Google defends tracking cookies—some experts aren’t buying it

reader comments

261 with 151 posters participating

Share this story

Google’s Chrome team is feeling pressure from competitors over ad tracking. Apple has long offered industry-leading protection against tracking cookies, while Mozilla recently announced that Firefox will begin blocking tracking cookies by default. Microsoft has been experimenting with tracking protection features in Edge, too.

But Google has a problem: it makes most of its money selling ads. Adopting the same aggressive cookie blocking techniques as its rivals could prevent Google’s customers from targeting ads—potentially hurting Google’s bottom line.

So in a blog post last week, Google outlined an alternative privacy vision—one that restricts some forms of user tracking without blocking the use of tracking cookies any time soon.

“Blocking cookies without another way to deliver relevant ads significantly reduces publishers’ primary means of funding, which jeopardizes the future of the vibrant Web,” Google’s Justin Schuh writes. (Those publishers, of course, include Ars publisher Conde Nast. We use cookies to serve targeted ads because they generate more revenue to support our journalism.)

Google also warns that completely blocking tracking cookies will cause ad networks to resort to browser fingerprinting as an alternative means of tracking users. Under this technique, a site harvests many small pieces of data about a user's browser—browser version, fonts installed, extensions active, screen size, and so forth—to generate a "fingerprint" that uniquely identifies a particular device.

So Google's proposal is to declare war on browser fingerprinting while only gradually restricting the use of cookies for ad targeting.

A privacy sandbox?

To prevent fingerprinting, Google says it's working on a new approach called a "privacy budget." Under this approach, the browser would impose a hard cap on the amount of information any site could request from the browser that might reveal a user's identity. If a site exceeded the cap, the browser would either throw an error or it would return deliberately inaccurate or generic information.

But this is only a proposal, not a shipping feature. And it has some obvious challenges. Some API calls might return so much information that they could identify the user all on their own. If a site made one of these calls, the browser would need to warn the user and get explicit approval—which could be annoying for users. And there's a risk that a too-strict privacy budget could break some existing sites even if they're not engaging in user fingerprinting.

The privacy budget is one component of a larger framework Google calls a "privacy sandbox." The goal is to enable advertisers to serve more relevant ads without allowing them to track individual users:

> *We're exploring how to deliver ads to large groups of similar people without letting individually identifying data ever*

> *leave your browser — building on the* ***Differential Privacy*** *techniques we've been using in Chrome for nearly 5 years to collect anonymous telemetry information. New technologies like* ***Federated Learning*** *show that it's possible for your browser to avoid revealing that you are a member of a group that likes Beyoncé and sweater vests until it can be sure that group contains thousands of other people.*

Some pro-privacy experts remain skeptical

Google's post was blasted by a pair of Princeton computer scientists who have long advocated for stricter browser privacy protections. They point out that Apple and Mozilla are also working to restrict browser fingerprinting. They argue that it's a non-sequitur to say that the risk of fingerprinting is a reason not to adopt robust restrictions on cookie-based tracking.

The researchers disputed Google's claim that nuking tracking cookies would undermine the economic foundation of the online advertising industry. They point out that after the EU adopted the General Data Protection Regulation, the New York Times discontinued its use of tracking cookies in Europe. The Grey Lady shifted to using contextual and geographic ad targeting—and its ad revenue hasn't suffered as a result.

They also argued that Google is now endorsing ideas that the company dismissed as impractical earlier this decade.

"Privacy preserving ad targeting has been an active research area for over a decade," the pair wrote. They argue that Google was dismissive of alternatives to cookie-based ad tracking during the Do Not Track debate earlier in the decade. "We are glad that Google is now taking this direction more seriously, but a few belated think pieces aren't much

progress.”

Browser privacy has emerged as an important differentiator for Google’s rivals in the browser market. Apple in particular has been running ads in recent months touting the privacy protections offered by the iPhone. These attacks put Google in a difficult position, because Google can’t match its rivals’ privacy protections without potentially hurting its own lucrative ad business.

https://arstechnica.com/?p=1558091

App4Italy. La recensione del giorno, ActivityTracker

@App4Italy è una rubrica settimanale promossa da **Key4biz** e **Neosperience**. Per consultare gli articoli precedenti, **clicca qui**.
Negli ultimi anni il mercato dell’**Health** è cresciuto costantemente grazie alla maggiore consapevolezza del pubblico nei confronti del proprio benessere. Di conseguenza, anche le applicazioni che si occupano di tracciare le performance fisiche degli utenti hanno visto un vero e proprio boom.

Quello che però distingue **Activity Tracker** da tutte le altre app è il fatto che non richieda di utilizzare il segnale GPS. Se avete a cuore i vostri dati personali, o la salute della batteria del vostro smartphone, sicuramente questa è una caratteristica che vi renderà felici; ma gli elementi positivi di Activity Tracker non finiscono certamente qui.

È da sottolineare la chiarezza del design, di facile utilizzo ed essenziale, ma allo stesso tempo completo. Per quanto

riguarda la raccolta dei dati, vengono conteggiati chilometri, passi, dislivello e calorie consumate. Inoltre, questi si possono visualizzare su base giornaliera, settimanale e mensile, e si possono impostare anche i propri obiettivi settimanali.

Sebbene funzioni in maniera indipendente, pagando la versione premium, è possibile collegare l'app a wearable e smartwatch così da avere un maggiore numero di dati a disposizione. La cosa bella, però, è che non è assolutamente necessario pagare per avere una più che soddisfacente esperienza di Activity Tracker.

In definitiva Activity Tracker ha tutte le caratteristiche per posizonarsi tra le migliori app di tracciamento dell'attività fisica dell'utente. Al momento è disponibile per Android 5.0 e successivi e iOS 9.0 e successivi.

Contenuti: @@@

Grafica: @@@

Usabilità: @@@

Legenda: @ sufficiente; @@ buono; @@@ ottimo

https://www.key4biz.it/app4italy-la-recensione-del-giorno-activitytracker/268656/

Privacy, qual è il valore

reale del dato personale?

Negli ultimi decenni il contesto socio-culturale è cambiato profondamente, modificando anche le modalità di comunicazione degli individui. Tale cambiamento ha avuto un profondo impatto anche sul rapporto esistente tra individuo e norma giuridica, soprattutto riguardo alla tutela della persona. Sono numerosi gli interventi legislativi che hanno dovuto modificare norme giuridiche o crearne nuove per adattarsi alla realtà virtuale del web.

In effetti, da un lato è noto che la diffusione di Internet e delle piattaforme di social networking abbiano inciso favorendo la possibilità di interazione tra gli individui; dall'altro, l'evoluzione tecnologica, soprattutto attraverso smartphone e tablet, ha favorito detta interazione in mobilità non essendo più necessario un computer.

Ciò ha determinato un mutamento delle modalità di comunicazione, che non è più solo verbale (nelle sue ampie accezioni) o scritta ma anche basata su immagini e contenuti multimediali, con un conseguente impatto sul comportamento delle persone nella loro quotidianità.

L'essere umano ha bisogno di comunicare (primo assioma della Scuola di **Palo Alto**)[1] e il vantaggio offerto da Internet di poter interagire con altre persone anche a distanza ha avuto successo. Del resto, sono numerosi i contributi divulgativi e scientifici che hanno descritto questa evoluzione (o involuzione, a seconda del punto di vista) di carattere sociale, che può avere indubbi riflessi di natura giuridico-legale.

Va riconosciuto che la "nuova" modalità di comunicazione per certi versi costituisce un miglioramento in termini puramente

sociali. Tuttavia, se si registra un vantaggio sociale della "nuova" comunicazione non può dirsi altrettanto per il contesto culturale che, molto spesso, denota, purtroppo, una involuzione.

La "nuova" modalità di comunicazione, paradossalmente, favorisce in maniera esponenziale la comunicazione tra gli individui, e la velocità di interazione ha fatto scaturire la consuetudine (divenuta ormai il modello) della celere (e comoda) consultazione dei contenuti presenti sul web (senza alcun discernimento delle fonti) anche con finalità, purtroppo, di apprendimento. In effetti, le fonti consultabili (non sempre corrette) sono fondamentalmente sul web e i contenuti sono poco articolati perché devono risultare facilmente leggibili e in breve tempo.

Accedere (comodamente e rapidamente) alle fonti presenti sul web consente di realizzare in maniera distorta il processo di autoformazione (o apprendimento autodiretto o autoapprendimento – *self learning*) in quanto "*la criticità nel tema dell'autoapprendimento è legata al fatto che per auto-apprendere, le persone devono avere una specifica competenza sul come sia possibile auto-apprendere*" e, quindi "*c'è bisogno di sviluppare una competenza ad auto-apprendere che non può essere data per scontata*"[2]. Il processo di autoapprendimento generalizzato può determinare un abbassamento del livello culturale.

In sostanza, l'esigenza di una comunicazione sempre più veloce molto spesso richiede altrettanta celerità nella acquisizione di nozioni e nell'accrescimento del profilo culturale che, invece, può subire un decremento sia in ragione della moltitudine di fonti presenti sul web alle quali si accede senza selezionare quelle certe e accreditate sia riguardo alla necessaria competenza per auto-apprendere.

