the warning. Even now, after I discussed the problem with both Enterprise and Ford representatives, Sinclair’s access still hasn’t been revoked.

“I have been opening the app and tracking the vehicle almost every day to see if my access is still there, and sure enough, I can see exactly where my old rental, affectionately named “The Beast,” is at any given moment,” Sinclair said. “This means that I can not only find this rental car whenever I want, but I can also unlock the doors and help myself to anything inside.”

Enterprise spokeswoman Lisa Martini wrote in an email:

> *Several years ago, we implemented employee training on best practices for clearing data as part of our standard vehicle cleaning procedures. Additionally, we have information in our privacy policy and rental agreements to remind customers to remove their data when returning a car. We also work closely with the various automotive manufacturers to ensure we update and enhance our procedures as needed in response to new features and technologies that are added to vehicles. To that end, we understand the concerns this specific situation has raised and are actively working with Ford to implement protocols for customers who attempt to enable this feature on a rental car using their personal account.*

Renter beware

A copy of Sinclair’s rental agreement, however, shows that the reminder is vague and applies only to a customer returning a vehicle, who isn’t threatened by this security lapse. It doesn’t warn a customer upon renting. It states: “We are not responsible for any data that is left in the vehicle as a

result of your use. We cannot guarantee the privacy or confidentiality of such information, and you must wipe it before you return the vehicle to us."

I couldn't find any language instructing a customer to ensure devices belonging to previous customers who are no longer connected. And in any event, the warning applies only to people who have used FordPass. A new customer who doesn't use the app isn't subject to the warning at all.

I asked Martini for clarification. She didn't respond. She also didn't respond to a question asking how Enterprise enforces its employee best practices for clearing data during the cleaning process.

Ford spokesman Martin Gunsberg, meanwhile, said that FordPass provides two ways to unpair a vehicle from a phone. The first is to use the infotainment system settings to perform a master reset. The second is to open the FordPass app, select the vehicle details button, scroll to the bottom, and select "Remove Vehicle."

Gunsberg wrote:

> *We alert all drivers… FordPass enabled vehicles have a telltale in the top right hand corner of the SYNC screen if location sharing and remote start/stop, lock/unlock are active. These services can be manually turned off by pressing on the telltale and disabling these features. A pop-up will also alert the driver on each ignition on that location services are active if no known paired Bluetooth devices are detected.*
>
> …
>
> *Per the above response, SYNC will alert a new driver on ignition on that location services are active if no known Bluetooth device is connected. This alert is designed to occur before a new owner pairs their phone. At Ford*

> *dealerships, performing a Master Reset is part of a dealer's used car checklist prior to the sale of a vehicle.*

He also said that, when a FordPass user remotely tracks the vehicle location, the infotainment screen will display the words "GPS alert message." Additionally, he said, when connecting FordPass to a vehicle that's already paired to another phone, the new person receives an alert.

"They are prompted to conduct a Master Reset of the vehicle's SYNC settings," Gunsberg wrote. "We will also soon be adding regular communication to all FordPass users to remind them to conduct a Master Reset whenever they sell their vehicle."

It's not clear just how conspicuous the notice to perform a master reset is. The failure for Enterprise employees and customers to wipe the Ford Expedition for five months suggests it's easy to miss. Additionally, the communication to do a Master Reset that Ford plans to add is problematic since only the seller sees it. The person who is at risk from unauthorized access is the buyer. The seller faces no threat. What's more, the message "GPS alert message" seems vague.

It wouldn't be surprising if remote apps from other third-party developers of car manufacturers also maintain access long after they're rented or sold to new people. The lesson from Sinclair's experience is a classic renter- and buyer-beware. The experience is also pertinent to survivors of abusive relationships or stalkers. Before anyone uses a new car, they should learn how to perform a full factory reset of the infotainment system and ensure it's done.

https://arstechnica.com/?p=1592603

Garante privacy, nei primi 6 mesi del 2019 multe per 11 milioni di euro

Le attività ispettive del **Garante Privacy** programmate per il secondo semestre 2019, vanno avanti.

Gli accertamenti in corso (circa un centinaio fa sapere il Garante in una nota), svolti in collaborazione con il **Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di Finanza**, interessano innanzitutto i trattamenti di dati effettuati dagli istituti bancari, con particolare riguardo ai flussi verso l'anagrafe dei conti correnti bancari, i trattamenti di dati svolti dalle società che operano nel settore del food delivery e quelli effettuati dalle aziende che svolgono attività di marketing.