La nostra vita quotidiana è incentrata sulla comunicazione e sull'imprescindibile utilizzo degli strumenti necessari alla

esecuzione della stessa. Le 24 ore (anche quelle notturne) sono quasi completamente impegnate dall'utilizzo di device (computer, tablet, smartphone) fondamentalmente per comunicazioni di natura lavorativa o personale.

Le app più note consentono una comunicazione multimediale che non si limita alla sola scrittura di testo, ma include anche la trasmissione di contenuti quali immagini, video o messaggi vocali. Gli utenti, però, scelgono le app seguendo il criterio della loro maggiore diffusione (spesso per moda o per essere parte di un gruppo) invece di prestare attenzione alla protezione delle informazioni che vengono veicolate. Paradossalmente, gli utenti preferiscono continuare ad utilizzare app potenzialmente meno sicure ma molto diffuse invece che riflettere sulle conseguenze dei rischi connessi alla sicurezza dei dati. A fronte dell'invito rivolto alle persone di riflettere sui potenziali rischi di sicurezza, si sente rispondere che quella o quelle app sono le più utilizzate; prevale, quindi, il criterio (imprudente?) delle scelte operate dalla maggioranza degli utenti (inconsapevoli). È altrettanto vero che gli sviluppatori hanno l'obbligo di rispettare le norme sulla protezione dei dati personali e in particolare il principio sancito dall'art. 25 del **GDPR** sulla "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" (**Data Protection by Design** and **by Default**).

Del resto, le scelte degli utenti sono al contempo indirizzate verso app che si assumono poter essere utilizzate gratuitamente senza alcuna riflessione sul reale costo da pagare che, quasi sempre, corrisponde ai dati degli utilizzatori (dati personali, indirizzi IP, data e ora di accesso e di utilizzo, metadati, ecc.). La smania di accedere a determinati servizi o di utilizzare le app prevale sul minimo buon senso che viene ampiamente prevaricato sia dalla accettazione incondizionata delle condizioni generali e delle privacy policy (quasi sempre non lette) sia dal disinteresse

per i rischi, anche minimi, connessi alla sicurezza delle informazioni (valutabili con tre banali domande: “A chi e dove invio i miei dati, da chi essi saranno trattati e dove gli stessi saranno salvati”?).

Molti utenti trasmettono messaggi vocali senza riflettere affatto sui rischi a cui potrebbero andare incontro nel caso in cui venisse acquisito da terzi il campionamento vocale, alterato e utilizzato per fini impropri.

Quale dato più personale della propria voce? Tuttavia, l’irrefrenabile desiderio di attestare la propria presenza (sulla rete o comunque mediante app) prevale sulla sicurezza per i propri dati personali e quelli delle altre persone.

In conclusione, al di là delle esigenze di comunicazione, emerge anche un desiderio, tipico dell’essere umano, che è quello dell’esibirsi e dell’apparire[3].

Essere o apparire: il tema è ovviamente antico e non si scopre l’acqua calda.

Comportamento e fattore umano

Abbiamo assistito, nel corso degli ultimi anni, alla proliferazione delle piattaforme di comunicazione sul web, dai forum ai social network.

È profondamente cambiato lo stile di vita (*lifestyle*) delle persone, sia in ambiente lavorativo sia in ambito privato.

Le persone, a volte anche consapevolmente, nel corso degli anni hanno alimentato – e continuano a farlo – le piattaforme di comunicazione con quantità enorme di dati, anche personali. È immaginabile quanto sia vertiginoso l’aumento della quantità di dati da parte dei provider delle piattaforme.

Il numero di utenti della rete (quasi 4 miliardi e mezzo e cioè oltre il 50% della popolazione mondiale) consente di

immaginare facilmente la enorme quantità di dati che vengono quotidianamente trasmessi (sms, app e sistemi di messaggistica, **Whatsapp, iMessage, Facebook, LinkedIn, Twitter**, pagine web, ecc.) e numerose sono le piattaforme da cui è possibile, anche solo indicativamente, avere idea del traffico di dati trasmessi (secondo Cisco[4] in un secondo il traffico di rete è di circa 24.000 GB e in un mese di 91,3 EB, oltre 98 bilioni di GB).

A ciò si aggiunga che l'evoluzione tecnologica ha consentito lo sviluppo di sistemi intelligenti, basati sulla **Intelligenza Artificiale** e sul **Machine Learning**, attraverso i quali è possibile ottenere risultati di analisi anche di grandi quantità di dati (Big Data) trasmessi dai singoli utenti, oltre ai cosiddetti metadati (informazioni aggiuntive rispetto al contenuto trasmesso, quali – ad esempio – indirizzo IP, data e ora, dati EXIF per le immagini, URL, HTTP GET, pagine web, file, email, transazioni con carte, ecc.).

Lo scenario descritto – sebbene sintetico e non esaustivo – illustra come, al di là dell'utilizzo di sistemi di mascheramento di alcune informazioni, la maggior parte dei dati che transitano sulla rete risultano identificabili.

Peraltro, la libertà di pubblicare contenuti sulla rete non trova il corrispondente opposto nella volontà dell'individuo di poter cancellare i medesimi contenuti quando si vuole, in ragione della possibile indiscriminata diffusione degli stessi contenuti su internet. In sostanza, una volta pubblicato un contenuto (che sia un like, un post, un'immagine, un articolo, o qualunque altra risorsa) non si ha la certezza che esso possa essere rimosso come se non fosse mai stato pubblicato.

Il fattore umano suscita sempre particolare attenzione, sia in ambito sociale per l'analisi dei comportamenti sia in ambito più tecnico per la valutazione dei rischi relativi alla sicurezza in generale. I comportamenti umani possono essere prevedibili e condizionabili ma resta sempre l'incognita della

mente umana che appartiene all'imponderabile; una persona può porre in essere azioni o omissioni che sono il risultato della sua capacità di autodeterminazione, tanto da potersi discostare dalle proprie comuni abitudini o consuetudini. In sostanza, il fattore umano, considerato sia sul piano del comportamento sia sul piano dei rischi per la sicurezza, potrebbe avere conseguenze dirompenti in ragione di decisioni imponderabili.

I contenuti pubblicati online, anche su piattaforme ad accesso riservato, non escludono il rischio consistente nell'utilizzo non autorizzato, e quindi abusivo, di determinate informazioni personali (a volte anche sensibili) appartenenti all'interessato.

Ogni contenuto generalmente lascia la sua traccia indelebile sulla rete.

Il 12 luglio 2019 è stato pubblicato sul sito del Comitato europeo per la protezione dei dati (**EDPB**) il documento dal titolo "*Guidelines 3/2019 on processing of personal data through video devices*"[5], in consultazione pubblica sino al 6 settembre 2019.

Il predetto documento si riferisce al trattamento dei dati personali effettuato tramite dispositivi video; nel paragrafo 1 della sezione 'Introduzione' si legge che l'uso intensivo di dispositivi video ha un impatto sul comportamento dei cittadini e le implicazioni sulla protezione dei dati sono enormi (*The intensive use of video devices has an impact on citizen's behaviour. … Data protection implications are massive*.).

Si legge, inoltre, che sussiste un rischio potenziale, consistente nell'abuso dei dati acquisiti dalle videocamere, che è direttamente proporzionale alla dimensione dello spazio monitorato e al numero di persone che frequentano detto spazio. L'EDPB evidenzia correttamente il "**comportamento**" dei

cittadini quale conseguenza dell'utilizzo di sistemi video, ove il presupposto ("*behaviour*") è connesso all'impatto delle tecnologie sulla privacy e sui dati personali.

Del resto, il comportamento è stato già oggetto di attenzione in relazione al fenomeno "*behavioural advertising*" (pubblicità comportamentale), con alto rischio di profilazione.

Si tratta di un provvedimento sul tema della video sorveglianza ove le preoccupazioni sono focalizzate sull'uso improprio dei dati anche mediante tecniche di analisi video intelligenti; non vi è dubbio che queste linee guida avranno effetti anche in ambito nazionale, con impatto sui provvedimenti già adottati in materia dal Garante.

Emerge dal citato provvedimento dell'EDPS l'importanza del comportamento, il "*behaviour*" che è imprevedibile, comunque strettamente connesso alla personalità di ciascun essere umano, e potrebbe trasformarsi in una potenziale fonte di rischio.

La smania dell'apparire, che pervade l'essere umano, costituisce lo spunto motivazionale che potrebbe indurre le persone a pubblicare i più disparati contenuti nell'ottica della massima libertà di espressione. In questo modo si contribuisce ad alimentare il "contenitore" di dati di ciascun provider ma soprattutto dei fornitori di social network.

Se da una parte si possono registrare soggetti "più attivi" socialmente, dediti alla pubblicazione smodata di informazioni, dall'altro non si può escludere l'abusivo utilizzo di informazioni appartenenti ad alcuni individui da parte di soggetti che potrebbero diffonderle.

Com'è evidente sussistono rischi per i dati personali. E allora, che fare?

Consapevolezza ed etica

Oggigiorno c'è l'esigenza di parlare di etica per consentire un approccio corretto alla dignità umana così come è necessario che si lavori per consolidare e accrescere una vera consapevolezza del valore della persona e dell'intera sfera di ciascun individuo.

La prevalenza dell'apparire rispetto all'essere si esplica *in toto* nel comportamento umano, senza possibilità di essere contenuta o mitigata con rimedi preventivi e specifici. Le sanzioni (successive al fatto) hanno un mero significato punitivo di un comportamento contrario alle norme dell'ordinamento giuridico.

Una adeguata consapevolezza e un approccio etico riguardo a ciò che si sta compiendo e soprattutto alle conseguenze che ne possono derivare potrebbero però costituire un valido strumento preventivo per ridurre il rischio in capo a ciascun soggetto per sé e per gli altri. Consapevolezza ed etica non costituiscono decisamente "la soluzione", ma componenti del processo sulla protezione dei dati personali.

In un'epoca come quella attuale, in cui si assiste al vertiginoso sviluppo delle innovazioni tecnologiche e alla conseguente incidenza sulla digital economy, il focus va ricercato nella reale consapevolezza del valore attribuito al dato personale e in una attenta e corretta analisi di ciò che accade nel resto del mondo in questa materia.

Molto spesso la voglia di apparire prevale sulla consapevolezza in quanto l'attuale società è del tutto condizionata dall'utilizzo delle tecnologie nonché dalla smania di confermare la propria presenza in numerosi contesti digitali. Anche un solo like attesta una presenza, un "ci sono".

Tutto ciò non deve però demotivare dalla diffusione della

cultura della consapevolezza e dell'etica, entrambe finalizzate a sensibilizzare gli utenti sulla importanza e sul rilievo che assumo i dati personali.

Il trattamento dei dati personali

Ulteriore riflessione è quella relativa alla "gestione", al trattamento dei dati che vengono forniti alle numerose piattaforme che ne sono responsabili.

Fino a qualche tempo fa gli utenti "si fidavano" (quasi ciecamente) dei social network provider riguardo al rispetto delle leggi vigenti in materia di protezione dei dati personali.

Tuttavia, il noto caso "*Cambridge Analytica*" ha dimostrato quanto sia debole il sistema basato sul "trust" e sulla accettazione e approvazione (unilaterale?) incondizionata delle privacy policy proposte (in questo caso da Facebook, titolare del trattamento). Il social network provider ha l'obbligo di rispettare le norme in materia di protezione dei dati personali e i singoli utenti.

Non è questa la sede opportuna per approfondire i dettagli del caso "*Cambridge Analytica*" ma appare evidente che le informazioni personali (a volte sensibili) di soggetti presenti su Facebook sono state utilizzate senza il loro consenso per finalità di analisi e condizionamento delle loro scelte per il raggiungimento di altri risultati diversi dalle finalità del titolare del trattamento.

Se non si considera l'alto valore dei dati personali, si corre il rischio di favorire – in un'ottica pericolosamente e apparentemente legittima ma del tutto illecita – la mercificazione delle informazioni personali anche corrispettivo per eventuali servizi forniti anche mediante l'utilizzo di applicazioni.

Il fenomeno già noto in passato, tanto che ha ricevuto adeguata attenzione da parte dell'EDPS, sta serpeggiando e tornando in auge. Sono addirittura sorti i *data broker*[6] per l'acquisto di set di dati.

È evidente che un simile fenomeno è inaccettabile, oltre che essere illecito in ragione delle norme vigenti, soprattutto perché comporta lo svilimento dell'alto valore proprio dei dati personali come si è illustrato.

Le ricerche dimostrano anche un altro aspetto di rilievo: è emerso che l'utilizzo dei social network attesti un alto livello di analfabetismo funzionale[7] in quanto la "*partecipazione non è andata di pari passo con un miglioramento delle capacità di comprensione del testo, nel senso di interpretarlo, di saper leggere fra le righe elaborando delle conclusioni proprie*".

Si tratta di uno scenario sconcertante che contribuisce ad aumentare le preoccupazioni circa la assoluta mancanza di consapevolezza sia sul valore del dato personale sia sugli effetti della pubblicazione e propagazione dei contenuti sui social network.

Quale **etica** alla base di un simile comportamento ?

Quanta **consapevolezza** da parte degli utenti ?

Per entrambe le domande, le risposte possono essere molto semplici, posto che il tutto si è basato (ma tuttora è lo stesso) sulla totale o parziale assenza di consapevolezza e comunque mancanza di etica.

Digital economy, e-Democracy e dati personali

I più grandi player a livello globale da tempo sanno che il vero capitale è costituito dai dati personali.

D’altra parte accade, invece, di rado che le persone effettuino scelte etiche consapevoli quando agiscono anche solo come utenti nel “sistema” delle piattaforme digitali.

Ogni azione, che sia un like, un post o una condivisione, sarà fagocitata dagli algoritmi basati sulla IA e fornirà ai provider precise indicazioni sul comportamento degli utenti: si tratta della c.d. *Big Data Analytics*.

Ciò consente ai provider di orientare le proprie scelte a seconda del comportamento degli utenti.

L’apparente libertà di espressione si tramuta in un vero e proprio condizionamento globale governato da chi ha il controllo dei potenti algoritmi di IA, che finisce per esplicarsi in una profilazione globale basata sul comportamento degli utenti sottoposti al monitoring delle proprie scelte.

Consapevolezza, allora, significa conoscere la realtà, apprendere e sapere quali sono le conseguenze di ogni comportamento per poi decidere se essere parte del “sistema” e in che modo.

È ovvio che da qualsiasi analisi di grandi quantità di dati si possono estrarre risultati di ogni tipo, non esclusi quelli su singoli profili.

Uno dei rischi maggiori è quello di perdere il pieno controllo delle proprie informazioni dopo averle pubblicate, qualora esse siano state oggetto di condivisione e replicate altrove.

I dati personali, pertanto, governano la *digital economy* e possono essere utilizzati per influenzare le scelte.

Il panorama così osservato e descritto, ricomprende, inoltre, ipotesi di gravi conseguenze anche riguardo ai rischi per un distorto esercizio della democrazia.

L’attuale contesto è evidentemente votato, ad una democrazia

digitale – *e-Democracy* – nella sua più ampia accezione, realizzata mediante l'utilizzo sempre più massiccio delle tecnologie.

Il tema è particolarmente delicato e merita il rinvio ad altra sede per gli opportuni approfondimenti.

L'utilizzo delle tecnologie costituisce un indubbio vantaggio anche in democrazia nelle diverse accezioni in cui si esplica, tra le quali, e-Government, e-Governance, e-Participation, e-Inclusion, e-Procurement. In questo generale contesto, però, l'uso incondizionato delle tecnologie può comportare rischi per la sicurezza e per i diritti fondamentali degli individui, tra cui quello alla protezione dei dati personali.

Il quadro diviene più nitido se si considera il fenomeno delle *fake-news*, a volte frutto di attività realizzate in laboratorio mediante la manipolazione di video con l'aggiunta di una base vocale diversa da quella originaria, ovvero attraverso l'utilizzo di un profilo digitale non ufficiale ma identico a quello, la manipolazione delle informazioni, ecc.

Le incertezze sulla impossibilità di avere pieno e sicuro controllo delle tecnologie e delle fonti di informazione ufficiali potrebbe costituire un rischio per la democrazia digitale. Se questi rischi, poi, sono connessi a dati personali è immaginabile come sia elevato il livello di preoccupazione.

Norme giuridiche e visione globale

Il **GDPR** è una pietra miliare in materia di protezione dei dati personali in quanto trasforma radicalmente il relativo sistema, comportando un profondo rinnovamento scientifico e culturale, attuabile modificando l'approccio a questa materia.

Tuttavia, a distanza di oltre un anno dalla sua applicazione, sembra opportuno guardare anche al di fuori dell'Europa per

avere una visione completa della incidenza delle tecnologie sui dati personali e sulla privacy. Non si può prescindere dalla osservazione di quanto accade al di fuori del perimetro nazionale o europeo in questa materia.

Infatti, prima di approfondire specifiche tematiche in materia di protezione dei dati personali e privacy, è necessario avere preventivamente chiari gli scenari europei e quelli dei principali Paesi del mondo, mediante un'efficace e corretta analisi di carattere generale. In un mondo globalizzato e decisamente condizionato dall'uso di Internet e delle tecnologie non è più possibile occuparsi di questi temi unicamente soffermandosi all'interno dei propri confini nazionali o europei.

Il GDPR, sappiamo, è applicabile – in presenza di specifiche condizioni – anche a soggetti che sono fuori dall'Unione, i quali, spesso, hanno approcci diversi alla protezione dei dati personali e alla privacy. In un sistema globale ove le tecnologie direttamente e indirettamente incidono sulla vita privata di ogni persona, non si può prescindere da valutazioni che – sebbene generali – riguardano anche altri sistemi giuridici.

L'analisi di altre realtà, dove possono essere utilizzati istituti giuridici diversi da quelli che conosciamo o ruoli non utilizzati nei nostri sistemi (es. *Data Custodian* in Canada), consente di avere un quadro più ampio e chiaro per poter affrontare correttamente e con le necessarie competenze le singole questioni. Esiste una matrice comune che riguarda privacy e protezione dei dati personali, ma gli approcci possono essere differenti a seconda del contesto territoriale.

È noto che negli USA e in Canada questa materia sia descritta come "*Data privacy and protection*", quasi come se tale approccio esprimesse la primazia della privacy rispetto alla protezione dei dati personali. Ciò induce a considerare la privacy e la protezione dei dati personali in termini globali

senza considerare confini, possibilmente con un comune standard privacy framework, così come descritto nel contributo dal titolo "***Privacy and Security in the Internet of Things***" pubblicato nel 2013 su *Cutter IT Journal*[8] (Vol. 26, No. 8 August 2013).