Sotto la lente del Garante anche altri delicati settori

Nel mirino del Garante sono inoltre coinvolti le banche dati di notevoli dimensioni degli enti pubblici e gli applicativi per la gestione delle segnalazioni di condotte illecite (c.d. whistleblowing); le attività di profilazione dei possessori di carte fedeltà; i trattamenti di dati svolti dagli intermediari che offrono servizi per la fatturazione elettronica. Particolare attenzione viene riservata anche alle società private che trattano dati personali in ambito sanitario.

I controlli si concentrano anche sul rispetto delle norme sull'obbligo dell'informativa e il consenso, e sulla durata della conservazione dei dati. Oltre alle ispezioni in programma nel secondo semestre, l'Autorità potrà disporre

ulteriori accertamenti d’ufficio a seguito di segnalazioni o reclami.

Il bilancio del primo semestre 2019 del Garante Privacy

Intanto per quanto riguarda il bilancio del primo semestre 2019, l’Autorità segnala l’iscrizione a ruolo di 779 contravventori che porterà ad una riscossione complessiva di circa **11 milioni di euro.**

A breve, poi fa sapere il Garante, si concluderà l’iter per l’iscrizione di altri 500 trasgressori. L’avvio della procedura esecutiva per un numero così rilevante di casi fa seguito alla scarsa adesione alla sanatoria introdotta dal d.lgs n. 101/2018: sugli oltre 1300 contravventori che rientravano nell’ambito di applicazione del decreto solo 88 si sono avvalsi di questa facoltà, versando un totale di 386.400 euro

Nel 2019 effettuate 65 ispezioni

Nei primi sei mesi del 2019, inoltre, il Garante dichiara che sono state realizzate 65 ispezioni, anche con l’ausilio della Guardia di finanza, che hanno interessato, tra l’altro, **call center, aziende di marketing, società che rilasciano Spid, grandi alberghi, banche dati di rilevanti dimensioni della Pa.**

Nello stesso periodo le entrate derivanti dall’attività sanzionatoria sono state pari a 1.222.955 euro e 86 sono state le ordinanze adottate, alcune relative a casi complessi riguardanti molteplici violazioni, per un totale di 3.250.390 euro.

https://www.key4biz.it/garante-privacy-nei-primi-6-mesi-del-2019-multe-per-11-milioni-di-euro/276888/

Privacy, scudo Ue-Usa: positivo il terzo riesame, coinvolte 5 mila imprese

Pubblicata la relazione sul **terzo riesame annuale dedicato al funzionamento dello scudo Ue-Usa per la *privacy***. I risultati sono stati giudicati positivi e il Report conferma che gli Stati Uniti garantiscono un adeguato livello di protezione dei dati personali trasferiti dall'Unione europea (Ue) verso le imprese partecipanti nell'ambito dello scudo per la *privacy*.

Dall'entrata in vigore dell'accordo, il 1° agosto 2016, fa sapere la Commissione europea, **oltre 5.000 imprese hanno assunto impegni pubblici e giuridicamente vincolanti per proteggere i dati trasferiti dall'Ue** conformemente ai principi dello scudo per la privacy.

"*Con la partecipazione di migliaia di imprese, **lo scudo per la privacy si è dimostrato un successo***", ha dichiarato in una nota **Věra Jourová**, Commissaria per la Giustizia, i consumatori e la parità di genere.
"*Il riesame annuale è uno strumento importante per accertare il suo funzionamento. Porteremo avanti il dialogo sulla diplomazia digitale con le nostre controparti statunitensi per potenziare lo scudo, anche per quanto riguarda la supervisione, l'applicazione e, a lungo termine, una maggiore convergenza dei nostri sistemi*".

Miglioramenti

Il terzo riesame rileva che il Dipartimento del Commercio degli Stati Uniti (*US Department of Commerce*) garantisce ormai una supervisione più sistematica in tema di dati personali, si legge in un comunicato della Commissione europea, "*per esempio effettuando controlli mensili su un campione di imprese per verificare il rispetto dei principi dello scudo per la privacy*".

La Commissione federale del commercio (*Federal trade commission* – Ftc) ha inoltre migliorato l'azione di contrasto nei confronti delle violazioni dello scudo per la privacy intervenendo in 7 casi, si legge nella relazione, mentre "*un numero crescente di cittadini dell'Ue fa valere i propri diritti nell'ambito dello scudo per la privacy e i pertinenti meccanismi di ricorso funzionano bene*".

Oltre alla nomina del mediatore permanente (ombudsman), sono stati coperti i due ultimi posti vacanti dell'Autorità per la tutela della vita privata e delle libertà civili (Privacy and civil liberties oversight board), garantendone così per la prima volta dal 2016 un organico completo.