In Europa abbiamo il privilegio di fare riferimento ai diritti fondamentali contenuti nella Carta dei Diritti Fondamentali dell'Unione Europea.

Tuttavia nel confronto con soggetti di altri continenti potrebbe risultare complesso discutere, a livello generale, del valore del dato personale con riferimento a principi codificati nella legislazione europea.

La protezione dei dati personali in Europa è un diritto fondamentale, ma l'assenza di normativa che attribuisca dignità alla privacy (il riferimento è a-tecnico e esteso anche alla protezione dei dati personali) non vuol dire poter ignorare o ridimensionare la portata.

Una valutazione che faccia riferimento alla persona e alla dignità umana porterebbe inevitabilmente ad attribuire un valore elevato e nobile al dato personale per il solo fatto che esso appartiene a una persona ed è intrinsecamente connesso ad essa. Infatti, la qualifica di valore assoluto deriva proprio dalla natura delle informazioni strettamente appartenenti a una persona fisica.

Con il termine valore, in questo caso, si intende affermare una qualità di particolare pregio che contraddistingue le informazioni personali poiché esse sono strettamente connesse alla persona e ne costituiscono il suo elemento ontologico. La vita al contempo è e ha un valore in senso assoluto, così come tutto ciò che appartiene ad una persona; per questo il regime di appartenenza alla persona consente a ciascun elemento ad essa afferente di acquisire lo stesso valore, pregio e condizione e, quindi, merita identico trattamento.

Questo approccio non è strettamente correlato alla normativa e all'ordinamento giuridico ma, più in generale, all'utilizzo di un criterio che si basi su consapevolezza ed etica andando ben oltre l'impianto del diritto.

Allo stesso modo, il lavoro per la realizzazione di standard tecnici di portata internazionale (tra i molti, "*Ontological Standard for Ethically Driven Robotics and Automation Systems*[9]" che mi vede direttamente coinvolto) molto spesso comporta delle difficoltà per la corretta applicabilità delle relative norme in Paesi dove alcuni concetti possono essere diversi o inesistenti.

Tutto quanto precede è necessario per ancorare un concetto che si ritiene essere basilare. Si discute di protezione dei dati personali e privacy solo e unicamente in quanto esistono norme *ad hoc*, diversamente non ci si porrebbe il problema di soffermarsi sulla essenza e sul rilievo dei dati personali.

La disciplina giuridica certamente costituisce l'elemento principale da considerare per valutare il rispetto delle regole in materia di protezione dei dati personali.

Pertanto, il processo logico e metodologico che viene adottato è quello della tutela o protezione dei dati personali, procedendo dall'elemento principale costituito dalle norme esistenti. Il riferimento immediato, infatti, è costituito dalle norme vigenti al fine di interpretarle per affrontare le singole fattispecie.

Non si può trascurare, però, che il dato personale debba essere considerato come valore in senso assoluto, anche attraverso un approccio etico e comunque prescindendo da qualsiasi norma.

L'analisi e la valutazione di una fattispecie in materia di privacy e protezione dei dati personali, oggigiorno, non possono essere affrontate basandosi – correttamente peraltro – unicamente sul dato normativo alla ricerca di una soluzione;

è, invece, necessaria una preventiva valutazione della fattispecie procedendo con un criterio che si basi su consapevolezza ed etica, aspetti che si collocano su un livello superiore rispetto a quello normativo.

Del resto, avere un previo e chiaro scenario internazionale su un aspetto specifico afferente privacy e protezione dei dati personali, consente di poter affrontare le relative questioni con consapevolezza. In uno Stato in cui non esiste una normativa in materia di protezione dei dati personali, infatti, qualora non si procedesse dalla consapevolezza e dall'etica considerando il dato personale un valore, verrebbe consentita qualunque azione fondamentalmente in pregiudizio della persona.

L'approccio descritto – che considera quale "**prerequisito**" il criterio preventivo basato sul principio secondo il quale il dato personale è un valore assoluto e richiede consapevolezza ed etica – è il vero e reale punto di partenza, non codificato, che si pone come elemento ultragiuridico.

Infatti, la normativa in materia di protezione dei dati personali esiste proprio perché vanno tutelate le informazioni appartenenti ad una persona, nel pieno rispetto della dignità umana.

In questo modo, con il criterio proposto, ci si posiziona ad un livello antecedente a quello delle norme giuridiche risultando lo ***starting-point***.

Il "**livello zero**", vero punto di partenza, è la considerazione anche etica dell'alto valore attribuibile al dato personale; senza questo assunto difficilmente si può avere un idoneo approccio alla normativa. Il "**livello uno**" sarà quello delle norme giuridiche.

In conclusione, consapevolezza ed etica senza prescindere dalle norme, possono condurre a risultati più efficaci: è una sfida.

[1] Secondo la Scuola di Palo Alto, il cui maggior esponente fu Paul Watzlawick, si distinguono 5 assiomi: 1. Non si può non comunicare; 2. All'interno di ogni comunicazione si possono individuare due livelli (contenuto "notizia o informazione" e relazione "comando"); 3. Il flusso comunicativo è espresso secondo la punteggiatura degli eventi; 4. La comunicazione avviene attraverso i canali verbali (digitale) e non verbali (analogica); 5. Gli scambi di comunicazione sono simmetrici o complementari, a seconda che siano basati sull'uguaglianza o sulla differenza. Tra i numerosi contributi, Alessandro Ferrari, "*I 5 assiomi della comunicazione umana*".

[2] Autoformazione o autoapprendimento, *Intervista Franco Bochicchio dell'Università del Salento.*

[3] *È vero che quella di oggi è la società dell'apparire, che è una società edonistica, che è una società che fa la fortuna dei chirurghi plastici, giacché tutti vogliono essere perfetti, tutti vogliono sembrare belli.* – "La società dell'apparire: intervista al sociologo Francesco Pira".

[4] https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~complete-forecast

[5] Guidelines 3/2019 on processing of personal data through video devices

[6] Intel Executive: Rein In Data Brokers

[7] Analfabeti funzionali e social network: la situazione in Italia?

[8] https://www.cutter.com

[9] https://standards.ieee.org/project/7007.html

email: info@fabiano.law

Copyright (Nicola Fabiano) Tutti i diritti riservati. All rights reserved.

https://www.key4biz.it/privacy-qual-e-il-valore-reale-del-dato-personale/268586/

Weople, privacy e monetizzazione dei tuoi dati: chi controlla i controllori?

Weople, che cos'è? È l'App tanto reclamizzata che promette di farti **riavere il controllo sui tuoi dati e persino di guadagnarci**. Come? Proprio questo è il punto.

Ultimamente se n'è parlato tanto, a seguito della notizia secondo cui, con una lettera a firma del Presidente Antonello Soro, **l'Autorità Garante per la privacy** ha posto all'attenzione del **Comitato europeo** per la protezione dei dati personali (Edpb) la questione relativa a Weople, l'App che promette ai propri iscritti una remunerazione in cambio della cessione dei loro dati personali. A partire dai primi mesi del 2019, infatti, sono state diverse le segnalazioni giunte all'Autorità da parte di imprese della grande distribuzione che lamentavano di aver ricevuto da parte di Weople numerosissime richieste di trasferire alla piattaforma dati personali e di consumo registrati nelle carte di fedeltà. L'impresa italiana, che gestisce l'App e offre servizi di vario genere (offerte commerciali, analisti statistiche e di mercato), si propone infatti come intermediaria nel rapporto tra aziende e utenti chiedendo, su delega di questi ultimi, di

ottenere le informazioni personali custodite presso grandi imprese allo scopo di riunirle all'interno della propria banca dati.

Ora, però, il richiamo da parte del Garante. La notizia ha fatto presto il giro delle principali testate, scatenando un vero tam tam in rete. E non è d'altronde la prima volta.

Le prime perplessità
Personalmente avevo posto la mia attenzione sull'App già tre o quattro mesi fa – quando giravano ammiccanti spot sull'App persino in TV – condividendo poi in rete, con un paio di semplici post, ma cui erano seguite interessanti discussioni, i miei dubbi e perplessità.

Su Facebook i commenti erano già illuminanti. «Mi avevano proposto una collaborazione marketing», scriveva un utente, «*ho rifiutato. Per quanto tecnicamente sembri in regola, a livello etico mi ha lasciato parecchio perplesso: per me l'utente medio non ha l'adeguata percezione del valore delle sue informazioni personali e si farebbe abbindolare in cambio di pochi centesimi alla settimana*». «*Un mio vecchio professore soleva sempre dire di tenersi alla lontana da situazioni o persone che si pongono come controllori e santi nel sanare una situazione*», gli faceva eco un altro, «*magari assurgendo che "tanto il sistema, se non lo faceva direttamente, lo facevano altri". La questione se meramente è legata alla protezione dei dati deve assurgere al vero modello di salvaguardia che risiede nel protocollo primo. Ossia l'unico conoscitore dei dati totali deve essere il proprietario. Ogni nodo di condivisione è un canale di diffusione. Ovviamente quando volontariamente siamo "costretti alla condivisione" in un sistema digitale è di per se molto difficile tracciare i dati, Una domanda che porrei a Weople è dove risiedono tecnicamente, "su che ferro ha i dati": risalire alla sorgente fisica dove*

risiedono è una prassi a mio avviso molto interessante». «*Sagge riflessioni e perplessità che condivido», concludeva infine un altro. «Potrà un'Azienda così piccola garantirmi la massima protezione dei miei dati? A questo punto vado su Google che almeno so di che morte dovrò morire*».