Raccomandazioni

Nonostante i passi in avanti registrati, la Commissione europea ha invitato gli Stati Uniti ad adottare ulteriori concrete misure per rendere il funzionamento dello scudo ancora più efficace4 in termini di tutela della privacy.

Prima di tutto, "*il rafforzamento del processo di (ri)certificazione delle imprese desiderose di partecipare, abbreviando i tempi necessari, l'ampliamento dei controlli di conformità, anche relativamente alle false dichiarazioni di partecipazione al quadro, e lo sviluppo di ulteriori linee guida destinate alle imprese in materia di dati afferenti alle risorse umane*".

In più, è auspicabile che la Ftc "*intensifichi le indagini relative all'adempimento dei requisiti fondamentali dello scudo per la privacy e fornisca alla Commissione e alle autorità di protezione dei dati dell'Ue informazioni in merito alle indagini in corso*".

https://www.key4biz.it/privacy-scudo-ue-usa-positivo-il-terzo-riesame-coinvolte-5-mila-imprese/276627/

Adeguamento GDPR in Italia e in Europa, a Firenze il punto delle Autorità e dei giuristi

Autorità e giuristi si sono dati appuntamento a Firenze al Palazzo Incontri della **Fondazione Cesifin** per fare il punto sullo stato dell'adeguamento del **GDPR** in Italia e in Europa.

E' ormai dal 25 maggio 2018 che occorre confrontarsi quotidianamente con la rilevante riforma della privacy dettata dal Regolamento UE 679/2016 meglio noto come General Data Protection Regulation (GDPR).

Tante le novità introdotte: Principio di responsabilizzazione, Gestione e prevenzione del rischio, Valutazione Impatto Privacy, Data Protection Officer, Diritto all'oblio, Diritto alla portabilità dei dati, protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, responsabilità del titolare e responsabile del trattamento oltre a un robusto apparato sanzionatorio solo per fare alcuni cenni senza pretese di esaustività.

Il **GDPR** è affiancato, in Italia, dal "nuovo" Codice della

Privacy così come modificato a far data dal 19 settembre 2018 dal D.Lgs. 101/2018 che ha novellato il "vecchio" Codice.

Tuttavia, resta ancora da scrivere – per completare il quadro regolatorio – il fondamentale tassello della privacy digitale: è tempo di concludere anche tale processo di riforma che porterà al superamento della Direttiva 2002/58/CE (c.d. "**Direttiva *ePrivacy***").

Il convegno

Il Convegno promosso e aperto dalla relazione introduttiva del **Prof. Avv. Emilio Tosi** Direttore Esecutivo **DNT®** Diritto nuove tecnologie dnt® – studi giuridici per L'innovazione® – Professore Associato Abilitato di Diritto Privato nell'Università di Milano Bicocca, Managing Partner Tosi & Partners high tech legal® – ha registrato il tutto esaurito, espressione concreta del successo dell'iniziativa non solo tra gli addetti ai lavori – giuristi e Data Protection Officer – ma anche tra professionisti, e imprenditori.

Tra le Autorità presenti in sala oltre alla dott.ssa **Augusta Iannini**, Vice Presidente del Garante per la protezione dei dati personali, che ha tenuto una relazione introduttiva sul complesso caleidoscopio normativo italo-comunitario delineato dal GDPR e sulle più recenti iniziative del Garante, la prof.ssa **Maria Enza La Torre**, Consigliere della Corte di Cassazione, già Ordinario di Diritto Privato nell'Università di Messina, che ha illustrato ai presenti l'evoluzione giurisprudenziale più recente sui temi della tutela della riservatezza e in particolare commentato il recente arresto delle Sezioni Unite del 22 luglio 2019, n.19681 sul diritto all'oblio, oltre al Colonnello **Marco Menegazzo**, Comandante del Nucleo Privacy, che è intervenuto su temi della responsabilizzazione e delle verifiche ispettive della GdF.

Il convegno ha ottenuto il patrocinio istituzionale del **Garante per la protezione dei dati personali,** dell'**European Data Protection Supervisor UE, Privacy Italia.**

L'iniziativa di studi aderisce, inoltre, all'**European Cyber Security Month (ECSM)** che si svolge, ogni anno, nel mese di ottobre – con il supporto italiano del **CLUSIT** – per sensibilizzare istituzioni e cittadini sui temi della Cyber Security e della privacy digitale.