Avevo rilanciato anche sul mio Canale Telegram della Educazione Civica Digitale il tema, scatenando pure lì commenti e grande interesse.

Qual è, infatti, il punto in estrema sintesi? Con Weople dovrai **depositare i tuoi dati in un caveau personale**, una **«cassetta di sicurezza» nell'App**, **unico filtro fra te e le aziende** interessate alle tue info personali. **Solo Weople** – occhio – **deterrà i tuoi dati**, **inoltrandoti possibili offerte interessanti**. E fin qui «tutto perfetto», si direbbe. Attenzione, però. Con ciò stesso **io *comunque consegno* a «qualcuno» i miei dati**. **Comunque li metto in una cassaforte di cui altri hanno le chiavi**. Dove starebbe, dunque, la vera ripresa del controllo? Sembra, d'altronde, che Weople stessa «svolga **analisi e profilazione su tali dati**». Da qui il problema, evidentemente ormai non più solo nostro.

Weople, come funziona

Qual è il funzionamento di Weople, in dettaglio? Andiamo con ordine. Abbiamo parlato di «caveau». Ecco, come si legge sul sito dell'App, per attivare una cassetta basterà inserire gli estremi identificativi del tuo account. Weople farà il resto per te e chiederà i dati a chi attualmente li possiede. Quali dati si possono depositare? Da subito sarà possibile depositare i dati relativi agli account social, i dati delle spese effettuate con le carte fedeltà personali, i dati delle spese on line tramite gli account e-commerce, i dati posseduti da Google e Apple. «*Ma questo è solo l'inizio!*», esclamano. «*Dall'autunno ci saranno altre novità e sorprese!*».

Come agisce Weople? Attivare una cassetta di sicurezza significa avviare la procedura per ottenere una copia dei tuoi

dati digitali. Weople agirà per te, chiedendo i dati a chi li possiede e ti comunicherà non appena saranno disponibili. Inoltre, potrai monitorare costantemente lo stato di questa procedura dall'App. I dati sono ospitati in un caveau maschera, trattati e investiti in forma anonima, con i massimi standard di sicurezza. All'inizio la cassetta di sicurezza è grigia, vuota e pronta per l'attivazione.Una volta attivata, cioè inserito l'account personale, la cassetta avrà il bordo azzurro, ma i dati sono in attesa e Weople li chiederà a chi attualmente li possiede. Quando i dati saranno in afflusso, la cassetta diventerà azzurra e inizierà il vero e proprio investimento. Potrai usare Weople come portafoglio digitale dei tuoi account e delle carte fedeltà. Per esempio, potrai accedere comodamente al codice a barre della tua carta fedeltà e utilizzarlo durante i tuoi acquisti.

«*Applicando l'articolo 20 del Gdpr, Weople* – su delega dei propri utenti – *chiede ai giganti del web e a tante altre aziende copia dei dati digitali riferiti all'iscritto all'App e li deposita in un conto del singolo utente*», aveva spiegato lo stesso fondatore dell'App, Silvio Siliprandi, in una intervista qualche mese fa. «*Insomma, mettiamo nelle condizioni di esercitare il nuovo diritto alla portabilità dei dati, quel diritto che permette di ricevere i dati personali forniti al titolare del trattamento, in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un diverso titolare. L'obiettivo ultimo è quello di accrescere il nostro controllo sui nostri dati personali, restituendo valore economico ma anche diritti, conducendo delle battaglie per conto delle persone che altrimenti non riuscirebbero a spuntarla con i colossi del web. L'unico impegno da parte di chi entra sulla piattaforma è l'iscrizione, non ci sono costi. Non solo: cerchiamo anche di trasferire al proprietario dei dati i vantaggi che derivano dalla loro condivisione. Weople si propone, infatti, anche come piattaforma di marketing diretto per offrire delle proposte e delle comunicazioni a target interessanti. In*

particolare troviamo clienti-aziende e proponiamo loro di veicolare, tramite App, pacchetti, offerte personalizzate e/o comunicazione a segmenti di correntisti che Weople ha dimostrato, grazie ai dati, essere potenzialmente interessanti. Ovviamente, senza mai dare dati personali all'azienda e ***ponendoci come filtro e unica piattaforma per raggiungerli****.* ***Quanto le aziende pagheranno per veicolare queste offerte personalizzate verrà dato, in grandissima parte, alle persone destinatarie delle stesse****. È la prima volta in assoluto, al mondo, che, per ricevere un'offerta o una comunicazione, il destinatario finale viene pagato. Una rivoluzione nella rivoluzione*».

«*Quest'attività genererà due forme di guadagno per l'iscritto*», continuava, «*un* ***salvadanaio personale*** *dove si possono accumulare il valore in* ***moneta vera****, e un* ***portafoglio di offerte personalizzate*** *a cui si può liberamente decidere di aderire o meno. A breve poi, potremo investire masse di dati anonimi, aggregati e protetti nel mercato in cui, al momento, si genera più valore: si tratta di attività di arricchimento e valorizzazione di database di terze parti, sempre fatte senza cedere i dati individuali e personali. Qui entrerà in gioco la massa dei dati degli iscritti a Weople e il valore che si genererà (aggiuntivo rispetto a quello visto sopra) sarà merito un po' di tutti: verrà quindi restituito attraverso un sistema di estrazioni su base periodica*».

Il punto, come si capisce, sta proprio in quella frase: essere, da parte di Weople, «filtro e unica piattaforma di conservazione dei dati dell'utente». Comunque sia **io non ho il vero, pieno e totale controllo dei miei dati se questi sono o sono *anche* in mano di altri**, di una qualche **cassaforte di cui qualcun altro, oltre a me, possiede i dati**. Tutt'al più il **problema si sposta**, non si risolve.

Le dichiarazioni di trasparenza

Sia chiaro, non intendiamo qui fare processi alle intenzioni o mettere in dubbio la buona fede dei fondatori. Si tratta

semplicemente di rilevare possibili incongruenze. Tanto maggiori quanto più forti sono le dichiarazioni dell'App di trasparenza e volontà di favorire in ogni modo l'utente. Sul sito, infatti, grande spazio è dato proprio alla trasparenza del contratto fra te e Weople. Leggiamo ad esempio la sintesi.

1. «Weople è un servizio offerto da Hoda e ti mette a disposizione, in forma completamente gratuita, una piattaforma APP per raggiungere i risultati che seguono:
2. Weople ti aiuta ad agire i **diritti più importanti che ti dà il GDPR** (legge europea sulla protezione dei dati personali 679/2016) e si impegna a **custodire e proteggere i tuoi dati**, sempre in **forma anonima e con la massima garanzia per la tua privacy**». «Sì, ma **chi controlla i controllori?**», verrebbe voglia di chiedere. **Forma anonima e rispetto della privacy per tutti, tranne che per i «santi custodi Weople»?**
3. «Weople s'impegna a farti recuperare il maggiore valore possibile dai tuoi dati», continuano, «tramite modalità di investimento e di valorizzazione degli stessi rispettose della tua privacy, **senza mai trasferire i tuoi dati personali a terzi e restituendoti fino al 90% del valore generato dall'investimento** al netto della copertura dei costi di struttura e di esercizio. Il tutto sarà costantemente comunicato in una pagina di trasparenza nell'APP e certificato ufficialmente da terze parti. Anche in questo caso **«dati personali mai trasferiti»: a nessuno tranne che a Weople**.
4. «Creando il tuo profilo depositi e investi in Weople i tuoi dati della scheda d'iscrizione e tutti quelli che vorrai fare arrivare nel tuo conto-dati attivando, con tua libera scelta e senza nessun obbligo imposto dall'App, le cassette di sicurezza che troverai disponibili e spiegate nel tuo caveau personale. Come vedrai, si tratta di dati di consumo dalle tue carte fedeltà, dei dati di utilizzo dei canali digitali come Social, Google, Amazon, eccetera e dei tuoi interessi.

Weople non raccoglie in nessun modo altri dati su di te al di fuori di quelli qui indicati e che tu deciderai liberamente di investire.