Focus sul GDPR

La Tavola Rotonda su Persona, riservatezza, protezione dati personali e GDPR nella società digitale – è stata moderata da **Raffaele Barberio** Presidente di Privacy Italia e ha coinvolto, oltre al promotore il prof. Tosi, **Guido De Vecchi –** DG Innovation Center Intesa Sanpaolo**, Vincenzo Franceschelli** – Università di Milano Bicocca**, Oreste Pollicino –** Università Bocconi, **Alberto M. Gambino – Università Europea di Roma, Carolina Perlingieri** – Università di Napoli, **Marco Menegazzo** – Gruppo Privacy GDF

Il Direttore del DNT® promotore dell'iniziativa scientifica ha aperto i lavori ricordando due punti fondamentali: la dimensione economica globale della società digitale e la conseguente vocazione transnazionale del GDPR alla luce dell'art. 3 che prevede un principio di applicazione territoriale esteso a tutti i soggetti, anche non stabiliti nella UE, che trattano dati di interessati UE; la natura di nuovo modello normativo, nuovo *legal benchmark* globale del GDPR: per una volta nella storia delle nuove tecnologie e della sua regolamentazione normativa è la vecchia Europa a tracciare la strada nei rapporti transatlantici con gli Stati Uniti.

Sui rapporti stretti tra persona, riservatezza e protezione dei dati nella società digitale Tosi ha dichiarato: "*Il titolo dell'odierno Convegno intende evocare la tensione evidente che*

intercorre tra istanze di tutela diritti fondamentali della persona – protetti, innanzitutto, dall'art. 2 della nostra Costituzione oltre che dal GDPR – e le esigenze contrapposte dei mercati digitali, che si fondano, sempre di più, sullo sfruttamento commerciale dei dati personali".

"Esigenze di tutela – ha spiegato Tosi – *che collidono con il fenomeno dell'economia della conoscenza, fondata sulla conoscenza dei nostri dati personali. I dati personali ormai costituiscono, a pieno titolo, il nuovo petrolio, inconsumabile e inesauribile, purché continuamente aggiornato, dell'economia digitale. Il substrato giuridico è, dunque, fondamentale per la governance del mercato digitale, per facilitare lo sviluppo economico, proteggere il soggetto debole di questo singolare rapporto asimmetrico – l'interessato dal trattamento – in ultima istanza la dignità personale. Emerge con tutta evidenza l'asimmetria di potere tra i soggetti del trattamento (Titolareinteressato) e la bontà di una lettura assiologica-costituzionale della tutela della riservatezza, della protezione dei dati personali e dell'identità che, attraverso il prisma delle fonti interne e comunitarie, consenta di dare piena efficacia a tali fondamentali diritti, offrendo un saldo appiglio per non soccombere di fronte alle plurime e cangianti pressioni mercatorie della società liquida digitale. Riflessi patrimoniali e asimmetria di potere che vengono colti anche nella recente decisione della Cassazione del 2 luglio 2018, n. 17178 – in relazione al caso di servizi informativi di un sito Internet condizionati a rilascio del consenso dell'interessato all'utilizzo dei dati personali per l'invio di messaggi pubblicitari da parte di terzi. La rilevanza patrimoniale del consenso informato al trattamento dei propri dati è, inoltre, plasticamente evidenziata dal comma 4 dell'articolo 7 del GDPR, secondo cui Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un*

servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".

"Senza evocare gli scenari futuristici delle impreviste evoluzioni della singolarità tecnologica, già ora Social Network, Cloud Computing, Smartphone, Smart Cars, Droni, Robot, Fintech, Blockchain, Internet of Things, Big Data e Artificial Intelligence costituiscono temibili variabili socio-economiche e tecnologiche che occorre disciplinare, con compiutezza bilanciando i contrapposti interessi in campo, per una piena tutela dei diritti fondamentali della persona", non ha mancato di osservare Tosi. *"Le predette variabili socio-economiche tecnologiche si intersecano sempre più significativamente con le nostre vite, dato che in concreto orientano decisioni personali e imprenditoriali oltre che scelte geopolitiche e strategiche degli Stati. Occorre, pertanto, scongiurare il progressivo, incontrollato e scarsamente trasparente, per non dire opaco, dominio dell'algoritmo, rischio denunciato dal giurista Frank Pasquale nel suo noto saggio Black Box Society del 2015: il controllo dei nostri dati personali elaborato dai software di gestione dei motori di ricerca, da sistemi esperti e intelligenze artificiali"*

In memoria di Giovanni Buttarelli

Il convengo si è concluso con il richiamo ai presenti della figura del compianto **Giovanni Buttarelli** European Data Protection Supervisor UE: "Avrebbe dovuto partecipare all'incontro di studi anche il Cons. Buttarelli che aveva già confermato la Sua presenza e che aveva anche curato la Postfazione della raccolta di studi Privacy Digitale- ventunesimo volume della Collana Diritto delle Nuove Tecnologie® – DNT® (Giuffrè Lefebvre 2019) curato da me– che oggi viene presentato proprio in occasione del IX Convegno DNT®", ha dichiarato il Prof. Avv. Emilio Tosi. *"Purtroppo, la*

notte dello scorso 20 agosto, il Presidente dell'European Data Protection Supervisor UE, valente magistrato e studioso dei temi privacy, ci lasciava improvvisamente. Ricordo di aver conosciuto Giovanni nel 1997, ormai un tempo lontano, quando giovanissimo magistrato, veniva chiamato ad esercitare le funzioni di primo Segretario Generale nella storica consiliatura del Garante per la Protezione dei Dati Personali presieduta dal Prof. Stefano Rodotà (1997-2005).

Nel corso degli anni, sino all'ultimo, Egli ha contribuito con perseveranza e convinzione a diffondere e far crescere, anche nella nuova dimensione globale della società digitale, la cultura della protezione dei dati personali e il rispetto dei diritti fondamentali. Anche per tale ragione, oltre che per l'amicizia e stima personale, si è deciso di dedicare alla sua memoria il IX Convegno DNT®", ha concluso Tosi.

https://www.key4biz.it/adeguamento-gdpr-in-italia-e-in-europa-a-firenze-il-punto-delle-autorita-e-dei-giuristi/276223/

Privacy bill would give FTC actual authority, land lying executives in jail

Enlarge / Sen. Ron Wyden questions witnesses during a Senate Intelligence Committee hearing on social media influence in the 2016 US elections in Washington, DC, on Nov. 1, 2017.

reader comments

43 with 32 posters participating

Share this story

Sen. Ron Wyden (D-Ore.) would like tech and data companies to mind their own business and get their noses out of yours. To that end, he has introduced a bill that would penalize them, potentially with jail time for executives, for not doing so.

The proposed bill (PDF), actually called the “Mind Your Own Business Act of 2019,” is in many ways an updated version of a discussion draft Wyden published last November.

The draft does not name any company specifically, instead focusing on the general concepts of personal data and company responsibility. That said, Wyden did name names in a statement, and Facebook is clearly front and center on his radar.

“Mark Zuckerberg won’t take Americans’ privacy seriously unless he feels personal consequences,” Wyden said. “A slap on the wrist from the FTC won’t do the job, so under my bill he’d face jail time for lying to the government.”

Not only do companies need to be more transparent and to give consumers more control, Wyden added, but also “corporate executives need to be held personally responsible when they lie about protecting our personal information.”

The proposal zeroes in on a few big challenges. First, consumers are tracked and monetized but do not have an effective way to control that tracking or to even know what’s done with the data collected from them. Second: businesses that siphon up and trade in consumer data have a terrible track record when it comes to securing that data and preventing unauthorized access. And third: the Federal Trade Commission, which is the closest thing we have to a privacy

regulatory body, is woefully underpowered and under-resourced for addressing the challenge.

Sen. Wyden's bill, then, would address those concerns by 1) imposing minimum privacy and security standards for user data, 2) increasing transparency for consumers to access their own data and learn what has been done with it, 3) creating steep penalties for companies that blow it, and 4) expanding the FTC's authority and resources so that it would be able to enforce those penalties. The bill would allow companies to charge for higher-privacy versions of services, but it would exempt from those fees anyone using a Lifeline subsidy (a small credit that low-income individuals and families can use to pay for phone or broadband services). This would be a gesture against reserving privacy as a luxury good.

Putting someone on the beat

The FTC recently established a small division dedicated to technology enforcement issues, but Wyden's proposal would beef it up substantially.

FTC chairman Joseph Simons has said several times this year that he feels his agency is hamstrung by its inability to impose stiff penalties for first-time violations of the FTC Act or of the Safeguards Rule, which requires financial institutions to take special care with consumer data.

"The CFPB and the states were able to obtain civil penalties for this massive breach by a major financial institution. The FTC could not," Simons said in a July press conference explaining the agency's settlement with Equifax. "Fortunately, other agencies were able to fill in the gap this time. That will not always be the case, which sends the wrong signal regarding deterrence."