5. Per raggiungere gli obiettivi indicati, tu ci permetti, tramite l'accordo, di:
6. Rappresentarti, se lo vorrai, nelle richieste di esercizio dei tuoi diritti GDPR mediante conferimento di apposita delega in nostro favore. Potrai sempre chiederci aggiornamenti sulle attività compiute;
7. Effettuare **operazioni di profilazione sui dati che hai depositato nel tuo conto-dati in Weople** al fine di inviarti **comunicazioni e offerte commerciali personalizzate**. Weople parlerà con i clienti potenzialmente interessati all'invio di queste offerte commerciali per convincerli, in base ai dati aggregati, a investire e a farle. Le offerte te le invierà solo Weople e i tuoi dati saranno trattati sempre in forma anonima e aggregata e non saranno mai trasferiti a livello individuale/personale a nessuno di questi clienti. Questa via d'investimento dei dati ti permetterà di guadagnare somme di denaro vero (non virtuale), versate dagli inserzionisti e depositate da Weople direttamente nel tuo salvadanaio nell'App; ovviamente, ti consentirà anche, in parallelo, di ricevere offerte personalizzate al meglio possibile». Inutile richiamare l'attenzione sulla dicotomia di fondo che ancora torna: Weople potrà svolgere «**operazioni di profilazione sui dati**» **depositati nel caveau** e, comunque anche in questo caso, riceverai **comunicazioni e offerte commerciali personalizzate**. Dove sta il **vero anonimato**, la **vera difesa della privacy** e l'autentica **libertà da pubblicità e inserzionisti**?
8. Conclude il «contratto» di Weople segnalando che, così, tu accordi il permesso a «**elaborare i tuoi dati** e generare modelli statistici generali, dunque non riferibili a te personalmente. I modelli saranno poi utilizzati per arricchire i database di terze parti

sempre, rispetto a te, in forma **anonima, protetta, garantita da Weople e senza trasferire i tuoi dati a livello individuale/personale alle terze parti**. Questo ti consentirà di partecipare alla distribuzione del valore comune, generato dalla piattaforma, in forma di estrazione di premi». Inutile anche qui mettere in luce nuovamente la **contraddizione** almeno apparente fra le **dichiarazioni di garanzia di anonimato** e, nella realtà, **piena proprietà di tali dati da parte di Weople**, che **li conosce nel dettaglio e in veste tutt'altro che anonima**.

La riflessione

Vale la pena, pur essendo chiara la posizione ormai non più solo nostra sul tema, aggiungere qualche riflessione in più: magari leggendo qualche passaggio di un articolo pubblicato sul suo blog da **Marco Valerio Principato**, esperto di comunicazione digitale, da lui sviluppato proprio sulla scia delle riflessioni da me lanciate in rete a maggio. «*L'utente autorizza il "travaso"*» dei dati, si legge, «*e Weople diviene automaticamente titolare di quei dati, che s'impegna a custodire con diligenza e a impiegarli per porre in essere un modello di business. Come fa (almeno teoricamente) Weople a sviluppare e attuare un modello di business fondato sul possesso di dati personali, tale che sia l'utente titolare che Weople stessa possano trarne profitto? In pratica la registrazione e l'identificazione a Weople fanno si che quest'ultima, in quanto titolare, svolga essa stessa analisi e profilazione su tali dati, servendosi anche delle operazioni commerciali, delle transazioni, delle interazioni e delle attività online già svolte sinora da quell'utente ed aggiungendovi ulteriori analisi. Il tutto – a dire dell'azienda – in modo "etico" (è una parola grossa)*», si fa acutamente notare, «*e salvaguardando l'utente stesso mediante anonimizzazione e custodia "cifrata" dei dati e delle relative elaborazioni*».

I problemi però non mancano. Intanto «ipotizzando che "tutti"

(ovvero: molti, moltissimi) facciano ricorso a Weople, si configurerebbe un'eccessiva concentrazione di dati personali e loro custodia in capo ad un solo soggetto giuridico e questo solleverebbe non poche problematiche antitrust. In tal caso, infatti, la raccolta potrebbe non avere i requisiti di liceità previsti». Infatti, ai sensi del GDPR, «*i dati personali possono essere raccolti ed elaborati al ricorrere di una delle condizioni di liceità previste dall'art. 6 del GDPR, per finalità determinate, esplicite e legittime e il trattamento potrà essere eseguito entro i limiti di quanto necessario per il raggiungimento di tali finalità prestabilite». Al contrario la raccolta effettuata da Weople, per sua stessa definizione, avrebbe finalità (almeno inizialmente) indeterminate e implicite, poiché sarebbe impossibile stabilire a priori quali e quanti dati siano necessari per il raggiungimento di una finalità che inizialmente è indeterminata. Inoltre, «i dati utilizzati devono essere limitati a quelli strettamente necessari rispetto allo scopo per cui gli stessi sono raccolti (scopo che deve, inoltre, essere stato precisamente comunicato prima della raccolta agli interessati)*» e «*se dei dati personali non servono, non devono neppure essere raccolti*».

Principato pone, inoltre, la giusta domanda, quanto alla portabilità dei dati sancita dal GDPR e alla base di Weople: «*Mentre le imprese italiane ma, al limite, anche quelle europee, potrebbero non avere troppe difficoltà a operare la portabilità, proprio perché soggette al GDPR, chi assicura che altrettanto facciano imprese che del GDPR possono altamente fregarsene (vedi Google, Samsung, Facebook, Amazon e compagnia)? Nessuno. E oggi moltissime attività di data analysis, di profilazione e di tracciamento passano proprio per quei nomi: basti pensare che il 75% degli smartphone è Android (cioè Google), dove Samsung è quella che ha la maggior quota di mercato, su tali smartphone si svolgono montagne di attività online rivolte a Facebook (basti pensare che tutti hanno WhatsApp, oltre a Facebook, Instagram e Messenger), moltissimi acquisti effettuati su Amazon, ricerche e*

navigazioni (sia Web che terrestri) su Google e comunicazioni interpersonali. Contro simili giganti non possono (quasi) nulla né gli Stati, né il GDPR né, men che meno, Weople».

«*I dati, ragazzi miei, non hanno proprio nulla di "olistico"*», si conclude. «*Sono fatti concreti. O ci sono, o non ci sono. O si trattano, o non si trattano. O se ne abusa, o non se ne abusa. Tertium non datur. Che qualcuno si arroghi il diritto di averli, custodirli, gestirli, "investirli" e farne profitto – condiviso o meno che sia – **non risolve il problema**, **tutt'al più lo sposta**, nel migliore dei casi*». Il che è **esattamente la conclusione cui eravamo giunti noi poco sopra**. In sostanza, che si voglia pensare «bene» o meno bene, il problema resta e si comprende il richiamo del Garante. Le ombre da dissipare ci sono, anche accordando la miglior fede possibile, di cui naturalmente siamo certi. Gli interrogativi, però, iniziano a esser troppi e richiedono risposte. La palla passa a Weople.

https://www.key4biz.it/weople-privacy-e-monetizzazione-dei-tuoi-dati-chi-controlla-i-controllori/268063/

La scomparsa di Giovanni Buttarelli nel ricordo delle associazioni, dei professionisti e degli esperti del settore

Giovanni Buttarelli, Garante europeo della Protezione dei Dati Personali, ci ha lasciati la scorsa notte dopo una lunga malattia.

È stato un *civil servant* di grande e riconosciuta qualità, con una competenza straordinaria ed una forza morale che ne hanno fatto un riferimento europeo insostituibile nella difesa dell'interesse pubblico in ambito di privacy e protezione dei dati. Come capo dell'**EDPS** ha rappresentato un forte motivo di vanto internazionale a favore dell'Italia.

Viene meno con la sua scomparsa un uomo di grande esperienza, ma anche di grande coraggio, che ha saputo affrontare nodi istituzionali di forte rilievo e per ultima una malattia che non gli ha dato tregua, ma che non gli ha impedito di mantenere sino alla fine tutta la sua cordialità, il suo tono accogliente e la sua immutata disponibilità, come quando ha accettato con entusiasmo, nonostante le condizioni avverse, l'invito a partecipare appena poche settimane fa al DIGEAT 2019, dove tutti noi abbiamo avuto il piacere di ascoltarlo nell'ultima apparizione in pubblico.

Giovanni Buttarelli lascia a noi tutti un'eredità di coerenza istituzionale e di conoscenza professionale, ma ancor di più un metodo: quello di aver avuto come riferimento indiscutibile l'interesse pubblico e il bene dei cittadini e dei consumatori.

Lascia questa eredità agli esperti del settore e addetti ai lavori, un'eredità che andrà coltivata e che, siamo certi, rappresenterà un comune patrimonio per gli impegni sfidanti del prossimo futuro.

Con le più rispettose condoglianze alla **famiglia Buttarelli**.

· **Raffaele Barberio**, *Presidente*, Privacy Italia

· **Nicola Bernardi**, *Presidente*, Federprivacy

· **Luca Bolognini**, *Presidente*, IIP

· **Gianluigi Ciacci**, *Presidente*, ANDIG

· **Matteo Colombo**, *Presidente*, AssoDPO

· **Ugo Carlo Di Nicolò**, *Presidente*, UniDPO

· **Michele Iaselli**, *Presidente*, ANDIP

· **Donato A. Limone**, *Direttore*, SNAD e *Presidente*, Advisory Board Privacy Italia

· **Andrea Lisi**, *Presidente*, ANORC-Professioni

· **Rocco Panetta**, Country Leader Italia, IAPP

· **Emilio Tosi**, *Direttore*, Centro Studi Diritto Nuove Tecnologie

https://www.key4biz.it/addio-a-giovanni-buttarelli/268581/

Addio a Giovanni Buttarelli, Garante privacy europeo e tra i padri del diritto alla protezione dei dati

Giovanni Buttarelli, 62 anni, Garante europeo della protezione dei dati, è venuto a mancare la scorsa notte, circondato dall'affetto dei suoi cari: è stato tra i più grandi esperti mondiali di diritto delle nuove tecnologie, diritto alla privacy e alla protezione dei dati personali.

"Siamo addolorati dalla tragica perdita di un uomo brillante e visionario, che si è sempre dedicato con passione alla

famiglia e al lavoro, servendo fino in fondo la magistratura italiana e l'Unione Europea, e onorandone i valori", questo il ricordo dell'European Data Protection Supervisor (**EDPS**), di cui Buttarelli era a capo.

"La sua passione, visionarietà ed intelligenza rappresentano ora e per sempre un'eredità unica e durevole per l'istituzione del Garante europeo e per tutti coloro che sono stati in contatto con lui", conclude la nota dell'EDPS.

Antonello Soro: *'A lui il nostro Paese deve enorme gratitudine per l'introduzione, lo sviluppo e la difesa di un diritto fondamentale per la democrazia e la libertà della persona, come il diritto alla privacy e alla protezione dei dati'*

Il Presidente e il Collegio del Garante per la protezione dei dati personali e tutto il personale dell'Autorità esprimono il più profondo cordoglio per la perdita di Giovanni Buttarelli.

"*E' una notizia dolorosissima, per il Paese, per l'Autorità e per me personalmente perché perdo un amico*" – ha commentato il Presidente **Antonello Soro**. "*La prematura scomparsa di Giovanni Buttarelli rappresenta una perdita inestimabile per la comunità italiana ed europea. A lui il nostro Paese deve enorme gratitudine per l'introduzione, lo sviluppo e la difesa di un diritto fondamentale per la democrazia e la libertà della persona, come il diritto alla privacy e alla protezione dei dati.*

Il ruolo svolto da Buttarelli a livello nazionale ed

internazionale – tra i fondatori dell'Autorità italiana prima e in Europa, poi, da Garante europeo – ha contribuito in maniera determinante alla crescita di una nuova cultura del diritto e a una visione della tecnologia più rispettosa dell'uomo. Ci lascia in eredità la sua esperienza, la sua passione, il suo grande impegno profuso fino all'ultimo a difesa dei valori più alti della persona."

La nostra videointervista a Giovanni Buttarelli in occasione della lezione che ha tenuto il 6 dicembre 2018 al **5G International PhD School** presso il CNR di Roma.

[embedded content]

Addio a Giovanni Buttarelli, Garante privacy europeo e tra i padri del diritto alla protezione dei dati

---

Kaspersky AV injected unique ID that allowed sites to track users, even in incognito mode

reader comments

149 with 88 posters participating

Share this story

Antivirus software is something that can help people be safer and more private on the Internet. But its protections can cut both ways. A case in point: for almost four years, AV products from Kaspersky Lab injected a unique identifier into the HTML of every website a user visited, making it possible for sites to identify people even when using incognito mode or when they switched between Chrome, Firefox, or Edge.

The identifier, as reported Thursday by c't Magazine, was part of a blob of JavaScript Kaspersky products injected into every page a user visited. The JavaScript, presented below this paragraph, was designed to, among other things, present a green icon that corresponded to safe links returned in search results.

c't reporter Ronald Eikenberg found something unsettling about the JavaScript injected by the Kaspersky AV product installed on his test computer—the tag 9344FDA7-AFDF-4BA0-A915-4D7EEB9A6615 was unique to his machine, and it was injected into every single page he visited. It didn't matter if he used Chrome, Firefox, Edge, or Opera or whether he turned on incognito browsing. The identifier acted as a unique serial number that website operators could use to track him.

Kaspersky stopped sending the identifier in June, after Eikenberg privately reported the behavior to the AV company. The identifier was introduced in the fall (for those in the Northern Hemisphere, anyway) of 2015. That meant that for close to four years, all consumer versions of Kaspersky software for Windows—including the free version, Kaspersky Internet Security, and Kaspersky Total Security—silently branded users with a unique identifier.

Eikenberg wrote:

> *In other words, any website can read the user's Kaspersky ID and use it for tracking. If the same Universally Unique*

> *Identifier comes back or appears on another website of the same operator, they can see that the same computer is being used. If this assumption is correct, Kaspersky has created a dangerous tracking mechanism that makes tracking cookies look old. In that case, websites can track Kaspersky users, even if they switch to a different browser. Worse yet, the super tracking can even overcome the browser's incognito mode.*

The behavior stopped in a new version Kaspersky Lab released in June, and the company issued an advisory about the threat a month later. The security issue is tracked as CVE-2019-8286.

Before readers get worked up into too much of a lather, let's review a few things. Even without a unique tracking number, there are plenty of ways for websites to uniquely identify their visitors. IP addresses and cookies are the most obvious ways, but often the specific combination of installed fonts, extensions, and configuration settings are all that's needed to fingerprint a specific user, in some cases even when someone uses multiple browsers.

What's more, Eikenberg told Ars he tested older Kaspersky products with the Tor browser and found no evidence the identifier was injected. The upshot of all this: adding a unique identifier to a security feature seems unnecessary and less than ideal for privacy, but it's not something to make a federal case out of. Last, it wouldn't be surprising if other AV products do, or have done in the past, similar things.

In a statement, Kaspersky officials wrote:

> *Kaspersky has changed the process of checking webpages for malicious activity by removing the usage of unique identifiers for the GET requests. This change was made after Ronald Eikenberg reported to us that using unique identifiers for the GET requests can potentially lead to the disclosure of a user's personal information.*

> *After our internal research, we have concluded that such scenarios of user's privacy compromise are theoretically possible but are unlikely to be carried out in practice, due to their complexity and low profitability for cybercriminals. Nevertheless, we are constantly working on improving our technologies and products, resulting in a change in this process.*
>
> *We'd like to thank Ronald Eikenberg for reporting this to us.*

Kaspersky Lab officials also confirmed that the company's AV products don't interact with TOR traffic.

The larger point of all this is that, as noted earlier, AV protection—whether from Kaspersky or anyone else—can be double-edged. Yes, it may save someone who clicks recklessly on links or attachments, but it can also increase attack surface or add behaviors that many security experts argue are unsafe. (Completely unmentioned in the c't article is the installation of a self-signed digital certificate that many AV products use to inspect HTTPS-protected traffic. That sits wrong with many people who say no application should tamper with TLS traffic.)

Deciding whether to use AV will depend on the user and the type of machine. For a dissident or government contractor actively targeted by state-sponsored hackers—especially when the target is using a Mac or Linux machine—AV probably offers more risk than benefit, since the unique identifier Kaspersky Lab was adding is within the scope of things that might be exploited.

A less experienced user surfing porn sites on a Windows machine, on the other hand, would arguably be better off using AV, since as Kaspersky's statement notes, the identifier isn't something profit-seeking hackers are likely to target. One thing is for certain, whatever decision you make, there will be someone on Twitter to tell you you're wrong and that your

choice is reckless.

https://arstechnica.com/?p=1552529

Found: World-readable database used to secure buildings around the globe

Enlarge / Passwords stored in a database for BioStar 2.

reader comments

71 with 57 posters participating

Share this story

Researchers said they have found a publicly accessible database containing almost 28 million records—including plain-text passwords, face photos, and personal information—that was used to secure buildings around the world.

Researchers from vpnMentor reported on Wednesday that the database was used by the Web-based Biostar 2 security system sold by South Korea-based Suprema. Biostar uses facial recognition and fingerprint scans to identify people authorized to enter warehouses, municipal buildings, businesses, and banks. vpnMentor said the system has more than 1.5 million installations in a wide range of countries including the US, the UK, Indonesia, India, and Sri Lanka.

According to vpnMentor, the 23-gigabyte database contained more than 27.8 million records used by Biostar to secure customer facilities. The data included usernames, passwords and user IDs in plaintext, building access logs, employee records including start dates, personal details, mobile device data, and face images.

“Ridiculously simple passwords”

“One of the more surprising aspects of this leak was how unsecured the account passwords we accessed were,” vpnMentor Internet Privacy Researchers Noam Rotem and Ran Locar wrote. “Plenty of accounts had ridiculously simple passwords, like ‘Password’ and ‘abcd1234’. It’s difficult to imagine that people still don’t realize how easy this makes it for a hacker to access their account.”

The researchers said the data also included more than 1 million records containing actual fingerprint scans. Wednesday’s report provided no data to support the claim, and vpnMentor researchers didn’t respond to a request from Ars to send examples of records that included such scans. TechCrunch security reporter Zack Whittaker said on Twitter that his investigation of several scrambled hashes was inconclusive.

Security experts widely agree that the best way to store or transmit biometric data is by hashing it first to prevent third parties from obtaining it in the event of a breach. If it turns out the database included more than 1 million actual fingerprints, that would be a serious breach because it would expose the people the prints belonged to, and the companies the people worked for, to fraud. Fingerprints, unlike passwords, can’t be changed.

Some of the organizations whose information was public included:

USA

Indonesia

- *Uptown – Jakarta-based coworking space with 123 users.*

India and Sri Lanka

- *Power World Gyms – High-class gym franchise with branches across both countries. We accessed 113,796 user records and their fingerprints.*

United Kingdom

UAE

- *Global Village – An annual cultural festival, with access to 15,000 fingerprints.*
- *IFFCO – Consumer food products group.*

Finland

- *Euro Park – Car parking space developer with sites across Finland.*

Turkey

- *Ostim – Industrial zone construction developer.*

Japan

- *Inspired.Lab – Coworking and design space in Chiyoda City, Tokyo.*

Belgium

- *Adecco Staffing – We found approximately 2,000 fingerprints connected to the staffing and human resources giant.*

Germany

- *Identbase – Data belonging to this supplier of commercial ID and access card printing technology was also found in the exposed database.*

Wednesday’s report said the researchers found the database through an Internet-mapping project that scanned ports of familiar IP blocks for vulnerabilities.