A few days later, when discussing the $5 billion settlement between the FTC and Facebook, Simons again called on Congress

for a new bill. “We are a law enforcement agency without the authority to promulgate general privacy regulations,” Simons said at the time. “Our authority in this case comes from a 100-year-old statute that was never intended to deal with privacy issues like the ones that we address today.”

If Sen. Wyden’s bill were to become law, the FTC would gain 175 additional staff members to help enforce data and privacy standards—and the penalties could be steep. A first offense, which currently carries no fine, would cost a company up to 4% of its annual revenue. In the case of the Equifax data breach, for example, that would have been an additional $136 million to the FTC, on top of the existing $500 million agreement.

Corporate officers would also be held personally accountable for their company’s behavior. If a business, such as Facebook or Google, were found to be filing incorrect reports about privacy, executives would be subject to penalties equaling 5% “of the largest amount of annual compensation received during the previous 3-year period,” or $1 million, whichever is greater, and up to 10 years in prison.

That’s just for an “oops.” If those officers were found to have lied intentionally on those reports, the penalties jump up to 25% of compensation or $5 million, whichever is greater, and up to 20 years in prison.

The challenge

Nearly everyone with a stake in the matter, including politicians from both major parties, agree that we in the United States are badly overdue for some kind of update to privacy law and regulation. The questions of what such a law should cover, what it should allow, and who should benefit, however, are contentious at best.

More than 50 of the nation’s largest companies—including Amazon, AT&T, and Comcast, among dozens of others—in September

signed onto a letter (PDF) to Congress asking for federal privacy legislation.

The companies wrote:

> *We are committed to protecting consumer privacy and want consumers to have confidence that companies treat their personal information responsibly… We are also united in our belief that consumers should have meaningful rights over their personal information and that companies that access this information should be held consistently accountable under a comprehensive federal consumer data privacy law.*

The Electronic Frontier Foundation and other critics called the corporate campaign "disingenuous," saying it amounted to a "ploy to undermine real progress on privacy" being made at the state level nationwide.

The poster child for those state efforts is California's Consumer Privacy Act, which becomes effective in less than three months, on January 1. California's high population and influence as a tech center have in the past caused its privacy-related regulations to effectively become de facto national standards, and companies that rely on the ability to collect, remix, and exploit user data are not enthralled with that idea. They likely won't love Wyden's federal proposal, either, as it explicitly does not preempt states from setting their own, more stringent guidelines.

Beyond the issue of corporate money and corporate preferences, however, the greatest challenge to getting anything through Congress this decade is Congress. Astute observers may have noticed that the political process in Washington, DC, is somewhat acrimonious these days. Not only is there a significant partisan divide to contend with, but in the immediate sense, both chambers are occupied with questions such as "Can we keep this government funded past November, please?" and "Are we impeaching the president?"

That said, Wyden’s bill could easily become a template to which he and other senators return in future sessions of Congress, when conditions for making actual law may become more favorable.

https://arstechnica.com/?p=1587021

Telecamere nascoste per controllare i lavoratori, Soro: ‘Non può diventare prassi’

“*I controlli devono essere proporzionati e non eccedenti e la sorveglianza occulta non può diventare prassi ordinaria*“. Così il Garante Privacy, **Antonello Soro**, commenta così la sentenza della Corte di Strasburgo sulla presenza di telecamere nascoste nei luoghi di lavoro. “*La sentenza della Grande Camera della Corte di Strasburgo se da una parte giustifica, nel caso di specie, le telecamere nascoste, dall’altra conferma però il principio di proporzionalità come requisito essenziale di legittimazione dei controlli in ambito lavorativo*“, afferma Soro.

“*L’installazione di telecamere nascoste sul luogo di lavoro è stata infatti ritenuta ammissibile dalla Corte solo perché, nel caso che le era stato sottoposto, ricorrevano determinati presupposti: vi erano fondati e ragionevoli sospetti di furti commessi dai lavoratori ai danni del patrimonio aziendale, l’area oggetto di ripresa (peraltro aperta al pubblico) era alquanto circoscritta, le videocamere erano state in funzione per un periodo temporale limitato, non era possibile ricorrere*

a mezzi alternativi e le immagini captate erano state utilizzate soltanto a fini di prova dei furti commessi.

La videosorveglianza occulta – continua il Garante – *è, dunque, ammessa solo in quanto extrema ratio, a fronte di "gravi illeciti" e con modalità spazio-temporali tali da limitare al massimo l'incidenza del controllo sul lavoratore. Non può dunque diventare una prassi ordinaria.*

Il requisito essenziale perché i controlli sul lavoro, anche quelli difensivi, siano legittimi resta dunque, per la Corte, la loro rigorosa proporzionalità e non eccedenza: capisaldi della disciplina di protezione dati la cui "funzione sociale" si conferma, anche sotto questo profilo, sempre più centrale perché capace di coniugare dignità e iniziativa economica, libertà e tecnica, garanzie e doveri", conclude Soro.

Il Garante Privacy coglie occasione di commentare la sentenza della corte di Strasburgo per sottolineare ancora una volta, il suo parere contrario alla **Legge Concretezza** votata dal precedente Governo, ma mai attuata, che prevede l'installazione di telecamere di videosorveglianza, e contestualmente le impronte digitali per tutti i dipendenti della Pubblica Amministrazione.

Sia il ministro dell'Istruzione, Università e Ricerca Lorenzo Fioramonti, sia la ministra della Pubblica Amministrazione **Fabiana Dadone** hanno già dichiarato di voler abrogare la Legge.

https://www.key4biz.it/telecamere-nascoste-per-controllare-i-lavoratori-soro-non-puo-diventare-prassi/275492/

Come tutelare le infrastrutture critiche e come gestire i dati degli utenti con la blockchain

Quali misure adottare in caso di disastri naturali o causati dall'uomo; come tutelare le infrastrutture critiche nazionali e in che modo gli utenti, attraverso a una piattaforma basata sulla blockchain, possono gestire i propri dati personali, in caso di cessione a soggetti terzi. Questi sono i temi principali del workshop internazionale sulla Data Protection e sicurezza nelle situazioni di emergenza, che si terrà il 24 ottobre prossimo presso la sede dello studio legale di **E-Lex** (via dei Barbieri, 6 – Roma).

Giovanni Maria Riccio, professore di Diritto comparato all'Università di Salerno e socio dello studio legale E-Lex, ci spiega nel dettaglio i 4 progetti che saranno presentati nel corso del workshop.

Key4biz. ***Su quale tema verterà il workshop internazionale?***

Giovanni Maria Riccio. Il workshop è articolato in due

sessioni. Nella prima, dopo una mia breve introduzione, saranno presentati quattro progetti finanziati nell'ambito della misura **Horizon 2020**. Si tratta di quattro progetti; in tre di questi progetti, quale partner giuridico, è presente lo studio **E-Lex**. "*Assistance*" è una ricerca che si occupa delle misure da adottare in caso di disastri, causati dalla natura o dall'uomo: un tema, quindi, molto importante, perché spazia dai cambiamenti climatici, e gli effetti che tali cambiamenti determinano in termini di situazioni catastrofiche, al terrorismo, nazionale e internazionale. "*Defender*", invece, è un progetto focalizzato sulla tutela delle infrastrutture critiche, ossia di tutte quelle infrastrutture – dalle reti di telecomunicazioni, al sistema dei trasporti, ai servizi bancari – che consentono la 'sopravvivenza' di una Nazione. Aspetti analoghi sono affrontati anche da "*Faster*". Il quarto progetto presentato, "*PoSeID-on*", mira alla creazione di una piattaforma attraverso la quale, anche per mezzo dell'uso della blockchain, gli utenti possono monitorare la 'vita' dei propri dati personali, in caso di cessione di tali dati a soggetti terzi. È un progetto sicuramente molto interessante, al pari degli altri, anche perché prevede il coinvolgimento di società che trattano dati personali, che, aderendo alla piattaforma, dimostrano una sensibilità effettiva e non solo dichiarata alla problematica del trattamento dei dati personali.

Key4biz. ***Quali sono i progetti e il ruolo della Commissione in ambito privacy?***

Giovanni Maria Riccio. L'attenzione della Commissione in materia di data protection è altissima. I progetti finanziati da Horizon 2020, anche quando non sono direttamente connessi con l'ambito privacy, hanno quasi sempre un collegamento con tale materia, a dimostrazione della sua centralità in tutti i flussi economici e sociali. I progetti che saranno presentati

nel corso del workshop, come dicevo, spaziano in ambiti differenti: eppure non sfugge come un attacco a una infrastruttura critica – ad esempio, a un operatore di telefonia o a reti di comunicazione – potrebbe essere determinato proprio dalla necessità di sottrarre dati, non necessariamente di natura personale. Discorso identico potrebbe essere fatto per lo studio degli eventi catastrofici, che impongono di soffermarsi su misure di *disaster recovery* che consentano non solo l'operatività continua dei servizi intaccati, ma altresì il recupero dei dati che potrebbero andar persi.