“The team discovered that huge parts of BioStar 2’s database are unprotected and mostly unencrypted,” the researchers wrote. “The company uses an Elasticsearch database, which is ordinarily not designed for URL use. However, we were able to access it via browser and manipulate the URL search criteria into exposing huge amounts of data.”

Besides storing the information in a world-readable database, the vpnMentor researchers said, Suprema also allowed records to be added, deleted, or modified. That left open the possibility that records were added to allow unauthorized people to access sensitive sites. It also opens the door to identity theft, phishing attacks, blackmail, and extortion.

The vpnMentor researchers said they discovered the exposed database on August 5 and privately reported the finding two days later. The data wasn’t secured until Tuesday, six days later. Representatives of Suprema didn’t respond to a request for comment on this story.

https://arstechnica.com/?p=1551547

Quattro app per appuntamenti rivelano l’esatta posizione degli utenti

Ago 14, 2019 Marco Schiaffino Gestione dati, In evidenza, News, Privacy, RSS, Vulnerabilità 0

Le informazioni fornite dalle applicazioni permettono di ricavare l'esatta posizione di 10 milioni di utenti iscritti. Una manna per stalker, spioni e regimi omofobi.

Ormai li conosciamo per essere tra i ricercatori più "tignosi" e scrupolosi nel loro lavoro. Gli analisti di **Pen Tester Partners**, che hanno recentemente reso pubbliche le vulnerabilità di alcuni router 4G, questa volta hanno messo nel mirino le applicazioni per incontri e appuntamenti.

Tutto è cominciato con il report su **3fun**, un'app per smartphone pensata per chi vuole trovare via Internet partner disposti a mettere insieme dei "triangoli amorosi".

Nel segnalare le voragini di sicurezza di 3fun, che permette di recuperare facilmente informazioni personali degli iscritti al servizio, i ricercatori hanno sottolineato anche la possibilità di individuarne l'esatta posizione attraverso una tecnica chiamata "trilaterazione".

Il concetto, simile a quello della triangolazione utilizzato per conoscere la propria posizione partendo dalla distanza da due punti conosciuti, sfrutta una funzione introdotta in molte applicazioni di questo genere, cioè quella che **permette di conoscere la propria distanza dagli altri utenti**.

Come spiegano i ricercatori, utilizzare questa funzione per ottenere l’esatta posizione di un utente è piuttosto semplice. Basta inviare una serie di false coordinate per la propria posizione e utilizzare un programmino che analizza i dati ottenuti relativi a un determinato utente. La precisione, grazie ai sistemi GPS, è elevatissima.

Il tutto funziona in tempo reale e permette, partendo dallo username, di ricostruire gli spostamenti di una persona

nell’arco della giornata arrivando a scoprire potenzialmente quale sia la sua abitazione, dove lavori e quali luoghi visiti nel corso della giornata.

A distanza di una settimana dall’analisi di 3fun, i ricercatori hanno scoperto che la stessa cosa si può fare anche con altre tre applicazioni simili: **Romeo**, **Recon** e il (decisamente) più celebre **Grindr**. La loro analisi è pubblicata in un report che rischia di trasformarsi in una vera “bomba”.

Il risultato è infatti una mappa che permette di localizzare e tracciare i circa 10 milioni di utenti iscritti ai quattro servizi.

La mappa qui sopra mostra gli iscritti alle quattro app individuati nel centro di Londra.

Un bel problema, visto che un’informazione del genere potrebbe essere usata da uno stalker o da un semplice ficcanaso che abbia voglia di sgretolare la (fragile) privacy garantita dalla dimensione digitale.

Per spiegare meglio la questione, i ricercatori sottolineano come nei loro test abbiano facilmente individuato utenti che risultavano posizionati stabilmente alla **Casa Bianca** così come

al **10 di Downing Street**, la residenza e sede del Primo Ministro del Regno Unito. Roba per cui i paparazzi potrebbero andare matti.

Ma c'è di peggio. Visto che le app riportano l'orientamento sessuale degli iscritti (e nel caso di Grinder l'intera utenza appartiene alla sfera gay e bisessuale) la funzionalità potrebbe essere usata anche a scopo discriminatorio, soprattutto in quei paesi in cui vigono legislazioni che reprimono la libertà sessuale.

Secondo i ricercatori, il rischio per la privacy potrebbe essere limitato utilizzando coordinate meno precise e adottando una serie di accorgimenti tecnici che possono impedire il recupero automatico di questi dati attraverso le API delle applicazioni.

Speriamo che gli sviluppatori delle quattro app gli diano retta. Prima che qualcuno decida di approfittarne davvero…

Condividi l'articolo

Nuove falle nel controllo remoto di Windows: aggiornare!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/14/quattro-app-per-appuntamenti-rivelano-lesatta-posizione-degli-utenti/

Airline tracks Twitter user’s real-world ID, publishes her flight number

reader comments

87 with 47 posters participating

Share this story

A security consultant who took to Twitter to call out inappropriate comments made by a Southwest Airline flight attendant received a surprising response when the airline’s official Twitter account included her flight number in its reply while the flight had yet to take off.

The consultant, peeved that the airline tracked down her real-world identity and then broadcast her location, sent a follow-up saying the number amounted to personally identifiable information that the airline was obligated to keep private. The airline’s response: flight numbers aren’t PII. The conversation started out with a tweets like this one, reporting that an attendant on the flight she was boarding was making jokes some passengers found to be offensive:

> *Forgive me because I don’t often fly this airline, but are there boundaries around jokes made by FAs or is that totally at their discretion?@SouthwestAir*
>
> *— Jackie (@find_evil) August 8, 2019*

A Southwest representative using the name Emilia responded

with this:

> *While Southwest Airlines Employees are encouraged to express their creativity and unique personalities when performing their job duties, they should also use good judgment, meet all Safety requirements, and maintain an astute regard for the comfort (1/2) -Emilia*
>
> *— Southwest Airlines (@SouthwestAir)* ***August 8, 2019***

In a follow-up that wasn't deleted until after Ars asked Southwest for comment, Emilia went on to include the flight number of the plane the consultant was boarding. The now apoplectic consultant responded with this:

> *Did you just drop my fucking flight number to the world????????*
>
> *We haven't even taken off, why would you do this? I haven't even DMed you! You just dropped my PII* ***pic.twitter.com/dBq1CvHWZl***
>
> *— Jackie (@find_evil)* ***August 8, 2019***

Emilia sent a response that has also now been deleted that insisted flight numbers aren't PII. Emilia also reminded the consultant that she was "welcome to reach out to us privately in the future if you do not wish to discuss your travel publicly."

The consultant, who identified herself as Jackie Singh, told Ars that a few days earlier, she had used Twitter to commend the service provided by another Southwest agent. In a direct message, a Southwest representative had asked Singh for her flight confirmation number. Singh told Ars that she believes Emilia used that previous interaction to tie Singh's Twitter account to her real-world identity. And with that, Emilia tracked and then tweeted the flight number of the plane Singh

was boarding.

A variety of onlookers came to Singh's defense by trying to explain to Emilia how broadcasting the flight number of a plane a passenger was boarding allowed others to know Singh's location. And for some passengers, this might pose a threat. One onlooker even posted this image showing Sing's real-time location:

> *evil_found* ***pic.twitter.com/WaxIvTNuhM***
>
> *— Neural Netmork (@starsprout)* ***August 8, 2019***

Ars asked Southwest if it was standard policy for representatives to tweet flight numbers of its passengers. More than four hours later, a company official wrote:

> *The Safety and personal comfort of our Employees and Customers is always our top priority, and that includes protecting their right to privacy. Our Team is equipped to respond to Customer inquiries on social media and is trained on handling sensitive Customer data, and they are coached to proactively gather relevant information to understand our Customers' need and quickly resolve their issue and provide an individualized and personal response. It is not our policy to publicly share personally identifiable information about our Employees or our Customers. We have reached out to the Customer to express our apologies and regret over their disappointment, and we look forward to the opportunity to resolve this issue.*

But at the time Ars received the statement, Singh had yet to receive any communication from Southwest. It was only after Ars followed up with the representative and asked if the representative was sure an apology was sent that Singh received a DM from Southwest. It read:

> *Hello Jackie, my name is Colin and I work in Customer*

> *Relations here at Southwest Airlines. I wanted to reach out and apologize for the interaction you had last night regarding your flight with us and the subsequent public post from us outlining your flight number. Our Social Care Team is equipped to respond to Customer inquiries on social media and is trained on handling sensitive Customer data, and we are coached to proactively gather relevant information to understand our Customers' need and quickly resolve their issue. I can definitely understand where your frustration came from as you had not posted your flight number publicly prior to our reply to your complaint. I sincerely apologize for this experience, we hope to see you onboard again soon. - Colin*

The Southwest representative never responded to a question asking if the company planned to train employees not to drop flight numbers of other private passenger information in social media.

https://arstechnica.com/?p=1548757