Key4biz. ***Quali quelli in ambito security?***
Giovanni Maria Riccio. A questa domanda, risponderei a mia volta con un'altra domanda: esiste privacy senza security? A mio avviso, ma si tratta anche dell'impostazione che mi sembra sia adottata in tutte le linee di ricerca, sono due aspetti interconnessi. Non dimenticherei, peraltro, il ruolo che sta assumendo il dibattito su *ethics e data protection*: non è un caso che il **GDPR**, nel sancire i principi applicabili al trattamento dei dati personali, parli di liceità e trasparenza, ma altresì di correttezza. A questo principio, del resto, si ispirano anche tutte le misure finalizzate a minimizzare i rischi associati al trattamento dei dati personali, quali, a titolo esemplificativo, la progettazione secondo canoni di privacy by design e privacy by default.

Speaker

Manuel Esteve – Universitat Politècnica de València – Assistance: https://assistance-project.eu

Luca Del Pizzo, Ministero dell'Economia e delle Finanze – PoSeID-on: https://www.poseidon-h2020.eu

Giuseppe Caracciolo, KPRF – Faster https://www.faster-project.eu

Gabriele Giunta, Engineering – Defender http://defender-project.eu

Dibattito

Angelo Tofalo – Sottosegretario alla Difesa

Silvia Scarpa – Università di Roma Luiss Guido Carli

Luigi Carrozzi – Autorità Garante per la protezione dei dati personali

https://www.key4biz.it/come-tutelare-le-infrastrutture-critiche-e-come-gestire-i-dati-degli-utenti-con-la-blockchain/275429/

Dpo, online la piattaforma e-learning dell'Autorità Garante per la protezione dei dati personali

Un'occasione di formazione gratuita sui temi della protezione dei dati, con focus specifici su tutti gli aspetti del Regolamento UE 679/2016, dedicata ai Responsabili della Protezione dei Dati (**RPD**) operanti presso i soggetti pubblici. L'opportunità è offerta dal Garante per la protezione dei dati personali che, nell'ambito del progetto formativo transnazionale **T4Data**, ha realizzato oltre 30 webinar che sono da oggi disponibili su una piattaforma formativa e-learning

sviluppata ad hoc grazie alla collaborazione, per la parte tecnologica, del Politecnico di Milano.

La partecipazione al corso online, conformemente ai requisiti del progetto T4Data, è riservata esclusivamente ai RPD dei soggetti pubblici i cui nominativi sono stati comunicati attraverso la procedura attivata sul sito web istituzionale del Garante in base all'articolo 37, paragrafo 7. Per accedere ai webinar sarà sufficiente collegarsi all'indirizzo web https://www.t4data.gpdp.it e creare un account seguendo le indicazioni fornite sulla pagina di registrazione, che prevedono anche l'inserimento delle coordinate identificative del RPD fornite all'atto della comunicazione dei dati al Garante (numero di protocollo a 11 cifre indicato nella mail di conferma inviata dal Garante al soggetto che ha effettuato la comunicazione del RPD e indirizzo email di contatto riportato nella comunicazione al Garante).

Ogni webinar approfondisce aspetti particolari della disciplina sul trattamento dei dati personali. Il programma formativo è articolato in 4 moduli principali: "I fondamentali della protezione dei dati", "Il Responsabile della Protezione dei Dati", "Il toolkit del RPD" e "Approfondimenti". Ogni modulo comprende un numero variabile di webinar, che potranno essere fruiti linearmente o secondo le modalità scelte dai partecipanti, grazie alla flessibilità della formazione online.

Le lezioni sono tenute da dirigenti e funzionari del Garante esperti delle materie trattate. Sulla piattaforma, oltre ai video-corsi (prodotti dal Garante utilizzando risorse interne), saranno disponibili le slides presentate dai docenti, eventuali materiali di approfondimento e link utili. Saranno inoltre messi a disposizione test di auto-valutazione per consentire ai partecipanti di verificare autonomamente la comprensione dei contenuti fruiti. La fruizione dei webinar non prevede procedure di monitoraggio o valutazioni da parte del Garante

Oltre ai webinar, il progetto T4Data offre altri importanti strumenti formativi per i RPD dei soggetti pubblici, come un ciclo di seminari locali organizzati in tutta Italia e un manuale per supportare i RPD nell'applicazione del Regolamento Ue 2016/679.

Tutte le informazioni sul progetto T4Data e sugli eventi previsti sono disponibili sulla pagina: www.garanteprivacy.it/regolamentoue/t4data.

https://www.key4biz.it/dpo-online-la-piattaforma-e-learning-dellautorita-garante-per-la-protezione-dei-dati-personali/275371/